CONTENTS

Preface xv

Obtaining Documentation and Submitting a Service Request xv

Safety Warnings xv

Safety Guidelines xviii

General Precautions xviii

Protecting Against Electrostatic Discharge xix

Rack Installation Safety Guidelines xix

CHAPTER 1

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 1-11

Cisco PAM Software Overview 1-13

Cisco PAM Desktop Client Software 1-13

Cisco PAM Server Administration Utility 1-14

Cisco Physical Access Gateway Administration Utility 1-15

The Enterprise Data Integration (EDI) Desktop Studio 1-16

Cisco Video Surveillance Viewer 1-17

Badge Designer 1-17

CHAPTER 2

New and Changed Information 2-1

Contents 2-1

Profile Enhancements 2-1

VTG Integration 2-2

VSM 7.0 Integration 2-3

Debounce Timer 2-3

Badge Authentication 2-3

Multifactor Authentication 2-3

Virtual Machine Ware 2-3
CHAPTER 3

Configuring and Monitoring the Cisco PAM Server 3-1

Contents 3-1

Overview 3-2

About the Cisco PAM Server Administration Utility 3-2
Logging on to the Cisco PAM Server Administration Utility 3-2
Using Redundant Appliances for High Availability 3-2
Understanding IP Addresses on the Cisco PAM Server 3-3
Cisco PAM Appliance IP Addresses 3-3
Upgrading a Single Standalone Server to an HA Configuration 3-4
Gateway Module IP Addresses 3-4

Entering the Initial Server Configuration 3-5
Before You Begin 3-5
Connecting a PC to the Appliance 3-5
Initial Setup Instructions 3-7

Configuring Cisco PAM on Virtual Machine (VM) 3-16
Before You Begin 3-16
Configuration Procedure 3-16

Using the Web Admin Menus, Commands and Options 3-17
Accessing the Cisco PAM Server Administration Utility 3-17
Menus and Options in the Cisco PAM Server Administration Utility 3-19
Monitoring 3-20
Setup 3-21
Commands 3-22
Launch Client 3-23
Downloads 3-23

Archiving Historical Events 3-24
Understanding Live, Pruned and Archived Events 3-24
Pruning and Archiving Historical Events 3-25
Installing and Revising Language Packs 3-29
Usage Notes 3-29
Creating or Revising a Language Pack 3-30

Changing or Recovering the Server Password 3-39
Changing the Cisco PAM Server Administration Utility Password 3-39
Resetting a Forgotten Password 3-40
Enabling the Forgot Password Feature 3-42
Recovering a Lost Server Password 3-43

Obtaining and Installing Optional Feature Licenses 3-44
Understanding Module Licenses 3-44
Licenses in a Redundant Configuration 3-44
### Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Purchasing Additional Feature Licenses</td>
<td>3-45</td>
</tr>
<tr>
<td>3</td>
<td>Part Numbers for the Optional Feature Licenses</td>
<td>3-45</td>
</tr>
<tr>
<td>3</td>
<td>Installing Additional Licenses</td>
<td>3-45</td>
</tr>
<tr>
<td>3</td>
<td>Displaying a Summary of Installed Licenses</td>
<td>3-47</td>
</tr>
<tr>
<td>3</td>
<td>Displaying the Cisco PAM Appliance Serial Number</td>
<td>3-47</td>
</tr>
<tr>
<td>3</td>
<td>Performing a Graceful Failover with Redundant Appliances</td>
<td>3-48</td>
</tr>
<tr>
<td>3</td>
<td>Troubleshooting and Monitoring</td>
<td>3-48</td>
</tr>
<tr>
<td>3</td>
<td>Next Steps</td>
<td>3-49</td>
</tr>
</tbody>
</table>

**CHAPTER 4**

**Getting Started With the Cisco PAM Desktop Software**

#### Contents

- Before You Begin 4-2
- Installing or Updating the Cisco PAM Desktop Software 4-2
- Logging in to Cisco PAM 4-3
- Understanding the Start Page and Window Management 4-4
- Keeping a Module On Top 4-6
  - Choosing Multiple *Always on Top* Windows 4-7
  - Deselecting *Always on Top* 4-7
- User Interface Elements 4-8
- Toolbar Features 4-10
  - Creating Reports 4-10
  - Using Filters 4-12
    - Filter Example 4-12
  - Revising the Column Display 4-14
  - Using Group Edit 4-14
    - Group Edit Example 4-15
  - Search 4-15

**CHAPTER 5**

**Configuring User Access for the Cisco PAM Desktop Client**

#### Contents

- Defining User Profiles for Desktop Application Access 5-2
- Creating User Login Accounts and Assigning Profiles 5-8
  - Additional Information 5-11
- Configuring LDAP User Authentication 5-12
  - Configure the LDAP Server 5-12
    - LDAP Example: User Principal Name 5-13
    - LDAP Example: sAMAccountName 5-14
CHAPTER 6

Understanding Door Configuration 6-1

Contents 6-1

Provisioned (Pre-Populated) vs. Discovered Gateway Configurations 6-2

Provisioned (Pre-Populated) Configuration 6-2
Discovered Configuration 6-2

Viewing Device and Door Configuration 6-3

Viewing Doors and Devices in the Hardware View 6-3
Hardware Manager in Cisco PAM 1.4.1 6-5
Viewing Doors and Devices by Location 6-6
Creating the Location Map 6-7
Filtering the Devices Displayed in the Locations View 6-8
Changing the Location of a Device or Door 6-8
Locations and Doors in Cisco PAM 1.4.1 6-9

Viewing Device and Door Status 6-11

Viewing a Status Summary for All Devices 6-11
Viewing the Status for a Single Door, Device or Driver 6-12
Understanding Device Status Colors 6-14
Monitoring Device Errors 6-15
Viewing the Recent Events for a Device, Driver, or Location 6-16
Generating a System Sanity Report 6-18

Understanding Door Configurations and Templates 6-22

Overview 6-22
Sequence for Configuring Templates and Doors 6-23
Door Configurations and Templates 6-24

Template Types 6-24
Impact of Template Changes on Configured Doors and Devices 6-25
Gateway Templates 6-25
Understanding Door Templates 6-25
Understanding Device Templates 6-26
Understanding Credential Templates 6-26
Understanding Reader LED Profiles 6-27

Understanding Door Modes, Door Schedules, and the First Unlock Feature 6-27
Overview  6-27  
Understanding Door Modes  6-28  
Viewing the Door Mode Status  6-29  
Understanding the Default Door Mode  6-30  
Understanding the Scheduled Door Mode  6-30  
Understanding First Unlock Impact on the Scheduled Mode  6-31  
Manually Override the Door Mode Using Commands  6-31  
Impact of Gateway Reset on the Default and Scheduled Modes  6-33  
Understanding Door Schedule Entries in Cisco PAM 1.4.1  6-34  
Configuring the Default and Scheduled Door Modes  6-35  
Locating Serial Numbers  6-39  
Locating Gateway and Expansion Module Serial Numbers  6-39  
Displaying the Cisco PAM Appliance Serial Number  6-39  
Related Documentation  6-40  

CHAPTER 7  
Configuring Doors  7-1  

Contents  7-1  
Configuring Doors  7-2  
  Adding Gateways and Doors Using Templates  7-2  
  Adding Doors Using Door Templates  7-10  
Modifying Door Configurations  7-18  
  Modifying Door and Device Templates  7-18  
  Modifying Devices in the Hardware Device View  7-18  
  Modifying Devices in Hardware Location View  7-19  
  Modifying Devices in the Locations & Doors Module  7-20  
Applying Configuration Changes  7-22  
  Applying Configuration Changes to Gateways  7-22  
    Applying Configuration Changes in the Hardware Module  7-22  
    Applying Configuration Changes in the Locations & Doors Module  7-23  
  Configuration Management in Provisioned vs. Discovered Configurations  7-23  
Disabling or Deleting a Device or Door  7-25  
  Disabling a Device or Door  7-25  
  Deleting Devices and Doors  7-26  
    Enabling the Delete Options  7-27  
    Deleting a Device  7-28  
    Deleting a Gateway Controller  7-28  
Enabling a Device or Door  7-29  
  Disable and Enable a Device and Door: Example  7-29  
Cloning a Gateway Configuration  7-33
CHAPTER 9

Configuring Personnel and Badges 9-1

Contents 9-1
Configuring Personnel 9-2
Downloading Credential Changes to the Gateway Modules 9-11
Viewing Audit Records and Events for Personnel Records 9-12
  Viewing Audit Records 9-12
  Viewing Recent Events 9-14
Editing Organization and Department Lists 9-14
Importing Personnel Records Using a Comma Separated Value (CSV) File 9-16
Using a SnapShell License Scanner to Create Personnel Records 9-22
  Install and Configure the SnapShell Scanner 9-22
  Scan a License to Create a New Personnel Record 9-26
Configuring Badges 9-28
  Configuring Badge Templates 9-28
  Badge Properties 9-30
    Badges Module: General 9-30
    Badges Module: Cisco Access Policy 9-32
    Badges Module: Advanced Gateway 9-33
    Badges Module: HSPD-12 Badge Extension 9-34
    Badges Module: Audit Records 9-35
    Badges Module: Recent Events 9-35
  Badge Authentication 9-36
    Usage Notes 9-36
    Limitations 9-37
Using the Badge Designer 9-37
  Printing Badges 9-45
    List of Recommended Badge Printers 9-45
    Printing Individual Badges 9-46
    Printing Multiple Badges 9-47
    Printing High Resolution Images 9-51
    Changing the Default Badge Printer 9-52
    System Configuration Settings for Badge Printing 9-53
Setting Up Image and Signature Options for Personnel Records 9-55
  Enabling Image Capture Devices 9-55
  Enabling Signature Capture Devices 9-56
CHAPTER 10  Multifactor Authentication  10-1
Contents  10-1
Configuring Generic Readers  10-2
Associating Generic Reader with Doors  10-3
Additional Information  10-6

CHAPTER 11  Configuring Cisco Access Policies  11-1
Contents  11-1
Configuring Access Policies  11-2
Access Policies in Cisco PAM 1.4.1  11-4
Managing Door Access With Access Control Policies  11-5
Using the Schedule Manager  11-8
Schedule Manager in Cisco PAM 1.4.1  11-11
Modifying Types and Time Ranges  11-13
Modifying Work Weeks  11-14
Modifying Holidays  11-14
Modifying Time Ranges  11-16
Modifying Special Cases  11-16
Modifying Time Entry Collections  11-18
Creating Anti-Passback Areas  11-19
Anti-Passback areas in Cisco PAM 1.4.1  11-19
Configuring Anti-Passback Areas  11-20
Using Local (Gateway) Credentials if Network Communication is Lost  11-22
Evicting a Badge from APB if the User Does Not Enter the APB Area  11-24
Monitoring Anti-Passback Events  11-26
Anti-Passback Events Displayed in the Events Module  11-26
Two-Door Policies  11-27
Two-Door Policies in Cisco PAM 1.4.1  11-27
Configuring Two-Door Policies  11-27
Two-Door State Monitoring  11-29

CHAPTER 12  Events & Alarms  12-1
Contents  12-1
Viewing Events, Alarms and Audit Trail Records  12-3
Events and Alarms in Cisco PAM 1.4.1  12-3
Understanding Live and Archived Events  12-3
Understanding Event Timestamps  12-4
Viewing Events  12-4
Contents

Viewing Alarms 12-8
  Main Alarm Window 12-8
  Alarm States 12-9
  Alarm Detail Window 12-9
  Alarm Properties 12-10
Viewing Audit Trail Records 12-13
Viewing Recent Events for a Device, Driver, or Location 12-15

Viewing Events Using Personnel Photos 12-17
  Viewing Event Photos 12-17
  Adding a Color Border to Event Photos (Credential Watch) 12-18
  Using Filters to Limit the Photos and Doors Events Displayed by Event Photos 12-21

Recording External Events 12-25
  Define External Event Types Using the Event Definition Format 12-25
  Create a Text File to Define the Event Names in Cisco PAM 12-26
  Import the Files into Cisco PAM 12-26

Viewing Workstation Activity 12-28

Configuring Events and Alarms 12-29
  Contents 12-29
  Modifying Default Event Policies 12-29
    Configuring Custom Event Policies 12-30
  Event Policy Manager in Cisco PAM 1.4.1 12-30
    Event Policy Properties 12-32
  Automatically Open the Alarm Window 12-34
  Configuring Time Schedules 12-34
  Configuring Alert Sounds 12-37
  Setting Event and Alarm Priorities 12-38
  Defining User Privileges for Editing Events 12-38

Using Graphic Maps 12-40
  Graphic Maps in Cisco PAM 1.4.1 12-40
  Graphic Maps Viewer 12-41
    Icon Colors and Status 12-42
    Device Commands 12-42
    Layers and Views 12-43
    Toolbar and Navigation Controls 12-43
  Graphic Map Editor 12-44

Backing Up and Archiving Events 12-50
  Including Events In System Backups 12-50
  Pruning and Archiving Old Events 12-50
  Creating Reports from Pruned Events 12-51
CHAPTER 13  Configuring Automated Tasks  13-1

Contents  13-1

Creating Quick Launch Buttons  13-2
   Creating a Button  13-2
   Creating a Button That Runs An Automated Rule  13-7
   Creating Panels (Windows) of Related Buttons  13-7
   Restricting User Access to Button Panels  13-8

Configuring Edge Policies  13-9

Configuring Device I/O Rules  13-15

Configuring Global I/O Automated Rules  13-18
   Enabling the Automation Driver  13-19
   Configuring Automated Tasks Using Global I/O  13-21
      Understanding Automated Rule Actions  13-25
   Example: Automated Weekly Report  13-31
   Automation Rules in Cisco PAM 1.4.1  13-35

Defining Reports (Report Manager)  13-39
   Report Manager in Cisco PAM 1.4.1  13-39
   Using the Report Manager  13-40
   Filter-based Report Template  13-41
   Object SQL-based Report Template  13-42
   SQL-Based Report Template  13-43
      Additional Information  13-44

CHAPTER 14  System Integration  14-1

Contents  14-1

Configuring URL Actions  14-2
   Creating or Modifying URL Actions  14-3
   Creating Automated Rules for URL Actions  14-7
   Viewing URL Events, Alarms, and Logs  14-12
      Viewing URL Action Events  14-12
      Viewing Alarms for Failed URL Action  14-13
      Event and Alarm Response Codes for URL Actions  14-13
      Viewing Logs for URL Action Output  14-14
      URL Action Failure Due to Invalid Security Certificate  14-15

Synchronizing Data Using Enterprise Data Integration (EDI)  14-16
   Before You Begin  14-16
      Understanding Photo File Compression When Importing Personnel Records  14-17
   Installing the EDI Licence and Desktop Application  14-18
Creating Active Directory Database Integration Projects Using EDI Studio 14-20
Creating Custom Employee Status Values 14-30
Creating SQL and Oracle Database Integration Projects Using EDI Studio 14-33
Importing, Starting, and Monitoring EDI Projects in Cisco PAM 14-41
  Importing and Starting EDI Projects 14-41
  Verifying EDI Projects (EDI Monitoring) 14-43
  Modifying a Running EDI Project 14-45
  Restarting a Failed EDI Project 14-47
Summary of EDI Administration Functions 14-47

Accessing the SQL Database 14-49
Personnel 14-50
Time and Attendance 14-51
User Tracking Data 14-52

Chapter 15

Video Monitoring 15-1
Camera Manager in Cisco PAM 1.4.1 15-1

Contents 15-2

Enabling Video Monitoring 15-4
  Configuring the Camera Driver 15-4
  Associating Cameras with Doors and Devices 15-8
  PC Workstation Requirements for Live Video Viewing 15-11
  Installing the Cisco VSOM Video Client Desktop Application 15-11

Viewing Video 15-13
  Viewing Live Video in a Grid Arrangement -VSM 6X 15-13
  Viewing Live Video in a Grid Arrangement -VSM 7X 15-17
  Viewing Video for an Event 15-19
  Viewing Event on a VSM Camera Driver 6X 15-20
  Viewing Event on a VSM Camera Driver 7X 15-24
  Defining the Duration of Event Video Recording 15-27

Managing the Camera Inventory 15-28
  Updating the Camera Inventory 15-28
  Deleting the Cisco VSM Cameras 15-30
  Deleting Individual Cameras 15-35

Recording Motion Events from Cisco VSM Cameras 15-37
Triggering Camera Actions and Video Recording in Cisco VSM 15-43

Chapter 16

VoIP Integration 16-1

Contents 16-1
APPENDIX B

Upgrading the Server Software   B-1

Contents   B-1

Upgrade Notes for Release 1.4.1   B-2
  Event Archive Settings Are Required   B-3
  Localization Feature Requires Database Upgrade   B-4
  Gateway Module Firmware Must Be the Same Version as Cisco PAM   B-4
  Credential Download Frequency Must be 60 Minutes or Higher   B-4
  The Door Groups Feature Added to Device Groups   B-5
  Enabling the Password Recovery Feature   B-5
  Upgrading From Release 1.0.3 to Release 1.4.1   B-5
  Split Holiday Schedule Configurations By Month   B-5
  Select the Following Options When Upgrading Gateway Firmware   B-6
  Generic Output Devices Installed Prior to Release 1.1.0 Must Be Rewired   B-6
  Generic Output Device Command and Event Name Changes   B-6
  Browser Time-out   B-7
  Upgrade the Cisco PAM Desktop Client Software   B-7
  Java Requirements   B-7
  Stop EDI Projects Before Upgrading Cisco PAM   B-7
  Change the Database Password Message   B-7

Obtaining Software Images   B-8

Obtaining Release Notes and Other Related Documentation   B-9

Upgrading the Cisco PAM Desktop Software   B-10

Upgrading the Cisco PAM Server Software   B-11

Replacing an Appliance   B-18
  Replacing a Stand-Alone (Non-Redundant) Appliance   B-18
  Replacing Both Appliances in an HA Configuration   B-19
  Replacing a Single Appliance in an HA Configuration   B-21

Reinstalling the Cisco PAM Server Software from a Recovery CD   B-23

APPENDIX C

Upgrading and Configuring Gateway Modules   C-1

Contents   C-1

Displaying the Gateway Network and Firmware Configuration   C-2

Changing the Gateway Module Network Settings   C-4

Changing the NTP Setting for Multiple Gateway Modules   C-7
  (Optional) Set a Default NTP Server   C-7
  Change the NTP Setting for Multiple Gateways   C-8

Using Locations & Doors to Change Gateway Network Settings   C-11

Upgrading Gateway Firmware Images Using Cisco PAM   C-12
Uploading Firmware Images to a TFTP Server C-12
Updating the Firmware on All Gateway Modules C-17
Updating the Firmware on Individual Gateway Modules C-22

APPENDIX D

Security D-1
Contents D-1
Cisco PAM TCP Port Requirements for Firewall Connections D-1
Related Security Documentation D-1
Disabling the Cisco PAM TFTP Server D-2

APPENDIX E

Troubleshooting E-1
Contents E-1
Licensing: Frequently Asked Questions E-1

APPENDIX F

Related Documentation F-1
Cisco Physical Access Control User Documentation F-1
Cisco Video Surveillance Manager (Cisco VSM) User Documentation F-1
Cisco IP Interoperability and Collaboration System (IPICS) Documentation F-2
Related Security Documentation F-2

GLOSSARY

INDEX

Cisco Physical Access Manager User Guide
Preface

- Obtaining Documentation and Submitting a Service Request, page xv
- Safety Warnings, page xv
- Safety Guidelines, page xviii

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.

<table>
<thead>
<tr>
<th>Warning</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read the installation instructions before connecting the system to the power source.</td>
<td>Statement 1004</td>
</tr>
<tr>
<td>Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.</td>
<td>Statement 1</td>
</tr>
<tr>
<td>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.</td>
<td>Statement 12</td>
</tr>
<tr>
<td>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.</td>
<td>Statement 106</td>
</tr>
</tbody>
</table>
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 1-11
- Cisco PAM Software Overview, page 1-13
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 1-11 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 3, “Configuring and Monitoring the Cisco PAM Server”

**Step 3** Install the desktop client. See Chapter 4, “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 6-2.

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:

To do this

Step 1

Assign the appropriate credential templates to the reader templates.

Menu:

Doors:Templates:Device Templates

Instructions:

- Understanding Device Templates, page 6-26
- Understanding Credential Templates, page 6-26
- Configuring Device Templates, page 8-18
- To create additional credential templates, see Configuring Credential Templates, page 8-21.
To do this

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 User Profiles are assigned to one or more locations. Users can only view or configure the devices assigned to those 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 6-2 for more information.

Menu:
Doors:Locations & Doors
Doors:Hardware

Overview Information:
- Viewing Doors and Devices by Location, page 6-6
- Gateway Templates, page 6-25

Instructions:
- Creating the Location Map, page 6-7
- Adding Gateways and Doors Using Templates, page 7-2
- Adding Doors Using Door Templates, page 7-10

Tip To create additional Gateway and door templates, see Chapter 8, “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 11, “Configuring Cisco Access Policies”
To do this

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 9, “Configuring Personnel and Badges”
To do this

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 Step2. 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 6-2 for more information.

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

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 7-22
To do this

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 7-33
- Creating Custom Gateway Configurations and Templates, page 8-2
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>
<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, “New and Changed Information”</td>
<td>New and Changed Information of the current release.</td>
</tr>
<tr>
<td>Chapter 3, “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 4, “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 5, “Configuring User Access for the Cisco PAM Desktop Client”</td>
<td>Describes how to configure Cisco PAM operators.</td>
</tr>
<tr>
<td>Chapter 6, “Understanding Door Configuration”</td>
<td>Describes the terms and concepts used to configure doors and templates.</td>
</tr>
<tr>
<td>Chapter 7, “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 8, “Configuring Door and Device Templates”</td>
<td>Describes how to create and modify Cisco PAM door and device templates.</td>
</tr>
<tr>
<td>Chapter 9, “Configuring Personnel and Badges”</td>
<td>Describes how to create personnel records and badges used to access doors in the Cisco Physical Access Control system.</td>
</tr>
<tr>
<td>Chapter 10, “Multifactor Authentication”</td>
<td>Describes how to configure additional access control devices to ensure security. These devices are called as Generic Readers. These generic readers are biometric devices.</td>
</tr>
<tr>
<td>Chapter 11, “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 12, “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 13, “Configuring Automated Tasks”</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 14, “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>
</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>Chapter 15, “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 16, “VoIP Integration”</td>
<td>Describes how to configure a VoIP phone to Cisco PAM as an additional feature to allow access to personnel without badges.</td>
</tr>
<tr>
<td>Chapter 17, “System Configuration Settings”</td>
<td>Describes the system-wide site settings available in the System Configuration module.</td>
</tr>
<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 the Server Software”</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, “Upgrading and Configuring Gateway Modules”</td>
<td>Describes how to configure network addresses, including IP addresses and an NTP server on the Gateway module using the Cisco PAM software. Also describes how to upgrade the module firmware.</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>Appendix E, “Troubleshooting”</td>
<td>Describes troubleshooting techniques for the Cisco PAM software.</td>
</tr>
<tr>
<td>Appendix F, “Related Documentation”</td>
<td>Provides links to related Cisco Access Control documentation, and documentation for related products.</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 1-13
- Cisco PAM Server Administration Utility, page 1-14
- Cisco Physical Access Gateway Administration Utility, page 1-15
- The Enterprise Data Integration (EDI) Desktop Studio, page 1-16
- Cisco Video Surveillance Viewer, page 1-17
- Badge Designer, page 1-17

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 4, “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 3, “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

![Cisco Physical Access Gateway Administration Utility](image-url)
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 14, “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 3-44 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 15, “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 9, “Configuring Personnel and Badges” for more information.

Figure 1-6 Badge Format Editor

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 3-44 for more information.
New and Changed Information

The Cisco Physical Access Control Release 1.4.1 is backward compatible with the Cisco Physical Access Control 1.3.x and 1.2.x releases. The services that worked with Cisco Physical Access Control 1.3.x continue to work with Access Control 1.4.1.

This chapter summarizes the new and changed features in the Cisco Physical Access Control 1.4.1 release, and provides information on where the feature is documented. For more information on the Cisco Physical Access Control 1.4.1 release, see http://www.cisco.com/en/US/products/ps9688/prod_release_notes_list.html.

Contents

- Profile Enhancements
- VTG Integration
- VSM 7.0 Integration
- Debounce Timer
- Badge Authentication
- Multifactor Authentication
- Virtual Machine Ware

Profile Enhancements

The profile enhancements is a new feature that enriches user profile by enabling location constraints that restricts the access of the logged in user to their locations alone. This feature can be set across several modules. The default hierarchy of a location is:

Base > Campus > Building > Floor > Area > Subarea

The enriched user profile feature is activated under the following conditions:

- Profile may not restrict by hierarchical location
- Allow profiles to be bound to hierarchical locations per assignment

On setting these conditions the system property changes. For more information, see Data Entry/Validation - Login, page 17-9. It displays fields and values that are applicable to the assigned area/location to the profile that is associated to the user. Thus, a user can be associated to several profiles and the one with higher privileges is applied to the login user.
The profile enhancement feature impacts the following modules:

**Table 1  Modules impacted by Profile enhancements**

<table>
<thead>
<tr>
<th>No</th>
<th>Module</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login</td>
<td>Creating User Login Accounts and Assigning Profiles, page 5-8</td>
</tr>
<tr>
<td>2</td>
<td>Profiles</td>
<td>Defining User Profiles for Desktop Application Access, page 5-2</td>
</tr>
<tr>
<td>3</td>
<td>Locations and Doors</td>
<td>Locations and Doors in Cisco PAM 1.4.1, page 6-9</td>
</tr>
<tr>
<td>4</td>
<td>Access Policy, Schedule, Holiday, Work Weeks and Time entry collections</td>
<td>Access Policies in Cisco PAM 1.4.1, page 11-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schedule Manager in Cisco PAM 1.4.1, page 11-11</td>
</tr>
<tr>
<td>5</td>
<td>Device Groups</td>
<td>Device Groups in Cisco PAM 1.4.1, page 7-34</td>
</tr>
<tr>
<td>6</td>
<td>Two-Door Policy/APB</td>
<td>Two-Door Policies in Cisco PAM 1.4.1, page 11-27</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Anti-Passback areas in Cisco PAM 1.4.1, page 11-19</td>
</tr>
<tr>
<td>7</td>
<td>Events and Alarms</td>
<td>Events and Alarms in Cisco PAM 1.4.1, page 12-3</td>
</tr>
<tr>
<td>8</td>
<td>Event Policy Manager</td>
<td>Event Policy Manager in Cisco PAM 1.4.1, page 12-30</td>
</tr>
<tr>
<td>9</td>
<td>Hardware Manager</td>
<td>Hardware Manager in Cisco PAM 1.4.1, page 6-5</td>
</tr>
<tr>
<td>10</td>
<td>Report Manager</td>
<td>Report Manager in Cisco PAM 1.4.1, page 13-39</td>
</tr>
<tr>
<td>11</td>
<td>Global/IO</td>
<td>Automation Rules in Cisco PAM 1.4.1, page 13-35</td>
</tr>
<tr>
<td>12</td>
<td>Graphic Maps</td>
<td>Graphic Maps in Cisco PAM 1.4.1, page 12-40</td>
</tr>
<tr>
<td>13</td>
<td>Camera Manager</td>
<td>Camera Manager in Cisco PAM 1.4.1, page 15-1</td>
</tr>
</tbody>
</table>

**VTG Integration**

The Cisco PAM Server supports use of IP Phone services to grant access to doors. External system can be integrated with Cisco PAM using HTTP. IP Phones can be integrated with Cisco PAM using HTTP service. The integration of VoIP phone to Cisco PAM enables users to grant access to doors through the VoIP phone. This new feature of Cisco PAM allows the entry of personnel without badges.

For more information see, VoIP Integration.
VSM 7.0 Integration

The Cisco PAM integrates with new VSM 7.0, while retaining its support to VSM 6x camera driver. However, at any given point of time, only one driver can be configured and associated with the camera device.

There following GUI level differences between the 6x and 7x camera drivers are:
- Configuring to the VSM server
- Grid Arrangement Options
- Default classification of the camera devices to System folder in 7x
- Viewing the event options

For more information see, Camera Manager in Cisco PAM 1.4.1, page 15-1.

Debounce Timer

The input devices like a door sensor can generate multiple spurious events due to technical defect, or due to vibrations. To prevent spurious events getting logged, a debounce timer can be used to mask events for a specified time interval. The debounce timer ensures that any event that is repeated till a given time is ignored. If the condition persist beyond the time, then the alarm is logged.

For more information, see Debounce Timer, page 8-36.

Badge Authentication

Badge authentication is to validate whether the badge being issued be authenticated for the selected door in the given futuristic timestamp.

For more information, see Badge Authentication, page 9-36.

Multifactor Authentication

The user can integrate additional access control devices like biometric devices with the Cisco PAM to ensure security. These devices are configured as Generic Readers in Cisco PAM server.

For more information, see Multifactor Authentication.

Virtual Machine Ware

Virtual Machine (VM) support is only on UCS Express and UCS C-series. The manufacturing SKU for VM image is done by downloading the software and documentation from CCO, the order and license details are delivered through email.

Currently VM ware supports 20 simultaneous connections for this release.

For more information, see Configuring Cisco PAM on Virtual Machine (VM), page 3-16.
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

- Overview, page 3-2
  - About the Cisco PAM Server Administration Utility, page 3-2
  - Logging on to the Cisco PAM Server Administration Utility, page 3-2
  - Using Redundant Appliances for High Availability, page 3-2
  - Understanding IP Addresses on the Cisco PAM Server, page 3-3
- Entering the Initial Server Configuration, page 3-5
- Configuring Cisco PAM on Virtual Machine (VM), page 3-16
- Using the Web Admin Menus, Commands and Options, page 3-17
  - Menus and Options in the Cisco PAM Server Administration Utility, page 3-19
  - Archiving Historical Events, page 3-24
  - Installing and Revising Language Packs, page 3-29
  - Changing or Recovering the Server Password, page 3-39
  - Obtaining and Installing Optional Feature Licenses, page 3-44
  - Displaying the Cisco PAM Appliance Serial Number, page 3-47
  - Performing a Graceful Failover with Redundant Appliances, page 3-48
- Troubleshooting and Monitoring, page 3-48
- Next Steps, page 3-49
Overview

This chapter provides background information to use the Cisco PAM Server Administration utility to perform the initial setup of your Cisco PAM appliance.

Refer to the following topics:

- About the Cisco PAM Server Administration Utility, page 3-2
- Logging on to the Cisco PAM Server Administration Utility, page 3-2
- Using Redundant Appliances for High Availability, page 3-2
- Understanding IP Addresses on the Cisco PAM Server, page 3-3

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 3-5.
- After the initial server configuration is complete, see Using the Web Admin Menus, Commands and Options, page 3-17.

Note

The Cisco PAM server software is different from the desktop client software. The desktop (client) software runs on a PC and is used to configure devices and access control settings. 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 4-2.

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 3-5.
- 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 optional feature licences.

Note

The high availability (HA) feature requires a separate license. See Obtaining and Installing Optional Feature Licenses, page 3-44.

Understanding IP Addresses on the Cisco PAM Server

The Cisco PAM appliance IP address provides network communication between the appliance and the Gateway modules. The IP address is also used to log in to the system using either a web browser or the Cisco PAM desktop client.

This section describes the different IP addresses that can be configured on an appliance: Eth0, Eth1 and the Shared IP Address.

- Cisco PAM Appliance IP Addresses, page 3-3
  - Eth0 Port IP Address, page 3-3
  - Shared IP Address, page 3-3
  - Eth1 Port IP address, page 3-4
- Upgrading a Single Standalone Server to an HA Configuration, page 3-4
- Gateway Module IP Addresses, page 3-4

Note

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

Cisco PAM Appliance IP Addresses

Each appliance must be configured with an Eth0 IP address. Servers in a redundant configuration must also be configured with a Shared IP address. The Eth1 port is disabled by default but can also be enabled and assigned an IP address. Review the following summaries to determine the configuration required by your deployment.

**Eth0 Port IP Address**

- In a standalone configuration, the Eth0 IP address provides communication between the Cisco PAM appliance and the Gateway modules. The Eth0 IP address is also used to log on to the Cisco PAM Server Administration utility.
- In a redundant HA configuration, the Eth0 ports provides communication between the active and standby appliances. The Eth0 IP address for the active and standby appliance must be different.

**Shared IP Address**

- The Shared IP address is used in a redundant HA configuration and is transferred from the active to the standby server if a failover occurs. This allows system communication to continue since Gateway modules and end users will continue to communicate with the same IP address even after a failover to a different physical server.
• In an HA configuration, the *Shared IP address* is used to log on to the Cisco PAM Server Administration utility, and is configured on each Gateway module.
• The *Shared IP address* and the *Eth0* IP address should be on the same subnet.

**Eth1 Port IP address**

• The *Eth1* port is disabled by default. You can enable and configure the *Eth1* port for remote Internet connections to the Cisco PAM Server Administration utility.
• *Eth0* and *Eth1* can be on separate subnets.

**Upgrading a Single Standalone Server to an HA Configuration**

To change a single standalone server to the active server in an HA configuration, you must configure a Shared IP address on the existing standalone server, and then configure a standby server with the same Shared IP address.

The new Shared IP address is used to log in to the system, and is used for network communication by the Gateway modules.

---

**Note**

The active and standby servers must have unique Eth0 IP addresses.

See the Appendix B, “Upgrading the Server Software” for more information.

If possible, we recommend assigning two IP addresses to a single standalone CPAM server: *Eth0* and the *Shared IP Address*. This allows you to switch from a standalone configuration to an HA configuration without changing the IP address required for user logins.

**Gateway Module IP Addresses**

The Gateway module is configured with the following.

• **Cisco PAM Configuration**—defines the IP address and port of the Cisco PAM appliance used to manage the Gateway. This can be either the Eth0 address in a standalone configuration, or the Shared IP address in an HA configuration. See the “Cisco PAM Appliance IP Addresses” section on page 3-3.
• **Eth0**—defines the network settings for the Eth0 port on the Gateway module. Eth0 is used for network connectivity with the Cisco PAM appliance.
• **DNS**—defines the domain name server (DNS) if names, not IP addresses, are used for the NTP or Cisco PAM addresses.

For instructions to install and configure the Gateway modules, see the Cisco Physical Access Gateway User Guide.

To use Cisco PAM to configure Gateway network settings, see the “Changing the Gateway Module Network Settings” section on page C-4.
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 3-5
- Connecting a PC to the Appliance, page 3-5
- Initial Setup Instructions, page 3-7

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 3-3.
- (Optional) If using NTP synchronization, the address of the NTP server.
- (Optional) The DNS server settings.
- (Optional) An FTP or SFTP server address, username and password, if event archives will be backed up to a remote server.
- 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 3-2:

default username: cpamadmin
default password: cpamadmin

Figure 3-1  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 3-7. The cpamadmin username cannot be changed.

Note  See Changing or Recovering the Server Password, page 3-39 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 3-5](#).

**Step 2**
Enter the server configuration, as shown in Figure 3-2:

- **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 addressees, host name, and HA license.

![Figure 3-2 Initial Setup: Server Configuration](image)

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

**Figure 3-3 Initial Setup: User Configuration**

- **Username**: The admin username cannot be changed. The default username is `cpadmin`.
- **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 3-40).
- Select **Next** to apply the settings and continue.
Step 4 Enter the Network configuration for the Cisco PAM appliance, as shown in Figure 3-4.

- 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 3-4  Initial Setup: Network Configuration

Complete the following Network settings:

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

b. **Shared IP Address**: 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. We recommend configuring a Shared IP Address on all appliances, even if the appliance is a standalone (non-HA) configuration. See Understanding IP Addresses on the Cisco PAM Server, page 3-3 for more information.

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

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

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

   **Note** SSL is enabled by default on all Gateways and Cisco PAM appliances. If SSL is disabled for a Gateway but enabled for Cisco PAM, the Gateway will not be able to connect to the appliance. If the SSL settings are changed, reset all Gateways and the Cisco PAM appliance. We recommend enabling SSL to ensure secure communications.
Chapter 3      Configuring and Monitoring the Cisco PAM Server

Entering the Initial Server Configuration

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 3-3 for more information.

- **IP Address**: Enter the IP address for the Eth0 port. This address should be on the same subnet as the Shared IP address, and must be different on the active and standby appliances.
- **Subnet Mask**: Enter the subnet mask provided by your system administrator.
- **Gateway**: (Optional) Enter the Gateway provided by your system administrator.

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

- **Enable Interface**: Click the check box to enable or disable the Ethernet interface.
- **DHCP**: Click the check box to enable or disable DHCP. When DHCP is enabled, the IP following address fields are inactive since the information is supplied by a DHCP server.
- **IP Address**: Enter the IP address for the Eth0 port. If configured, this address must be different on the active and standby appliances.
- **Subnet Mask**: Enter the subnet mask provided by your system administrator.
- **Gateway**: (Optional) Enter the Gateway provided by your system administrator. If a Gateway is provided for Eth0, leave this field blank.

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

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

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

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

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

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

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

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

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

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

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

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

Step 7 Enter the Date and Time settings. Enter an initial date and time for the server. These settings are used by the appliance and the Cisco Physical Access Gateways. Enter the same settings on the active and standby appliance.
e. **Date & Time**: Click the calendar icon to open a pop-up window and select the current day. The current date and time are inserted from your computer’s date and time settings.

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

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

| Note | We strongly recommend using NTP to synchronize the Cisco PAM appliance and Gateway module clocks to ensure correct event and messaging. See the “Change the NTP Setting for Multiple Gateways” section on page C-8 for more information. |

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** Enter the Event pruning and archiving settings, as shown in Figure 3-5.

- Pruned events are removed from the main events database table and placed in a separate events database, allowing you to reduce the size of the main database while keeping old events accessible on the Cisco PAM system. Pruned events are not visible in Events & Alarms, but are included in reports. Pruned events are also included in system backups.

- Archived events are removed from all Cisco PAM database tables and copied to a compressed file. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archived events are not visible in the Events & Alarms listings or Reports, and are not included in system backups. See the “Archiving Historical Events” section on page 3-24 for more information.

a. Select the **Pruning** tab (Figure 3-5), and enter the following settings:

**Figure 3-5**  **Initial Setup: Event Pruning and Archiving**

- **Live Events Window (days)**—Enter a value between 0 and 500 (inclusive). This is the minimum number of days the events will be available in the live view. The default is 30 days. After the minimum number of days the events will be removed at the next scheduled pruning. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are subject to pruning and archiving (depending on the schedule defined in the following steps).

- The **Pruning Hours** field is enabled only when you select Daily in Schedule. The default value is one.
For other options in Schedule, the Pruning Hours field is read-only. See Figure 3-5.

Note

To ensure that events are regularly pruned, we recommend entering 30 days or less in the Live Events Window field. Entering a value greater than 30 can cause an excessive number of event entries to accumulate in the main database and negatively impact system performance.

The number is rounded to midnight of the last day.

Schedule—define the time and frequency when events should be pruned.
- **Date**—To schedule pruning for one day per month, select Date and then select a day of the month. For example: 15.
- **Weekday**—To schedule pruning once per week, select Weekday and then select a day of the week. For example: Tuesday.
- **Daily**—To run pruning every day, select Daily.
- **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run pruning at 2 p.m., enter 14:00:00. To run pruning at 1 a.m., enter 01:00:00.

b. Select the Archive tab (Figure 3-7) and enter the following settings:
Figure 3-7 Archiving Events

The archive settings are required during the initial setup. After the server is up, you can disable auto-archiving if necessary. See the “Archiving Historical Events” section on page 3-24.

- Enter and re-enter the administrator Password. This password is used to restore the archive file.

- Historic Events Window (days)—Enter the number of days that events will be available in the live view. After the minimum number of days the events will be archived to a compressed file. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are subject to archiving (depending on the schedule defined in the following steps).

- Enter a Schedule when the historic events will be removed from the pruned database and placed into a compressed archive file (archived files are listed above the entry fields).
  - Date—To schedule archiving for one day per month, select Date and then select a day of the month. For example: 15.
  - Weekday—To schedule archiving once per week, select Weekday and then select a day of the week. For example: Tuesday.
  - Daily—To run archiving every day, select Daily.
  - Time—Enter the time in 24 hour format (hh:mm:ss). For example, to run archiving at 2 p.m., enter 14:00:00. To run archiving at 1 a.m., enter 01:00:00.

- (Optional) Select Copy to remote server to automatically copy the archived event files to a remote FTP or SFTP location.
Entering the Initial Server Configuration

**Note**
Only the three most recent archive files are saved. If you do not save the archive file manually or by copying it to a remote server, then the oldest file will be permanently deleted when the fourth file is created.

- **FTP**—for standard File Transfer Protocol servers.
- **SFTP**—for secure file transfers using the Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).
- **Address**—the IP address or hostname of the remote server.
- **Username**—the username required to log in to the server.
- **Password**—the login password for the remote server.
- **Path**—the directory path where the compressed archive will be copied. The path must exist on the remote server. If the directory is not available, the archive will fail.

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

**Tip**
Pruning and Archiving schedules must not overlap each other.

**Step 9**
(Optional) Install additional software license.

![Figure 3-8 Initial Setup: License Installation](image)

**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 3-44 for more information. See also Licensing: Frequently Asked Questions, page E-1.

a. Locate the Product Authorization Key included with the Cisco Physical Access Manager appliance or purchased separately. See Purchasing Additional Feature Licenses, page 3-45.

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 3-8), 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 10**

When you click Finish, the initial installation is applied, as shown in Figure 3-9. 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 3-9 Initial Setup: Setup Progress**

Step 11

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 12

Disconnect your PC from the Eth0 port and connect the Eth0 port to the IP network.
Configuring Cisco PAM on Virtual Machine (VM)

From 1.4.1 Release the Cisco PAM is configured virtually on VM Ware. The VM ware is installed in the UCS server by the UCS Admin. Once connected to the VM ware 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 3-5

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.

In addition, gather the following information:

- An IP address to launch CPAM in VM ware.

Note

Ensure that the VM ware is already created through Vsphere client and the IP address is received.

- 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, three IP addresses are required: One address for the active server, second address for the standby server and third a Shared IP Address setting.
  - (Optional) If using NTP synchronization, the address of the NTP server.
- (Optional) The DNS server settings.
- (Optional) An FTP or SFTP server address, username and password, if event archives will be backed up to a remote server.
- Administrator password. If you are setting up the appliance for the first time, use the default password cpamadmin.

Configuration Procedure

Step 1

Open a web browser on your PC and enter the URL: https://<<cpam IP address>>

Note

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

Step 2

Enter the default username and password as shown in Figure 3-1:

  default username: cpamadmin
  default password: cpamadmin

Step 3

Follow the remaining steps in the setup process, for more information, see Initial Setup Instructions, page 3-7.
Chapter 3      Configuring and Monitoring the Cisco PAM Server

Using the Web Admin Menus, Commands and Options

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.

Refer to the following topics for more information:

- Accessing the Cisco PAM Server Administration Utility, page 3-17
- Menus and Options in the Cisco PAM Server Administration Utility, page 3-19
- Archiving Historical Events, page 3-24
- Installing and Revising Language Packs, page 3-29
- Changing or Recovering the Server Password, page 3-39
- Obtaining and Installing Optional Feature Licenses, page 3-44
- Displaying the Cisco PAM Appliance Serial Number, page 3-47
- Performing a Graceful Failover with Redundant Appliances, page 3-48

Accessing the Cisco PAM Server Administration Utility

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 3-5.
- 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 3-2, 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 3-10. Each tab includes additional selections on the left, or additional drop-down menus.

Step 3 Select an option or command as described in the “Menus and Options in the Cisco PAM Server Administration Utility” section on page 3-19.

Step 4 For settings in the Setup menus, click Update to activate the changes.
Figure 3-10  Cisco PAM Server Administration Utility: Setup Menus

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

**Setup List**
- User
- Network
- DVS
- Email
- Date & Time
- License
- Log Level
- Backup
- Archive
- Restore
- Upgrade

**Setup > User**
- Username: openedmin
- Current Password: ********
- New Password: 
- Re-enter Password: 
- Email Address: user@abc.com

[Update] [Cancel]
Menus and Options in the Cisco PAM Server Administration Utility

The following sections describe the configuration, administration, and monitoring tasks available in the Cisco PAM Server Administration utility.

- Monitoring, page 3-20
- Setup, page 3-21
- Commands, page 3-22
- Launch Client, page 3-23
- Downloads, page 3-23
## Monitoring

Monitoring displays the current and past state of the server, and includes the following submenus.

### Table 3-1 Monitoring Menu

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
  - **Admin State**: *Up* means the appliance is available for use. *Down* means the appliance is unavailable for access control functions. This allows you to take the server offline for administrative functions and updates without actually shutting down the server.  
  - **Server Mode**: In an HA configuration, the server mode can be either *Active* or *Standby*. See the “Using Redundant Appliances for High Availability” section on page 3-2.  
  - **Version**: The release number of the current Cisco PAM appliance server software.  
  - **Serial Number**: the serial number of the Cisco PAM appliance. For example, 00151729764C.  
  - **High Availability Audit**: If HA is configured, the audit is enabled.  
  - **Peer Address**: The IP address of the HA server paired with the current server. For example, 192.168.2.1.  
  - **Peer Hostname**: The hostname of the HA server paired with the current server. For example, CPAM-75.  
  - **Synchronization Status**: the status of the HA synchronization process. The options are:  
    - **Synchronized**: HA synchronizations were completed without errors.  
    - **Failed to retrieve the Status**: An error occurred while retrieving the Sync status. For example, the peer server is down or unreachable. See the `webapp.log` file for details.  
    - **Stopped**: the appliance is in Admin *Down* state, and HA synchronization is stopped.  
    - **Error**: An error was detected during synchronization. Additional details are displayed with the `Error Code` and `Error String` retrieved from the database.  
    - **In-progress**: The synchronization process is in progress. At least one synchronization actions has not completed.  
  - **TFTP Service**: Determines if the TFTP service is available for updating firmware images. See the “Upgrading Gateway Firmware Images Using Cisco PAM” section on page C-12 and the “Disabling the Cisco PAM TFTP Server” section on page D-2.  
  - **Web Service API**: Determines if Cisco PAM web services are available. The service is enabled by default but requires an optional license for activation. See the Cisco Physical Access Control API Reference Guide for more information. |
| Server Log         | Displays real-time information regarding server tasks. |
| Setup Log          | Displays real-time information regarding server setup tasks performed on the appliance. |
| Web Application Log| Displays real-time information regarding events related to server administration tasks. |
| Audit Log          | Displays a history of tasks performed by the administrator username. |
| Console Log        | Displays a real-time console log. |
Chapter 3  Configuring and Monitoring the Cisco PAM Server

Using the Web Admin Menus, Commands and Options

Table 3-1  Monitoring Menu (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability Audit Log</td>
<td>Displays real-time events related to a redundant server configuration.</td>
</tr>
<tr>
<td>URL Log</td>
<td>Displays the output (HTTP response) from URL actions.</td>
</tr>
</tbody>
</table>

**Setup**

Allows you to view and edit the server configuration using the following submenus.

*Note*  Click **Update** to save and activate your changes.

Table 3-2  Setup Menu

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The username, password and email of the administrator login.</td>
</tr>
<tr>
<td>Network</td>
<td>The IP address configuration for the appliance and for the Eth0 and Eth1 network ports. See Entering the Initial Server Configuration, page 3-5 for more information.</td>
</tr>
<tr>
<td>DNS</td>
<td>The DNS settings for the appliance, if DNS is used.</td>
</tr>
<tr>
<td>Email</td>
<td>The email settings for the appliance, including SMTP Server Address and SMTP Email Address from. These settings are used to send notifications and other information from the server.</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>Date &amp; Time</td>
<td>The server date and time settings. If a network time protocol server is used, click NTP enable and enter the NTP Server Address settings.</td>
</tr>
<tr>
<td></td>
<td><em>Note</em> We strongly recommend using NTP to synchronize the Cisco PAM appliance and Gateway module clocks to ensure correct event and messaging. See the “Change the NTP Setting for Multiple Gateways” section on page C-8 for instructions to set NTP on Gateway modules.</td>
</tr>
<tr>
<td>License</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 3-44.</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>Log Level</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>Backup</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-1.</td>
</tr>
<tr>
<td>Event</td>
<td>Prunes and archives historical events from the Cisco PAM database. Prunes events are moved to a separate database table. Archived events are saved in a password protected .zip file. See the Archiving Historical Events, page 3-24 for more information.</td>
</tr>
</tbody>
</table>
Table 3-2  Setup Menu (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore</td>
<td>Restores data from a backup or archive file. The server must be stopped using Stop Server in the Commands menu. See Restoring a Server Backup File, page A-8.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Upgrades the server software. To upgrade the server, select Stop Server from the Commands menu, click Browse to select an upgrade file, and then click Upgrade. Select Start Server from the Commands menu when the upgrade is complete. See Upgrading the Cisco PAM Server Software, page B-11.</td>
</tr>
<tr>
<td>Localization</td>
<td>Allows you to create and add language packs that display Cisco PAM menus and other text in a language other than English. You can also display both English and a second language at the same time. See the “Troubleshooting and Monitoring” section on page 3-48.</td>
</tr>
</tbody>
</table>

**Note**  The server has to be stopped to enable Localization. You need to upload the required language pack, start the server and download the new client for the server.

Commands

Provides commands to stop, start and reboot the server. Also includes commands to gather current information from a running server for use in troubleshooting and monitoring. This menu includes the following:

Table 3-3  Commands Menu

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Server</td>
<td>Enables the Cisco PAM access control server functions and user logins.</td>
</tr>
<tr>
<td>Stop Server</td>
<td>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>
</tr>
</tbody>
</table>

**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,

**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. See Importing, Starting, and Monitoring EDI Projects in Cisco PAM, page 14-41.

| Reboot           | Performs a hard reboot of the appliance which restarts the OS and the access control server. |
| Shut Down        | Shuts down the appliance. All access control functions stop unless a standby appliance is installed and configured. To restart the appliance and access control server, you must physically power down and then power on the appliance. |
| Show 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. |
| Processes        | Displays the processes running on the system for use in troubleshooting. |
Launch Client

Launches the Cisco PAM desktop client. If the client is not installed or is out of date on your workstation, an installation screen appears. Follow the onscreen prompts to install or upgrade the desktop client (if necessary), and launch the application.

Note

If necessary, the required Java application is also installed. This link is the same as the client installation link on the log in page (Figure 3-2) and in the Downloads menu.

Downloads

Provides links to download additional software, including the following:

<table>
<thead>
<tr>
<th>Table 3-4 Downloads Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Download</strong></td>
</tr>
<tr>
<td>JRE 1.6 (Windows)</td>
</tr>
<tr>
<td>Cisco PAM Client (JRE required)</td>
</tr>
<tr>
<td>Cisco EDI Studio (JRE required)</td>
</tr>
<tr>
<td>SnapShell Driver</td>
</tr>
<tr>
<td>Snap Shell SDK</td>
</tr>
</tbody>
</table>
Archiving Historical Events

If access control events are allowed to accumulate in the Cisco PAM database, the storage and backup requirements of the database tables can become unmanageable and affect system performance. To avoid this condition, use the event management feature to automatically prune old events from the main Cisco PAM database, and create compressed archive files of historic events. The archive file includes a password-protected SQL script, and can be run on an offline database to view the purged events.

This event management process is defined during initial system setup, as described in the “Entering the Initial Server Configuration” section on page 3-5. Use the instructions in this section to change the pruning and archiving settings.

This section includes the following topics:

- Understanding Live, Pruned and Archived Events, page 3-24
- Pruning and Archiving Historical Events, page 3-25

Understanding Live, Pruned and Archived Events

Events are stored according to the following categories:

- Live Events
- Pruned Events
- Archived Events

Live Events

Live events are recent events that are stored in the main Cisco PAM database table. Live events are visible in Events & Alarms and can be included in system backups.

Pruned Events

Pruned events are removed from the main events database table and placed in a separate events database, allowing you to reduce the size of the main database while keeping them accessible on the Cisco PAM system. Pruned events are not visible in Events & Alarms, but are included in reports. Pruned events can also be included in system backups.

Tip

See the “Creating Reports from Pruned Events” section on page 12-51

The following conditions apply when pruning events:

- 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

The pruning process can impact system performance. Schedule pruning to occur during off-peak hours.
Archived Events

Archived events are removed from all Cisco PAM database tables and copied to a compressed file. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archived events are not visible in the Events & Alarms listings or Reports, and are not included in system backups.

Archiving historic events improves system performance and simplifies monitoring since only the latest, most relevant, events and alarms are displayed. System backup file sizes are also reduced. 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.

The saved file includes the date (mm/dd/year), the Cisco PAM version number, and other information. For example, cpam-09242012-1200001.4.1_0.3.6.archive.zip. The three most recent archive files are saved. When a fourth archive file is added, the oldest file is deleted. You can right click a filename to save it to a local or network drive, or use the option in the following procedure to automatically copy archive files to a remote server.

Archived event files can be restored to Cisco PAM, if necessary. Restored archive events do not appear in the Event and Alarm Monitoring windows, but you can run reports on them. See the “Creating Reports from Pruned Events” section on page 12-51 for more information. Archived event files can also be used by other applications to view old events or run reports.

Pruning and Archiving Historical Events

Event management settings are entered during the initial server setup, as described in the “Entering the Initial Server Configuration” section on page 3-5. Use the following procedure to revise the pruning and archiving settings.

Procedure

Step 1 Log on the Cisco PAM Server Administration utility, as described in the “Logging on to the Cisco PAM Server Administration Utility” section on page 3-2.

Step 2 Choose Setup and then Event (Figure 3-11).
Step 3  Select the **Pruning** tab, and enter the following settings:

a. **Live Events Window (days)**—Enter a value between 0 and 500 (inclusive). This is the number of days of events that will be available on live view. All the events older than the specified days will be removed at the pruning schedule time. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are subject to pruning and archiving (depending on the schedule defined in the following steps).

Note  To ensure that events are regularly pruned, we recommend entering 30 days or less in the **Live Events Window** field. Entering a value greater than 30 can cause an excessive number of event entries to accumulate in the main database and negatively impact system performance.

- The number is rounded to midnight of the last day.

b. **Schedule**—define the time and frequency when events should be pruned.

- **Date**—To schedule pruning for one day per month, select **Date** and then select a day of the month. For example: 15.

- **Weekday**—To schedule pruning once per week, select **Weekday** and then select a day of the week. For example: Tuesday.

- **Daily**—To run pruning every day, select **Daily**.

- **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run pruning at 2 p.m., enter **14:00:00**. To run pruning at 1 a.m., enter **01:00:00**.

c. **Pruning Hours**— This field is enabled only when Daily is selected in Schedule. The default value is one.

Note  The Pruning Hours field is available from Cisco PAM 1.4.1 release.

d. Select **Update** to save the changes.
Step 4  Select the Archive tab (Figure 3-12) and enter the following archive settings:

**Figure 3-12   Archiving Events**

- Compressed files containing archived events are listed above the entry fields. The file name includes the archive date & time. For example: March 01, 2011 11:16:08 AM PDT.

- The three most recent archive files are saved. When a fourth archive file is added, the oldest file is deleted. You can right click a filename to save it to a local or network drive, or use the option in the following procedure to automatically copy archive files to a remote server. The saved file includes the date (mm/dd/year), the Cisco PAM version number, and other information. For example: cpan-09242012-1200001.4.1_0.3.6.archive.zip.

- No of Historical Events are the number of historical pruned events that were pruned from the main database table. See the “Understanding Live, Pruned and Archived Events” section on page 3-24.

  a. Enter and re-enter the administrator **Password**. Enter and re-enter the administrator **Password**. This password is used to restore the archive file (similar to backup files).

  b. **Historic Events Window (days)**—Enter the number of days that events will be available for reports. After the minimum number of days the events will be archived to a compressed file. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are subject to archiving (depending on the schedule defined in the following steps).

  c. Select **Automatic Archive** to enter a schedule when the historic events will be removed from the database and placed into a compressed archive file (archived files are listed above the entry fields).
Tip
De-select **Automatic Archive** to run manual archive operations only, or to disable archiving on the standby appliance in an HA configuration.

- **Date**—To schedule archiving for one day per month, select **Date** and then select a day of the month. For example: 15.
- **Weekday**—To schedule archiving once per week, select **Weekday** and then select a day of the week. For example: Tuesday.
- **Daily**—To run archiving every day, select **Daily**.
- **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run archiving at 2 p.m., enter 14:00:00. To run archiving at 1 a.m., enter 01:00:00.

d. (Optional) Right-click an archived filename and select a save option from the browser menu.

e. (Optional) Select **Copy to remote server** to automatically copy the archived event files to a remote FTP or SFTP location.

Note
Only the three most recent archive files are saved. If you do not save the archive file manually or by copying it to a remote server, then the oldest file will be permanently deleted when the fourth file is created.

- **FTP**: for standard File Transfer Protocol servers.
- **SFTP**: for secure file transfers using the Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).
- **Address**—the IP address or hostname of the remote server.
- **Username**—the username required to log in to the server.
- **Password**—the login password for the remote server.
- **Path**—the directory path where the compressed archive will be copied. The path must exist on the remote server. If the directory is not available, the archive 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.

f. Click **Update** to save the changes.
Installing and Revising Language Packs

Optional language packs are installed on the Cisco PAM appliance to display Cisco PAM menus and other text in a language other than English. You can install more than one language pack, and users can select one of those languages when logging in to the Cisco PAM application (Figure 3-13). Users can also select Dual-language mode to display text and menus in both English and the selected language.

Figure 3-13 Login Screen

Although a language pack may be available for your deployment, you can create new language packs or edit the installed packs by downloading and editing a set of XML files used to display the menus and other text.

Usage Notes

- If you upgrade the Cisco PAM appliance from release 1.2.0 or lower to release 1.3.0 or higher, you must also upgrade the system database to support localization. This is a one-time process performed by clicking an Enable Localization button the first time you access the localization feature. This procedure is also required if you restore a data backup from release 1.2.0 or lower to release 1.3.0 or higher. This process can take up to one hour (or more) to complete for large databases. See the “Creating or Revising a Language Pack” section on page 3-30 for instructions.

- Log files and the Cisco PAM Server Administration utility appear in English even if a language pack is installed.
Creating or Revising a Language Pack

To create a new language pack translation, download a set of XML template files for the language you want to use. You can download and edit a language pack that was previously uploaded, or download and edit a new set of template files.

Next, edit the XML files to include the translated text you want to appear in the Cisco PAM desktop application. Then save the revised files using the same filename and compress the directory containing the XML files.

**Note**
The directory and compressed .zip archive can be any name you choose, but the XML files contained in that compressed .zip file must have the same file names as the originals.

Import the compressed language pack file into the Cisco PAM appliance using the Cisco PAM Server Administration utility. Finally, reinstall the Cisco PAM desktop application, which includes the new language pack.

Editing a language pack that was previously installed is the same process as creating a new language pack. Instead of downloading a new template, however, you download and edit the language pack files that were previously installed.

**Procedure**
Complete the following procedure to create or edit a language pack for any language.

**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 3-5.
- For an Internet connection, open a web browser and enter the IP address used for the Cisco PAM Server Administration utility. See Accessing the Cisco PAM Server Administration Utility, page 3-17, or ask your system administrator for assistance.

**Step 2**
(Optional) Perform a system backup, as described in Appendix A, “Backing Up and Restoring Data”.

**Tip**
Back up system data before performing any major operation to ensure the integrity of your existing data.

**Step 3**
Select **Setup**, and then select **Localization** (Figure 3-14).

**Step 4**
Enable localization, if necessary (Figure 3-14):
- This step is only necessary if you are upgrading or restoring data from Release 1.2.0 or lower.
- If your appliance is a new installation, skip to **Step 5**. You can also skip to **Step 5** if localization was previously enabled on the appliance.
a. Place the server in the Down state.
   - Click the Monitoring tab and select Stop in the Admin State entry.
   - Verify that the Admin State is Down.

b. Return to the Localization window and click Enable Localization (Figure 3-14).

c. Click OK when the confirmation message appears.

d. Wait for the message The localization feature is enabled to appear. This can take up to one hour or more for large databases.

Tip The Upload and Download buttons are also enabled when the conversion process is complete.

Step 5 To edit an existing language pack, click the Download link next to the installed language (Figure 3-15), and skip to Step 7.
To create a new language pack, download a language template:

a. Select the **Download templates** radio button (Figure 3-16).

b. Choose a language from the Language menu.

c. Select **Download**.

d. Continue to **Step 7**.

Select a location on your hard drive to save the compressed `.zip` file.
Chapter 3  Configuring and Monitoring the Cisco PAM Server

The filename includes the release number, and language code. For example: languagepack_zh_1.4.1_0.3.31

Step 8  Edit the XML files to include the translated text:

a. Unzip the compressed language pack directory.

b. Open each file in a Unicode-supported editor.

   For example: in Windows, right-click the file name and select Open with and then XML Editor (Figure 3-17).

   c. Enter the translated text for each Translation Unit.

   For each Translation Unit, there are two item entries: one for English (en), and another for the language you are translating (Figure 3-18).

   ```xml
   <TranslationUnit type="ModuleCategory">
     <uniqueId>GW.SCHEDULES</uniqueId>
     <Map id="names">
       <item>
         <String id="key">en</String>
         <String id="value">Schedule Manager</String>
       </item>
       <item>
         <String id="key">es</String>
         <String id="value">Schedule Manager</String>
       </item>
     </Map>
   </TranslationUnit>
   ```

   English text  Translate this "value"
- **String id “key”** identifies the language. The English (en) entry shows the English text, and an additional “key” entry identifies language you need to translate. For example, Spanish is represented as “es”. Do not change these “key” values.

- **String id “value”** is the actual text of the item. Replace the English sample with the translated text for your language. This is the text that will appear in the Cisco PAM application.

**Note**
- Do not change the text value of the “en” item. This is the English text and allows both languages to appear in the Cisco PAM client application.
- The items for English and the second language appear in a different order, depending on the language pack and XML file. For example, in some XML files, the English entry may appear first. In other files, the second language may appear first. Always verify that you are editing the correct language. Never modify the English (en) key or value.

d. Save each XML file using the same file names as the originals.
e. Repeat these steps to translate each required XML file in the language pack.

**Step 9**
Place the translated language pack files in a directory and compress the directory as a .zip archive. The directory and compressed .zip archive can be any name you choose, but the XML files contained in that compressed .zip file must have the same file names as the originals.

**Step 10**
Place the active and standby Cisco PAM appliances in the Admin State Down state.
The server must be in Admin State Down to upload the compressed language pack file. If your deployment includes a redundant standby server, place the standby server in Down state first to prevent a failover.

**Caution**
Placing the server in Admin State Down stops all Cisco PAM services. If a redundant Standby server is configured, you must also place the Standby server in the Admin State Down state.

a. Log on to the standby Cisco PAM appliance (if configured).
b. Select Monitoring and then Status (Figure 3-19).
c. Select Stop (next to Admin State).
a. Log on to the active Cisco PAM appliance.
b. Select Monitoring and then Status (Figure 3-19).
c. Select Stop (next to Admin State).

Step 11 Upload the revised language pack.

a. Select Setup and then select Localization.
b. Select the Upload language pack radio button (Figure 3-20).
c. Select the language you want to import from the drop-down menu.
d. Click Browse and select the compressed file that contains the revised XML files.
   For example: languagepack_zh_1.4.1_0.3.31

e. Click Upload.
Figure 3-20  Apply the Language Pack

Step 12  Wait for the upload to complete and click OK when the confirmation message appears.

Step 13  Confirm that the correct language pack was installed (Figure 3-21).

Figure 3-21  Languages Installed on the Cisco PAM Server

Step 14  Restart the Cisco PAM server.
Chapter 3  Configuring and Monitoring the Cisco PAM Server

Using the Web Admin Menus, Commands and Options

Note  The server must be in Admin State *Up* to initialize the language pack and for users to access the system.

a. Select **Monitoring** and then **Status**.
b. Select **Start** next to Admin State.

**Step 15**  Download and install the new version of the Cisco PAM client application.

Note  The new language will not be available until you uninstall and reinstall the client application.

a. If the Cisco PAM client is installed on your Windows PC, uninstall it.
   - Go to **Start** > **Programs** > **Cisco Physical Access Manager** > **Uninstaller** and follow the onscreen instructions.
   - Or go to **Start** > **Control Panel** > **Uninstall a Program** > **Cisco Physical Access Manager** and choose **Uninstall**.
b. Use one of the following methods to reinstall the desktop client:
   - In the Cisco PAM Server Administration utility, click **Launch CPAM Client**.
   - Select **Downloads** and then **Cisco PAM Client (JRE required)**.
   - Click **Launch CPAM Client** on the web utility login page.

tip  See the “Installing or Updating the Cisco PAM Desktop Software” section on page 4-2 for more information.

c. Follow the onscreen instructions to install and launch the updated Cisco PAM client.

**Step 16**  Select the new language when logging in to the Cisco PAM desktop client (Figure 3-22).

a. Launch the Cisco PAM application.
b. In the Log In window, choose the language you want to use (Figure 3-22).
c. (Optional) Select **Dual-language mode** to display both languages in the application.
d. Enter the server hostname or IP address, username, and password.
e. Click **Log In**.
Step 17 Verify that the translated text appears correctly in the Cisco PAM application (Figure 3-23). If you chose Dual-language mode, English appears after the translated text (in parentheses).

![Figure 3-22 Selecting a Language at the Cisco PAM Login](image)

Step 18 If corrections are required, return to Step 5 to download and edit the XML files for an existing language pack. You must uninstall and reinstall the CPAM client application each time you upload a language pack for the changes to appear.

Tip The Login screen (Figure 3-22) also displays the selected language the next time you log in.
Changing or Recovering the Server Password

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

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

Note

- The cpamadmin username is the only username supported on 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.
- 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 effect the desktop account. See Chapter 5, “Configuring User Access for the Cisco PAM Desktop Client” for more information.

This section includes the following information:

- Changing the Cisco PAM Server Administration Utility Password, page 3-39
- Resetting a Forgotten Password, page 3-40
- Recovering a Lost Server Password, page 3-43

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 3-5.
- 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 3-2, or ask your system administrator for assistance.
Step 2  Select the Setup tab and then select the User menu, as shown in Figure 3-24.

Figure 3-24  Cisco PAM Server Administration Utility: Setup Menus

![Cisco PAM Server Administration Utility: Setup Menus]

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 5, “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 3-42). 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 3-43.
- The server password is different from the Cisco PAM desktop client password. See Chapter 5, “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 3-25.

**Figure 3-25  Forgot Password Link**

![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 3-26.

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

**Figure 3-26  Reset Password Page**

![Reset Password Page](image)

**Step 4** Enter and reenter your new password, and then click **Update**.

**Step 5** Log in using the new 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 3-27.

**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 3-28.

---

**Figure 3-27  Email Recipient for Forgot Password**

![Email Recipient for Forgot Password](image)

b. Enter an Email Address that will receive Forgot Password emails.

c. Click **Update**.
Figure 3-28  Send Email Settings for Forgot Password

<table>
<thead>
<tr>
<th>SMTP Server Address:</th>
<th>email.cisco.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Email Address from:</td>
<td><a href="mailto:user@cisco.com">user@cisco.com</a></td>
</tr>
</tbody>
</table>

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 cpmadmin password is lost and the Forgot Password? feature is not enabled, do the following.

---

Step 1  Reinstall the server software and enter a new cpmadmin password, as described in Reinstalling the Cisco PAM Server Software from a Recovery CD, page B-23. 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 1.2 includes a 4 module base license
- Release 1.3.1 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 3-5 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 3-44
- Licenses in a Redundant Configuration, page 3-44
- Purchasing Additional Feature Licenses, page 3-45
- Installing Additional Licenses, page 3-45
- Displaying the Cisco PAM Appliance Serial Number, page 3-47
- Displaying a Summary of Installed Licenses, page 3-47

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 32 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 3-45 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 E-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 appliance. See Entering the Initial Server Configuration, page 3-5.

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 3-5: 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 3-47 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 3-45 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 3-5 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

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 3-5.

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.
Figure 3-29  Installing Optional Feature Licenses

Procedure

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 3-29), 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 3-47 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 3-30.

![License Features List](image)

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 3-5.
- 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 3-2, 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 3-31.

**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 Using the Web Admin Menus, Commands and Options, page 3-17 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 Using the Web Admin Menus, Commands and Options, page 3-17 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 E-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 4, “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.
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 4-2
- Installing or Updating the Cisco PAM Desktop Software, page 4-2
- Logging in to Cisco PAM, page 4-3
- Understanding the Start Page and Window Management, page 4-4
- Keeping a Module On Top, page 4-6
- User Interface Elements, page 4-8
- Toolbar Features, page 4-10
  - Creating Reports, page 4-10
  - Using Filters, page 4-12
  - Revising the Column Display, page 4-14
  - Using Group Edit, page 4-14
  - Search, page 4-15
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:
  - Windows XP or Vista and Internet Explorer 6.0 or higher, or Windows 7 (64-bit only) and Internet Explorer 8.0 (32-bit only).
  - 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.
  - 2GB 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 3-5.
- 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 3-3, or ask your system administrator for assistance.

**Step 2** Select **Launch Cisco PAM Client** from the Login window, as shown in Figure 4-1.

- 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 4-2).

Figure 4-2  Login Screen

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).
Step 3 Choose a language, if available.

Step 4 (Optional) Select Dual-language mode to display both languages in the application.

Step 5 Click Log In.

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 4-3. The main menus provide access to Cisco PAM features, and are also displayed in the main window for each feature.

Figure 4-3 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 3-44 and Chapter 5, “Configuring User Access for the Cisco PAM Desktop Client”.

Note
Select a menu item to open the main window for that feature in a new window, as shown in Figure 4-4. 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 4-4    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 4-5.

**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 4-5  Always on Top**

When selected, **Always on Top** is displayed with a check (Figure 4-7). 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 4-6), 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 4-6** Always on Top Confirmation Message

![Figure 4-6](image)

Deselecting *Always on Top*

To deselect Always on Top, do the following:

1. Deselect *Always on Top* to remove the check (Figure 4-7).
2. Click OK to close the confirmation message (Figure 4-6). If the confirmation message is hidden behind an existing Window on Top, rearrange the windows so you can clear the message.
3. Close the Cisco PAM window and reopen it for changes to take effect.
4. Repeat these steps to deactivate *Always on Top* for additional windows.

**Figure 4-7** Deselecting Always on Top

![Figure 4-7](image)
User Interface Elements

The user interface for most features includes the following elements:

The following items are shown in Figure 4-8:

Table 4-1  User Interface Elements

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Window Title Bar</td>
</tr>
<tr>
<td>2</td>
<td>Menu Bar</td>
</tr>
<tr>
<td>3</td>
<td>Table Columns</td>
</tr>
</tbody>
</table>
### Table 4-1: User Interface Elements

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| **4** Toolbar | Contains a set of button functions that are specific to the module being used. Typical buttons include:  
  - **Scroll Lock**: Disable or enable automatic scrolling of the list as new items are inserted.  
  - **View...** or **Edit...**: View or edit the selected item in a detail window.  
  - **Add...**: Add a new item.  
  - **Disable or Delete**: Disable or delete the selected item.  
  - **Report...**: Display the available data as a report, which may be printed or saved as a PDF. See **Creating Reports**, page 4-10.  
  - **Filter**: Select or edit a filter. This determines which items are visible in the table. See **Using Filters**, page 4-12.  
  - **Columns...**: Configure which columns are visible, and the order in which they appear. See **Revising the Column Display**, page 4-14.  
  - **Group Edit**: Make changes to all items displayed in a module table. See **Using Group Edit**, page 4-14.  
  - **Quick Search**: Quickly search results in the main module window. See **Search**, page 4-15. |
| **5** Table | 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. |
| **6** Status Bar | Appears at the bottom of each module window. It is divided into 4 panes:  
  - **Pane 1**: 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.  
  - **Pane 2**: 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.  
  - **Pane 3**: Shows the number of items in the table.  
  - **Pane 4**: Displays the username of the logged-in operator, as well as the IP address or hostname they are logged in from. |
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 4-10
- Using Filters, page 4-12
- Revising the Column Display, page 4-14
- Using Group Edit, page 4-14
- Search, page 4-15

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 4-9).

Figure 4-9  Report Generation Window

The following items are shown in Figure 4-9:

<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 details in report</td>
<td>Depending on the type of objects in the report (event, badge, personnel record, etc.), there may be additional details that are available to be included in the report. If so, these will be available as checkboxes. For example, in a report of personnel records, checking the Badges option will 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 report will be grouped by the specified property, with a header for each group.</td>
</tr>
</tbody>
</table>
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 4-10 shows a report in PDF format from the **Events** module.

**Figure 4-10  Events Report in Report Viewer**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
<th>Device</th>
<th>Address</th>
<th>Personnel Record</th>
<th>Date</th>
<th>Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>Logical Driver: Started</td>
<td>Logical Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>Driver Manager: Started</td>
<td>Driver Manager</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>EDI Driver: Started</td>
<td>EDI Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>Logical Driver: Started</td>
<td>Logical Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>EDI Driver: Started</td>
<td>EDI Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>Gateway Driver: Started</td>
<td>Gateway Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>Driver Manager: Started</td>
<td>Driver Manager</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>Device record inserted</td>
<td>user-acc/ID</td>
<td>10.21.51.03</td>
<td></td>
<td>10.21.51.03</td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>School list inserted</td>
<td>user-acc/ID</td>
<td>10.21.51.03</td>
<td></td>
<td>10.21.51.03</td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>School list inserted</td>
<td>user-acc/ID</td>
<td>10.21.51.03</td>
<td></td>
<td>10.21.51.03</td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>School list inserted</td>
<td>user-acc/ID</td>
<td>10.21.51.03</td>
<td></td>
<td>10.21.51.03</td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>School list inserted</td>
<td>user-acc/ID</td>
<td>10.21.51.03</td>
<td></td>
<td>10.21.51.03</td>
<td></td>
</tr>
<tr>
<td>6/1/2009 05:59:18.600</td>
<td>School list inserted</td>
<td>user-acc/ID</td>
<td>10.21.51.03</td>
<td></td>
<td>10.21.51.03</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 4-12.
- **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 4-11.
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 4-12.

- 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 4-13.

- 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 4-13 Columns Window for the Event Manager](image)

**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 4-12 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 4-12 for more information.

**Step 3** In the Badges window, click the **Group Edit...** button to open the **Group Edit...** window, as shown in Figure 4-14.

**Figure 4-14  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.
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 4-2.

**Contents**

- Defining User Profiles for Desktop Application Access, page 5-2
- Creating User Login Accounts and Assigning Profiles, page 5-8
- Configuring LDAP User Authentication, page 5-12
- Viewing Audit Records for Changes to Usernames, page 5-16
- Managing Desktop Client Passwords, page 5-17
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.

If the profile enhancement feature is set in the system configuration settings (for more information, see Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- While creating user profiles, the application prompts the user to select hierarchical location for a specific user profile.
- When the profile enhancement feature is set, the administrator profile cannot be reused even by the cpamadmin, i.e. the cpamadmin cannot assign the administrator profile to any profile users.
- Assigning a location to a profile in the Hierarchical location field specifies the location of the profile. Other than the cpamadmin this specific profile can be accessed only by the users belonging to this location.

Note

You cannot modify the Administrators profile (read-only).

To create profiles, do the following:

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

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

**Step 3** Select any one of the following Profile template that closely matches the desired level of user access:

- Default— A basic set of privileges is set.
- Most Restrictive— No privileges are set.
- Least Restrictive— All privileges are set.

![Profiles Module Main Page](image)

![Profile Templates](image)
Step 4  Click OK to open the Add Profile screen,

Figure 5-3  Add Profile

Step 5  Enter the basic profile settings:
- Profile name
- Enabled
- Hierarchical Location
- Site(Auto-populated)

Step 6  Click the General tab to define the basic profile properties. Check the relevant check boxes next to each field to enable or disable the privilege, as described in Table 5-1.

Table 5-1  General Settings: Profile Module

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</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>Allow change password</td>
<td>Allows user to change password.</td>
</tr>
<tr>
<td>Allow edit preferences</td>
<td>Allows user to edit preferences.</td>
</tr>
</tbody>
</table>

Events/Alarms: Alarm Annotations (Ack., Clear, Comment)
Table 5-1  General Settings: Profile Module (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow annotations</td>
<td>Allows user to acknowledge, clear, and comment alarms. Click the <em>Filter</em> 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>

Events/Alarms: On new alarms

<table>
<thead>
<tr>
<th>Open Alarms Module</th>
<th>The <em>Alarms</em> module automatically opens with new system alarms. Click the <em>Filter</em> button to define the events that trigger the action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Manage Alarm window</td>
<td>The <em>Alarms</em> module automatically opens with new system alarms. Click the <em>Filter</em> button to define the events that trigger the action.</td>
</tr>
<tr>
<td>Open graphic map</td>
<td>The <em>Graphic Map</em> module automatically opens with new system alarms. Click the <em>Filter</em> 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 <em>Filter</em> 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 <em>Filter</em> button to define the events that trigger the action.</td>
</tr>
</tbody>
</table>

Help: defines access to the different help systems.

<table>
<thead>
<tr>
<th>Allow access to help documentation</th>
<th>Allows access to help documentation.</th>
</tr>
</thead>
<tbody>
<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. Adobe PDF viewer is required.</td>
</tr>
</tbody>
</table>

Assignment to Login

| Ignore hierarchical location restriction for devices matching filter | Allows the cpamadmin to populate the automation driver.                     |
Step 7  Click the Modules tab to define the modules accessible to the profile, as shown in Figure 5-5.
   a. Select a Cisco PAM module.
   b. Select Allow access to module to enable access to the module.
   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:
   – Create a profile with access to the Events module, as described in the previous steps.
   – Click Default Filter, as shown in Figure 5-5.
   – Select the Device tab.
   – Click Choose.
   – In the Choose Devices window, expand the Logical Driver device tree and select a door.

Figure 5-4  Choose Device

– Click OK to save the changes and close the windows.
Step 8  Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-6).
Figure 5-6 Profiles- Device Command Tab

- Expand or collapse the list of commands for a device.
- Highlight a command.
- 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 9** Click the **Data Types** tab to define the data available to the profile.
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 5-8) lists all the usernames in the system.

Figure 5-8 Logins Module Main Window

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 You cannot modify most of the properties of the cpamadmin login.

Step 3 Complete fields in the General tab, Table 5-3 describes the field properties.

Table 5-3 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>
</tbody>
</table>
Creating User Login Accounts and Assigning Profiles

Table 5-3 General Tab Fields. (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm password</td>
<td>Required. The value must be entered exactly as it was in the Password field.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The personnel record the login is assigned to. If the login is for an operator already entered in the Personnel module, click the Select... button. For more information on adding personnel to the system, see Chapter 9, “Configuring Personnel and Badges”.</td>
</tr>
<tr>
<td>Validity</td>
<td>Active or Inactive. 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 To create a location-restricted user:

a. Select the Profiles tab.

Figure 5-10 Profiles

b. Click Add. A new page opens.
c. Select an existing Profile from the drop-down list or click New to create a new profile.

d. Click Choose to associate the profile to a specific location in the location hierarchy.

e. Click Save and Close to save the changes and close the page.

**Step 5**
To verify the changes, log off and then log in with the new username and password. Verify whether the appropriate devices are populated for this location-restricted user.

**Additional Information**

- The Hierarchical location is a new field in the Login module. Assigning a location in this field specifies the location of the login. Other than the cpamadmin this particular login can be accessed only by the users belonging to this specific location.

- If the user does not associate a profile to login, the user will not be able to login into the system.

- When a login is associated with a profile without any hierarchical location, the user associated with that profile is not bound to any hierarchical location and can access devices from all locations.

- Existing logins that have the administrator profile will continue to have the privileges of the administrator. It is the responsibility of the cpamadmin to unassign the administrator profile from these logins if required.

**Note**
If the user does not select the fields that associate locations to logins (See Data Entry/Validation - Login, page 17-9), the user actions are not restricted to the locations. The configuration settings now reflects the Cisco Physical Access Manager 1.3 release.
Configuring LDAP User Authentication

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

- Configure the LDAP Server, page 5-12
- Create the LDAP User Account in Cisco PAM, page 5-14

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 5-13
- LDAP Example: sAMAccountName, page 5-14

**Step 3**
Enter the other LDAP server settings (Table 5-4):

<table>
<thead>
<tr>
<th><strong>Table 5-4</strong> LDAP System Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Enable LDAP</td>
</tr>
</tbody>
</table>
| **LDAP server URL** | URL of LDAP server, must begin with `ldap://`
| | Example: `ldap://192.168.1.1:389`
| | **Note** 389 is the port number. |
| **Principle suffix** | Appended to the username for authentication. See above. |
| **Principle prefix** | Prepended to the username for authentication. See above. |
Chapter 5  Configuring User Access for the Cisco PAM Desktop Client

Configuring LDAP User Authentication

Table 5-4  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.LdapCtxFactory</td>
</tr>
</tbody>
</table>

Step 4  Log out and log back in to the Cisco PAM application and restart the server to enable the changes (selectLogout from the Options menu).

LDAP Example: User Principal Name

In the example shown in Figure 5-12, the user principal name is cpsm.user@ad1.cpamlab. The Cisco PAM user login must be the same (cpsm.user).

Figure 5-12  User Principal LDAP Configuration Example
LDAP Example: sAMAccountName

In the example shown in Figure 5-13, the user login is the same as the samaccount name (cpmuser).

Figure 5-13  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.
Configuring LDAP User Authentication

**Figure 5-14 Login Window: LDAP Login Type**

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 5-12).

Step 4 Enter the username, password, and other settings for the LDAP login. See Creating User Login Accounts and Assigning Profiles, page 5-8.

*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 , page 5-1 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 5-15**.

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

**Figure 5-15**  Logins Audit Records Window

![Logins Audit Records Window](image)

**Table 5-5**  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</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 <strong>View</strong> to display</td>
</tr>
<tr>
<td></td>
<td>details for the device where the change was made, including the IP address of</td>
</tr>
<tr>
<td></td>
<td>the workstation device.</td>
</tr>
</tbody>
</table>
Managing Desktop Client Passwords

- Changing Your Password, page 5-17
- Changing Another User’s Password, page 5-17
- Managing the cpadmin Login and Password, page 5-18

Tip

To determine password expiration and strength requirements, see Password Policy Settings, page 17-11.

Changing Your Password

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

- **Step 1** From the Options menu, select **Change Password**.
- **Step 2** Enter your old password, and then enter a new password.
- **Step 3** Re-enter the new password to confirm the setting.
- **Step 4** Click **OK**.

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 5-8 for instructions.

Note

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

### Table 5-5 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 <strong>View</strong> to display and 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 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>
Managing the `cpamadmin` Login and Password

The `cpamadmin` login and password are created during the initial server setup, as described in Chapter 3, “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 affect the server login. See Changing or Recovering the Server Password, page 3-39 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 7, “Configuring Doors” for more information.

Contents

- Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 6-2
- Viewing Device and Door Configuration, page 6-3
- Viewing Device and Door Status, page 6-11
- Understanding Door Configurations and Templates, page 6-22
- Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 6-27
- Locating Serial Numbers, page 6-39
- Related Documentation, page 6-40
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 6-2
- Discovered Configuration, page 6-2

Note: See also Configuration Management in Provisioned vs. Discovered Configurations, page 7-23.

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 7-22.
- 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 7, “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 6-3
- Hardware Manager in Cisco PAM 1.4.1, page 6-5
- Viewing Doors and Devices by Location, page 6-6
  - Creating the Location Map, page 6-7
  - Filtering the Devices Displayed in the Locations View, page 6-8
  - Changing the Location of a Device or Door, page 6-8
  - Locations and Doors in Cisco PAM 1.4.1, page 6-9

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 6-1.

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 6-1. 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 6-1 Expanded Hardware Tree: Gateways and Related Devices

1. SanJose
2. localhost - Driver Manager [started]
3. localhost - Cisco VSM Camera Driver [started]
4. localhost - Access GW Driver [started]
5. /SanJose/gw_FHH11290012 - gw_FHH11290012 [Up]
   - /SanJose/gw_FHH11290012/m00 - m00 [Up]
   - /SanJose/gw_FHH11290012/m00/input01 - input01 [Up]
   - /SanJose/gw_FHH11290012/m00/input02 - input02 [Up]
   - /SanJose/gw_FHH11290012/m00/input03 - input03 [Up]
   - /SanJose/gw_FHH11290012/m00/output01 - output01 [Up]
   - /SanJose/gw_FHH11290012/m00/output02 - output02 [Up]
   - /SanJose/gw_FHH11290012/m00/output03 - output03 [Up]
   - /SanJose/gw_FHH11290012/m00/pwrfail01 - pwrfail01 [Up]
   - /SanJose/gw_FHH11290012/m00/rdr01 - rdr01 [Up]
   - /SanJose/gw_FHH11290012/m00/rdr01/reader - reader [unknown]
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 6-1 describes the icons and drivers shown in Figure 6-1:

### Table 6-1 Elements of the Device Tree

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Site</td>
</tr>
</tbody>
</table>
| 2    | Driver Manager | 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.  
**Note** If you disable the Driver Manager then all the drivers, doors, gateways and expansion modules are also disabled. If you enable the Driver Manager then you need to enable all driver modules, gateways, doors and expansion modules manually. |
| 3    | Access GW Driver | The Access GW Driver allows you to add Cisco Physical Access Gateway hardware modules to the system configuration, and supports the additional expansion modules (Reader, Input and Output) connected to a Gateway. The Access GW Driver also manages the events and alarms generated by devices, modules, and Gateways. The Access GW Driver is enabled by default.  
**Note** The Access Gateway Driver is an example of a Device Driver. Device Drivers enable software and hardware functionality. Additional Device Drivers include the Logical Driver, Automation Driver, EDI Driver, and Cisco VSM Driver. Each of these drivers enables the functionality for that feature, and provides basic configuration settings. There can only be one instance of each driver. |
| 4    | Gateway Controller | A Gateway controller is added for each Gateway device. The modules and devices configured on the Gateway are listed below the Gateway Controller and include the Gateway module, any expansion modules and the other devices attached to the module interfaces. Figure 6-1 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**. |
Chapter 6 Understanding Door Configuration

Viewing Device and Door Configuration

Table 6-1 Elements of the Device Tree

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Access Control Modules</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. <strong>Note</strong> 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 <em>Cisco Physical Access Gateway User Guide</em>. For instructions to configure modules, see Chapter 7, “Configuring Doors”.</td>
</tr>
<tr>
<td>6 Module Interface</td>
<td>Each module includes a set of interfaces for connecting door hardware and other devices. For descriptions of each module interface, see the <em>Cisco Physical Access Gateway User Guide</em>.</td>
</tr>
<tr>
<td>7 Devices</td>
<td>Devices include hardware such as card readers and locks. Device configurations are applied using pre-defined templates, or for a specific interface. See Chapter 7, “Configuring Doors” and Chapter 8, “Configuring Door and Device Templates”.</td>
</tr>
</tbody>
</table>

Hardware Manager in Cisco PAM 1.4.1

In Cisco PAM 1.4.1, if the profile enhancement feature is set in the system configuration settings (*Data Entry/Validation - Login*, page 17-9), the following changes are impacted in this module:

- The Hardware module displays the gateways, expansion modules and other devices based on the user’s hierarchical location only.
- The gateway and the associated doors must be in the same location of the location-restricted user for the seamless operation of the profile enhancement feature.
- The respective local host – Access Gateway Driver and local host – Logical Driver is populated only if the gateway or door is assigned to the location-restricted user’s location.
- A location-restricted user is restricted from creating doors.
- A location-restricted user does not have access to EDI and Historical Events drivers. To access these drivers the cpamadmin has to assign appropriate locations to these drivers and associate these locations to the location-restricted user.
- If the door is in one location and the (related) gateway is in another location (not of the location-restricted user), the gateway is still visible to the location-restricted user and the user can execute commands on this gateway.

**Note**

- The Export option fetches values of all unprivileged devices.
- A location-restricted user is allowed to create doors using the gateway template module.

**Note**

These features are applicable only when the profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version(1.3).
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 6-2. 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 6-2 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 6-7 for more information.

Figure 6-2  Hierarchical Location View of Hardware Devices

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>View Menu</td>
<td>5</td>
<td>Floor</td>
</tr>
<tr>
<td>2</td>
<td>Base</td>
<td>6</td>
<td>Area</td>
</tr>
<tr>
<td>3</td>
<td>Campus</td>
<td>7</td>
<td>Sub-Area</td>
</tr>
<tr>
<td>4</td>
<td>Building</td>
<td>8</td>
<td>Door</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 6-6.

Figure 6-3 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 7, “Configuring Doors”.

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

Figure 6-3 Locations & Doors: Main Window

Note: Hierarchical locations cannot be deleted. Door and Gateway names must be unique.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add Base button</td>
</tr>
<tr>
<td>2</td>
<td>Base</td>
</tr>
<tr>
<td>3</td>
<td>Campus</td>
</tr>
<tr>
<td>4</td>
<td>Building</td>
</tr>
<tr>
<td>5</td>
<td>Floor</td>
</tr>
<tr>
<td>6</td>
<td>Area</td>
</tr>
<tr>
<td>7</td>
<td>Sub-Area</td>
</tr>
<tr>
<td>8</td>
<td>Door</td>
</tr>
<tr>
<td>9</td>
<td>Devices</td>
</tr>
<tr>
<td>10</td>
<td>Unassigned</td>
</tr>
</tbody>
</table>

1. Unassigned includes Doors and Devices that are not assigned to a location.
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 6-4).

Figure 6-4 Locations & Doors: View Menu

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 6-4.
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 edit the configuration, as described in the following steps.
**Chapter 6  Understanding Door Configuration**

**Viewing Device and Door Configuration**

**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 6-5. You can also click the **Choose** button to select a location from the location map.

*Figure 6-5  Editing the Location for a Door or Device*

---

**Note**  
If the location constraint is enabled ([Data Entry/Validation - Login, page 17-9](#)), the location-restricted users are allowed to change location to any location/sub location only under their hierarchical location.

---

**Locations and Doors in Cisco PAM 1.4.1**

Location and Doors is the module where the location hierarchy is defined. The location hierarchy is defined as Base > Campus > Building > Floor > Area > Sub-Area.

After the profile enhancement feature is set in the system configuration settings ([Data Entry/Validation - Login, page 17-9](#)), the following changes are impacted in this module:
- A location-restricted user is able to view the entire hierarchy, but only the devices from the assigned location is populated for the location-restricted user.
The doors are displayed to users based on hierarchical location assigned to their user profiles. For example: if a user profile “campusadmin” is assigned to a location “BVVC”, the user can view doors and devices related to this location and its sub locations only. The action points for other locations (e.g.: BVDC) are grayed out. (see Figure 6-6)

Figure 6-6 Locations and Doors based on hierarchical location

The Unassigned node (locations) is only available for the cpamadmin and those logins who are not bound by hierarchical location.

The location-restricted user will not be able to execute device commands on devices from unprivileged nodes.

The extended status page shows device information of assigned devices for the location restricted user.

If cpamadmin wishes to drag and drop a gateway from one location to another, the cpamadmin should ensure that all interfaces and modules of the gateway are pointed to the new location. This action will prevent the location-restricted user of the old location from accessing the gateway.

These points are applicable only when the profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3).
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 6-11
- Viewing the Status for a Single Door, Device or Driver, page 6-12
- Monitoring Device Errors, page 6-15
- Viewing the Recent Events for a Device, Driver, or Location, page 6-16
- Generating a System Sanity Report, page 6-18

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 6-7.

**Figure 6-7    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 4-10 for more information.

**Step 3**

(Optional) Double-click an entry to view additional status details for the device, as shown in Figure 6-8.
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 6-9 shows an example for a Gateway device in the Hardware module.

Figure 6-9  Status and Extended Status in the Hardware Module

Step 4  Click the **Extended Status** tabs to view additional details for the device. The available tabs vary depending on the driver or device type.
Understanding Device Status Colors

The status of a Gateway, Door, or driver is signified by the color in the icon, and the color bar in the Status field, as shown in Figure 6-10.

**Figure 6-10   Device Status Colors**

<table>
<thead>
<tr>
<th>Color</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Green</td>
<td><img src="image" alt="Green Icon" /></td>
<td>The device or door is Up and the configuration is current.</td>
</tr>
<tr>
<td>2 Dark Green</td>
<td><img src="image" alt="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 7-22.</td>
</tr>
<tr>
<td>3 Red</td>
<td><img src="image" alt="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><img src="image" alt="Green, Dark Green, or Red Icon" /></td>
<td>The Status bar color also signifies the device or door status.</td>
</tr>
</tbody>
</table>
Monitoring Device Errors

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

**Step 1** Select **Error Monitoring** from the **Admin** menu.

The main window displays a summary of the errors for all devices, as shown in Figure 6-11. By default, the errors are sorted chronologically, most recent first.

**Figure 6-11  Error Monitoring: Main Window**

<table>
<thead>
<tr>
<th>Time</th>
<th>Level</th>
<th>Source</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMMAND</td>
<td>Error: Send...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMMAND</td>
<td>Required fields module type or serial number missing in module...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMMAND</td>
<td>Error: Send...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMMAND</td>
<td>Failed to receive response...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMMAND</td>
<td>Failed to receive response...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Lost Connection With The Remote Host...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Lost Connection With The Remote Host...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Lost Connection With The Remote Host...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
<tr>
<td>12/22/2009</td>
<td>Low</td>
<td>COMM</td>
<td>Error: In Closing A Channel: Exception: (bound closed before)...</td>
</tr>
</tbody>
</table>

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

See **Toolbar Features**, page 4-10 for more information.

**Step 3** (Optional) Double-click an entry to view additional status details for the device, as shown in Figure 6-12.
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 4-10**.

**Step 3** Right-click the device or driver, and select **View Recent Events** from the drop-down menu, as shown in Figure 6-13.

**Figure 6-13** View Recent Events Menu

**Step 4** Double-click an event to view event details, as shown in Figure 6-14.
**Figure 6-14  Recent Events**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
<th>Device</th>
<th>Address</th>
<th>Personnel</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2/2013 21:55:57.000</td>
<td>Received credential ready. Access Gw...</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2/2013 21:55:57.000</td>
<td>Send credential acknowledgment success. Access Gw...</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2/2013 21:56:04.000</td>
<td>Received credential info.     Access Gw...</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2/2013 21:56:04.000</td>
<td>Gateway disconnected          Access Gw...</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See Viewing Events, Alarms and Audit Trail Records, page 12-3 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 6-15 shows a sample report.

**Figure 6-15  System Sanity Report Example**

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.

Tip

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 13-18 and select **Sanity Report Action** in the Actions field.
- 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 6-16.

**Figure 6-16 System Sanity Report Command**

**Step 3** In the Sanity Report window, expand the menu for a topic, as shown in Figure 6-17.
In Figure 6-17, 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 6-17.

b. In the Report Generation Window (Figure 6-18), 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 6-15 on page 6-18.
Understanding Door Configurations and Templates

This section includes the following information:

- Overview, page 6-22
- Sequence for Configuring Templates and Doors, page 6-23
- Door Configurations and Templates, page 6-24
- Template Types, page 6-24
- Impact of Template Changes on Configured Doors and Devices, page 6-25
- Gateway Templates, page 6-25
- Understanding Door Templates, page 6-25
- Understanding Device Templates, page 6-26
- Understanding Credential Templates, page 6-26
- Understanding Reader LED Profiles, page 6-27

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 6-19 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 7-2**: 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 7-10**: 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**: define 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**: define 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.

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

- **Understanding Device Templates**: define typical settings for devices, such as locks and sensors. Device templates are used to help define door templates.
- **Understanding Credential Templates**: define 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**: define the LED states on a reader interface for a Gateway or Reader module.
Note

See also the “Configuring Badge Templates” section on page 9-28. Badge templates 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.

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 7-22 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 8-2

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 7-2.

Tip

To create an exact copy of a Gateway configuration for a single Gateway, see Cloning a Gateway Configuration, page 7-33.

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 7-2
- Adding Doors Using Door Templates, page 7-10

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.
Understanding Door Configurations and Templates

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 8, “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 7-22 for more information.

Related Documentation

Chapter 7, “Configuring Doors”.
Chapter 8, “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 8-21 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 8-25 for more information.

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

- Overview, page 6-27
- Understanding Door Modes, page 6-28
- Viewing the Door Mode Status, page 6-29
- Understanding the Default Door Mode, page 6-30
- Understanding the Scheduled Door Mode, page 6-30
- Understanding First Unlock Impact on the Scheduled Mode, page 6-31
- Manually Override the Door Mode Using Commands, page 6-31
- Impact of Gateway Reset on the Default and Scheduled Modes, page 6-33
- Understanding Door Schedule Entries in Cisco PAM 1.4.1, page 6-34
- Configuring the Default and Scheduled Door Modes, page 6-35

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 6-20.

**Figure 6-20  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 6-30.
- 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 6-30.
- **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 6-31

**Tip**
See Configuring the Default and Scheduled Door Modes, page 6-35 to create a schedule and apply it to a door. See also See Step 6, page 8-14 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 6-30.

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 6-30.

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 6-31.

### 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 6-21, 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 6-21 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 6-31 and Impact of Gateway Reset on the Default and Scheduled Modes, page 6-33.
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 Configuring the Default and Scheduled Door Modes, page 6-35 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 6-31 to avoid this situation.

To override a door schedule, see Manually Override the Door Mode Using Commands, page 6-31.
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 Configuring the Default and Scheduled Door Modes, page 6-35 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 6-31
- Impact of Gateway Reset on the Default and Scheduled Modes, page 6-33

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 6-22 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 6-23 on page 6-33.
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 6-33. Resetting the Gateway has the same affect as the **Reset Door Mode** command.

For example, in Figure 6-23 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 6-31).
- 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 he guard is absent.

**Understanding Door Schedule Entries in Cisco PAM 1.4.1**

The Door Schedule is evaluated to determine the state of a given door at any point of time. A door can be in any one of the four states:

- Door Open
- Close
- Lock and
- Secure

The current state of a door is determined by two door properties namely the Default mode and the Scheduled mode. The default mode and the scheduled mode are configured for each door using the CPAM. Both default mode and scheduled mode can be configured to any one of the four door states. When you set the current state of door to the default mode, it automatically carries a ‘Deny access’ command and in schedule mode it carries a ‘Permit access’ command.

At any given time, the current door state (i.e. when the door is idle and not being used by any user) is determined by its door schedule which in turn depends on the default mode or the scheduled mode. The door schedule consists of one or more schedule entries. Every 45 seconds, for each door, the gateway runs through each door’s schedule entries to determine the current door state of each door.

The current door state is determined as follows:

- If the current time is outside the time range defined by its door schedule entries, then the current state of the door is set to default mode.
- If the current time matches or falls under any one of the door schedule entry’s time ranges, then the door’s current state is set to either scheduled mode or default mode. If the schedule entry’s action is scheduled mode, then current state of the door is set to scheduled mode and if the schedule entry’s action is default mode, then the current door state is set to default mode.
- When the current time matches more than one schedule entry of a given door schedule then the action taken is determined as follows:
  - If there is any schedule entry set to default mode, then this action takes over the schedule entries that are set to schedule mode.

From Cisco PAM 1.4.1 release, when the current time matches more than one schedule entry of a given door schedule then the action taken is determined as follows:

- The order of the door schedule entries is taken into account and the first matching schedule entry’s action is taken.

For example, If the first matching schedule entry’s action is set to default mode, the current door state is set to default mode. If the first matching schedule entry’s action is set to scheduled mode, the current door state is set to scheduled mode. If there are no matching entries, the current door state is set to default mode.
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 be 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 11-8.
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.

The schedule is not active until you apply it to a door, as described in the following steps.
Chapter 6  Understanding Door Configuration

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

To do this

Step 2  Open the door configuration Properties window.

a.  Select Hardware or Locations and Doors from the Doors menu.
b.  Double click an existing door icon to open the door edit window.
c.  Select Properties.

![Door Configuration Properties Window](image)

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 8-10.

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.

![Default Mode Setting](image)

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.
To do this

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.
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 Configuring Cisco PAM on Virtual Machine (VM), page 3-16.
- 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 3-2, 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 6-24.

Step 3  Refer to the entry for Serial Number.

Figure 6-24  Cisco PAM Appliance Serial Number
Related Documentation

- Chapter 7, “Configuring Doors”
- Chapter 8, “Configuring Door and Device Templates”.
- To install Gateways and expansion modules, see *Cisco Physical Access Gateway User Guide*. 
CHAPTER 7

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 6-2 for more information.

Contents

- Configuring Doors, page 7-2
  - Adding Gateways and Doors Using Templates, page 7-2
  - Adding Doors Using Door Templates, page 7-10
- Modifying Door Configurations, page 7-18
- Applying Configuration Changes, page 7-22
- Disabling or Deleting a Device or Door, page 7-25
- Cloning a Gateway Configuration, page 7-33
- Configuring Device Groups, page 7-34
- Replacing a Gateway or Expansion Module, page 7-38
- Changing Gateway Passwords, page 7-38
- Device and Driver Commands, page 7-41
- Door Modes, page 7-46
- Door Commands, page 7-46
Configuring Doors

This section includes the following information.

- Adding Gateways and Doors Using Templates, page 7-2
- Adding Doors Using Door Templates, page 7-10

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.

To do this

Step 1

Create the locations for door and devices.

a. Select Locations & Doors from the Doors menu.

b. To create a new site, click Add Base.

c. To create a sub-location, right-click a location and select New [Element].

d. To change the properties for an element, right-click a location and select Edit.

Tip

You can create any combination of location elements. Door configurations can be assigned to any level of the hierarchical tree.
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 6-3 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 6-2.
To do this

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 6-22 and Chapter 8, “Configuring Door and Device Templates”.
To do this

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 6-39.

c. **Location**: the assigned location of the module. See Viewing Doors and Devices by Location, page 6-6.

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

d. Click **Next**.
To do this

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.
To do this

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 7-10.

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 6-6).
d. Click **Update**.
e. Repeat these steps for each available door.
f. Click **Finish** to create the door configuration(s).
To do this

Step 8  (Optional). 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 6, “Understanding Door Configuration”
- Door Configuration Properties, page 8-29
- Device Configuration Properties, page 8-31

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

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 7-22

Step 10  *(Optional)* Continue to **Adding Doors Using Door Templates**, page 7-10

**Note**  In Cisco PAM 1.4.1, you can view the gateways, modules, devices and doors assigned to your location only. For more information, see *Locations and Doors in Cisco PAM 1.4.1*, page 6-9.

**Related Documentation**

For more information, see the following:

- Chapter 6, “Understanding Door Configuration”
- Chapter 8, “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.

**To do this**

**Step 1** Verify that the Gateway for the door configuration exists in the Hardware module.

To do this

**Step 1** Verify that the Gateway for the door configuration exists in the Hardware module.

To do this

**Step 1** 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:

- Adding Doors Using Door Templates, page 7-10
- Creating Custom Gateway Configurations and Templates, page 8-2

**Note** See also Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 6-2.

**Step 2** Create a new door:

a. Select Locations & Doors from the Doors menu.

b. Right-click a location and select New Door.

**Note** If the location does not exist, refer to Creating the Location Map, page 6-7 for more information.

**Tip** You can also create a door in the Hardware module. Right click on the Logical Driver and select New Door.
To do this

Step 3

Enter the General settings:

- **Door name**: enter a descriptive name for the door configuration.
- **Door Template**: select the door template that contains the correct set of door devices. See Configuring Door Templates, page 8-10 for more information.
- **Gateway**: select the Gateway used for the door configuration. The devices in the door template are assigned to the Gateway interfaces.

Step 4

Select a location for the door.

a. Select the Location sub-menu.

- Click Choose to select the location from a hierarchical map (see example screen).

**Note** If you create a new door in a specific location in the Locations & Doors module, the door location takes the location of the hierarchy as a default location.

**Note** If you create a new door using the location assigned gateway in the Hardware module the door location takes the location of the gateway as a default location.

- Click Clear to remove the setting. The door will appear in the Unassigned category.
Step 5  
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.

a. Select the **Associate Devices** sub-menu.

![Associate Devices Sub-menu](image)

b. Highlight a device (such as Reader) and click **Associate Device**.

c. In the **Select Device** window, click the **New** button.

![Select Device Window](image)

d. In the **New Device** window, select a module and module interface for the device.

![New Device Window](image)

**Note**  
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.

e. Click **OK**.
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 8-31 for more information.

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.
To do this

**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.

**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 6, “Understanding Door Configuration”
- Door Configuration Properties, page 8-29
To do this

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.

![Usage Profiles sub-menu](image)

**Note**  
If there are two doors created from a gateway, the reader LED profile changes does not apply to the second door.

See **Configuring Reader LED Profiles, page 8-25** for more information.
To do this

Step 11  (Optional) Modify the Facility Codes for the credential templates used in the door configuration:

a. Click the **Facility Code Information** sub-menu.
b. Uncheck the Default box to activate the configuration fields.
c. Click **Add** to add a credential template to the list.
d. Select a credential template from the drop-down menu.
e. Enter the Facility Codes. Separate codes with a comma (,).
f. Click **Save**.

To Edit a credential template:

a. Highlight the template in the Credential Template list box.
b. Click **Edit**.
c. Select a credential template from the drop-down menu.
d. Enter the Facility Codes. Separate codes with a comma (,).

To delete a credential template:

a. Highlight the template in the Credential Template list box.
b. Click **Delete**.

**Note**  By default a door can have 26BitWeigandCT credential with 456,123 facility code.

See Configuring Credential Templates, page 8-21 for more information.
To do this

**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.
To do this

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 7-22

Related Documentation

- Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 6-2
- Adding Gateways and Doors Using Templates, page 7-2
- Creating Custom Gateway Configurations and Templates, page 8-2

### 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 7-18
- Modifying Devices in the Hardware Device View, page 7-18
- Modifying Devices in Hardware Location View, page 7-19
- Modifying Devices in the Locations & Doors Module, page 7-20

### Modifying Door and Device Templates

For instructions to modify templates, see Chapter 8, “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.
Chapter 7  Configuring Doors

Modifying Door Configurations

Step 2  Expand the hardware tree, right-click on the device name, and select Edit, as shown in Figure 7-1. 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 8-29 and Device Configuration Properties, page 8-31.

Step 4  Download the configuration changes to the Gateway. Changes do not take effect until downloaded. See Applying Configuration Changes, page 7-22.

Figure 7-1  Edit Menu for a Device in the Hardware Device View

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 7-2. 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 7-22.
**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 6-7.

---

**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 7-3.

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

---

**Figure 7-3**
**Edit Menu for a Door in the Hardware Location View**

---

**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 7-22.
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 7-22
- Configuration Management in Provisioned vs. Discovered Configurations, page 7-23

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 6-14.
Applying Configuration Changes in the Locations & Doors Module

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

**Specific Gateway**

a. Select **Gateway Controllers** from the View menu to display the Gateways.

b. Right-click a Gateway icon and select **Apply Configuration Changes** to download the configuration for a single device.

or

**Multiple Gateways**

a. Right-click a location icon.

b. 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 6-14.

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 6-2 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 7-25
- Deleting Devices and Doors, page 7-26
- Enabling a Device or Door, page 7-29

**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 7-4).

**Figure 7-4**

Disabling a Device Using the Hardware Module

![Disabling a Device Using the Hardware Module](image)
Disabling or Deleting a Device or Door

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 7-5. Select the devices to be disabled, or check the box for Select All, and then click Yes.

Figure 7-5 Confirmation Warning When Disabling a Door Configuration

Step 3 Download the configuration changes to the Gateway. Changes do not take effect until downloaded. See Applying Configuration Changes, page 7-22.

Step 4 (Optional) To delete a device, Gateway or door configuration, see Deleting Devices and Doors, page 7-26.

Tip 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 7-27
- Deleting a Device, page 7-28
- Deleting a Gateway Controller, page 7-28
Enabling the Delete Options

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

**Step 2** Select the **Miscellaneous** sub-menu, as shown in **Figure 7-6**

**Figure 7-6  Device Delete Options in The Admin Module: System Configuration**

**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** Log out and log back in to the Cisco PAM application to enable the changes (select **Logout** from the Options menu). The **Delete** menu does not appear in Cisco PAM until you log out and log back in.
# Deleting a Device

To delete a device, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable the Delete functions, as described in <a href="#">Enabling the Delete Options, page 7-27</a>.</td>
</tr>
<tr>
<td>2</td>
<td>Disable the device, as described in <a href="#">Disabling a Device or Door, page 7-25</a>.</td>
</tr>
<tr>
<td>3</td>
<td>Select <strong>All Devices</strong> from the <strong>Filter</strong> menu to display the disabled device(s).</td>
</tr>
<tr>
<td>4</td>
<td>Right-click the device and select <strong>Delete</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Select <strong>Yes</strong> to confirm.</td>
</tr>
<tr>
<td>6</td>
<td>Download the changes to the Gateway, as described in <a href="#">Applying Configuration Changes, page 7-22</a>.</td>
</tr>
</tbody>
</table>

# Deleting a Gateway Controller

To delete a Gateway Controller, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable the Delete functions, as described in <a href="#">Enabling the Delete Options, page 7-27</a>.</td>
</tr>
<tr>
<td>2</td>
<td>Disable all devices in all doors associated with the Controller, as described in <a href="#">Disabling a Device or Door, page 7-25</a>.</td>
</tr>
<tr>
<td>3</td>
<td>Select <strong>All Devices</strong> from the <strong>Filter</strong> menu to display the disabled device(s).</td>
</tr>
<tr>
<td>4</td>
<td>Delete the Gateway Controller by right-clicking the Controller and selecting <strong>Delete</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Select <strong>Yes</strong> to confirm.</td>
</tr>
<tr>
<td>6</td>
<td>Download the changes to the Gateway, as described in <a href="#">Applying Configuration Changes, page 7-22</a>.</td>
</tr>
</tbody>
</table>
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:

**To do this**

**Step 1** Disable a device:

a. Right-click the device and select **Disable**. A confirmation message appears.

b. Click **Yes** to disable the device. The door is also disabled.
To do this

Step 2  Re-enable the door.

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

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

b. Right-click on the door and select **Edit** to open the edit window.

c. Select the **Associate Devices** sub-menu, as shown in the example to the right.

d. Highlight a device (such as Reader) and click **Associate Device**.

e. In the **Select Device** window, click the **New** button.

f. In the **New Device** window, select a module and module interface for the device.

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

g. Click **OK**
To do this

Step 3
Accept or modify the device settings.

Click **Save and Close** to save the configuration.

![Image of device settings](image1)

Step 4
Select the interface for the device in the **Select Device** window:

- 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.

- Click **OK** to save the change and complete the device association.

![Image of Select Device window](image2)
To do this

**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.

**Step 6**
Re-enable the door.

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

Right-click the door name, and select **Enable**.
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 affect 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 7-2 for more information.

To do this

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.
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 12-29), Global IO, Quick Launch, Graphical Map and Access Policies (Configuring Access Policies, page 11-2).

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.

Device Groups in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings (see Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The device groups present in the users hierarchical location and sub locations alone can be added. Only those device groups of locations to which the user profile is associated with is displayed for selection. For example: If a user assigned location is ‘BVVC’ only those device groups under BVVC is displayed. See (Figure 7-8)

To create a template from a Gateway configuration, see Creating Custom Gateway Configurations and Templates, page 8-2.
While creating device groups, a location-restricted user can view devices up to the root of their respective location hierarchy. However only those devices that are within their assigned location are available for selection (to form a device group).

The location-restricted user can reuse device groups present up to their root level provided there is at least one device in those groups that belong to their assigned location, this behavior is specific to global I/O and graphical editor.

**Note**

These points are applicable only when the profile enhancement feature is set in the System Configuration of the CPAM. Otherwise the CPAM appliance retains its behavior as in the previous version (1.3).

To configure device groups, do the following:

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

The Device Groups - Cisco Physical Access Manager window opens, as shown in Figure 7-9.
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 7-10), enter a Name for the device group.

Figure 7-10  Device Group Detail Window

Step 4  From the Type drop-down list select any one of the following devices types:
- Door
- Gateway
- Module
- Reader

When selected, the Group Members field displays the devices for that device type. Site is auto-populated.

Step 5  Select the Hierarchical location.

Step 6  Select the devices to include in the 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.

Step 7  Click Save and Close to save the changes. The new door group appears in the main window (Figure 7-9).
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.

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

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

**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 7-11 and Figure 7-12 for examples to change the Gateway passwords.

**Figure 7-11  Reset Gateway Password**

![Figure 7-11 Reset Gateway Password](image)

**Figure 7-12  Reset Gateway Password**

![Figure 7-12 Reset Gateway Password](image)

**Step 3**  (Optional) In the Reset Gateway Password window (Figure 7-13 on page 7-40), 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 7-13).
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 7-11 on page 7-39).

- 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 7-11 on page 7-39).

† **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

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 7-41
- Gateway Controller Commands, page 7-42
- Reader Module Commands, page 7-44
- Input and Output Module Commands, page 7-44
- Logical Driver Commands, page 7-45

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 7-22.</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 9-11.</td>
</tr>
<tr>
<td>Reset Gateway Password</td>
<td>Resets the password on all configured Gateways. See Changing Gateway Passwords, page 7-38.</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 C-12.</td>
</tr>
<tr>
<td>Set NTP Server</td>
<td>Sets the Network Time Protocol (NTP) server for one or more Gateways. See Changing the NTP Setting for Multiple Gateway Modules, page C-7.</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 6-16.</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 7-25. Disabled Devices can be re-enabled.</td>
</tr>
</tbody>
</table>
Device and Driver Commands

Table 7-1  Access GW Driver Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Permanently removes the Gateways and attached devices from the configuration. See Disabling or Deleting a Device or Door, page 7-25.</td>
</tr>
<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 6-11.</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 12-44.</td>
</tr>
</tbody>
</table>

Gateway Controller Commands

Table 7-2  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></td>
<td><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. For more information, see Applying Configuration Changes, page 7-22.</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>
<tr>
<td>File Manager</td>
<td>Provides info of various files available on the Gateway:</td>
</tr>
<tr>
<td></td>
<td>• Images: Set of firmware images available on the Gateway including status. See Upgrading Gateway Firmware Images Using Cisco PAM, page C-12 for more info.</td>
</tr>
<tr>
<td></td>
<td>• Core Files: Core files for any core dumps that occurred on the Gateway.</td>
</tr>
<tr>
<td></td>
<td>• Log File: List of debug log files.</td>
</tr>
<tr>
<td></td>
<td>• Technical Summary: Technical data to assist in debugging issues.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Each screen also provides options to download or upload the files.</td>
</tr>
<tr>
<td>Save As Gateway Template</td>
<td>Saves the Gateway configuration as a template that can be used to configure additional devices. See Creating Custom Gateway Configurations and Templates, page 8-2 and Gateway Templates, page 6-25.</td>
</tr>
<tr>
<td>Clone Gateway</td>
<td>Creates an exact duplicate of a Gateway configuration. See Cloning a Gateway Configuration, page 7-33.</td>
</tr>
</tbody>
</table>
## Table 7-2  Gateway Controller Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Gateway</td>
<td>Performs a soft reset of the Gateway. See the <em>Cisco Physical Access Gateway User Guide</em>.</td>
</tr>
<tr>
<td>Set Gateway Address</td>
<td>Replaces the Gateway Network configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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 cannot 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 Gateway Network Address 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 a 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 7-38.</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 7-38.</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 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 6-16.</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 7-25. 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 7-25.</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 12-44.</td>
</tr>
</tbody>
</table>


Reader 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>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 6-16.</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 7-38.</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 7-25. 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 7-25.</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 12-44.</td>
</tr>
</tbody>
</table>

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 7-38.</td>
</tr>
</tbody>
</table>
Table 7-4  Input and Output Module Commands (continued)

<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 6-16.</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 referenced door configurations. See Disabling or Deleting a Device or Door, page 7-25. 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 7-25.</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 12-44.</td>
</tr>
</tbody>
</table>

Logical Driver Commands

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

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 6-16.</td>
</tr>
<tr>
<td>New Door</td>
<td>Creates a new door configuration. See Configuring Doors, page 7-2.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit window to revise the driver properties.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables the device and all attached devices. See Disabling or Deleting a Device or Door, page 7-25. 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 7-25.</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 12-44.</td>
</tr>
</tbody>
</table>

Note  If you run any gateway commands or door commands in the Locations and Doors module, all the related events are populated as Logical Driver commands.
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 the 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 7-46 for more information.

Tip

For more information, see **Understanding Door Modes, Door Schedules, and the First Unlock Feature**, page 6-27.

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 <strong>Door Configuration Properties</strong>, page 8-29 for more information.</td>
</tr>
<tr>
<td>Update State</td>
<td>Updates the door state displayed in the hardware tree.</td>
</tr>
</tbody>
</table>
Table 7-5  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>
### 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 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:</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>• Successfully execute 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></td>
<td><strong>Note</strong> Badge access is still allowed, or you can manually grant access 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 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 is denied.</td>
</tr>
</tbody>
</table>

Activate/deactivate access levels for multiple doors:

- Select **Locations & Doors** from the Doors menu, right click a location and select **Deactivate Access Levels**. All doors in that location are affected.

Activate/deactivate access levels for a single door:

- Right-click a door icon in the **Locations & Doors** module and select the command.
- In the **Hardware** module, expand the Logical Driver device tree, right-click a door and select the command.

To reactive the access levels, select **Activate Access Levels**.
CHAPTER 8

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 6, “Understanding Door Configuration” for more information.

Contents

- Creating Custom Gateway Configurations and Templates, page 8-2
- Configuring Door Templates, page 8-10
- Configuring Device Templates, page 8-18
- Configuring Credential Templates, page 8-21
- Configuring Reader LED Profiles, page 8-25
- Duplicating Templates, page 8-27
- Door Configuration Properties, page 8-29
- Device Configuration Properties, page 8-31
- Debounce Timer, page 8-36
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).

![Gateway Templates Main Window](image)

Figure 8-1 shows the main window. The default Gateway templates cannot be changed. Only user-created templates can be modified.

**Figure 8-1** Gateway Templates Main Window
Creating Custom Gateway Configurations and Templates

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.

To do this

**Step 1**
Open the Hardware module in the Device view.

a. Select **Hardware** from the **Doors** menu.

b. Select **Device** from the **View** menu.

Tip   See also Viewing Doors and Devices in the Hardware View, page 6-3.

**Step 2**
Add a Gateway module.

a. Right-click the **Access GW Driver**.

b. Select **New Gateway Controller**.

Tip   See also Viewing Doors and Devices in the Hardware View, page 6-3.
To do this

Step 3  Select No to configure the Gateway without using a template.

Click Next to continue.
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 6-39.

c. **Location**: the assigned location of the module. See Creating the Location Map, page 6-7.

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 6-39.

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

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

d. Click Add. The expansion module is added to the list.

e. Repeat these steps for each additional module.

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

Tip To modify the module list, select a module and click Edit or Remove.
To do this

**Step 6**

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

**Note** Devices are usually added when configuring a door. See Chapter 7, “Configuring Doors”.

1. Expand the hardware tree to view the Gateway or expansion module interfaces.
2. Right-click an interface and select the device for the interface. For example: **New REX**.
3. 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.
   - Enter the **Debounce Timer (ms)** value.
4. Click **Save and Close**.
5. Repeat these steps for each device connected to the Gateway.
To do this

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 7-22.

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 8-1).

- Select *Clone Gateway* to create an exact copy of a Gateway configuration for a single Gateway. See *Cloning a Gateway Configuration*, page 7-33.
Step 9

(Optional) Add the door configuration that use the ports on the Gateway. See Configuring Doors, page 7-2. To do this
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 6, “Understanding Door Configuration” for more information.

Figure 8-2 Door Templates Main Window

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

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

**To do this**

**Step 1** Select Door Templates from the Doors menu, in the Templates sub-menu.
To do this

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.
To do this

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 8-18 for instructions to create and modify the available templates.

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

f. Click Next to continue.
To do this

**Step 5**

Define the door lock properties.

a. Select the **Properties** tab.

b. **Relock 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 **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.

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

![Door Template Configuration](image)

**Usage Notes**

By default, when a door access request is granted, the door remains unlocked until the **Relock 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 **Relock 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 **Relock 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 **Relock interval time** is elapsed for the most recent request, set **Door lock on close** to **No**.
### Configuring Door Templates

#### Step 6

**To do this**

Define the door mode and schedule:

- **Select the Properties tab.**

- **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.

- **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 11-8 to add or modify the available door schedules.

- **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*.

- **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 6-27 for more information.
To do this

**Step 7**

Enter the additional door **Properties**:

- **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 (APB)**: the action to be taken by gateway in case it cannot reach Cisco PAM. See the “Using Local (Gateway) Credentials if Network Communication is Lost” section on page 11-22.

- **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.
To do this

**Step 8** Enter the door **Usage Profiles** used by the reader device(s). These profiles define what LED or buzzer action occurs under the following events:

- **Grant access**: the LED display when normal access is granted.
- **Grant access ADA**: the LED display when access is granted for an ADA enabled badge.
- **Deny access**: the LED display when access is denied.
- **Grant facility code**: the LED display when access is granted based on a Facility Code.
- **Mode open**: the LED display when the door mode is *Open*.
- **Mode close**: the LED display when the door mode is *Close*.
- **Mode lock**: the LED display when the door mode is *Lock*.

**Tip** See Configuring Reader LED and Buzzer Profiles, page 8-26 for more information
To do this

Step 9
Enter the **Facility Code Info**:  
Click **Add** to add a credential template and facility code.

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 **Server Unreachable** and **Server Access Timeout** if necessary.

Step 10
Enter the **Duress Specifications**.  
Click **Add** to add an alarm type and code.

Step 11
Click **Save and Close** to save the template and close the window.
Configuring Device Templates

Device templates are pre-defined configurations for the device types used 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 8-3 Device Templates Main Window

For more information, see Chapter 6, “Understanding Door Configuration” and Chapter 7, “Configuring Doors”.

Creating a Device Template

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

To do this

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

Step 2  
Select Add..., and then select Device Template Wizard.

You can also do the following:

- 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.
- Right-click on a template name to access the Edit and Delete functions.
**To do this**

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

![Create New Device Template](image)

**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 8-31** 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.
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 8-21
- Credential Templates Settings Summary, page 8-22
- Creating a Credential Template, page 8-23

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 8-22 for a configuration overview.

Existing templates cannot be modified. See Creating a Credential Template, page 8-23 for instructions to create a new template.

Figure 8-4  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.

To do this

**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.
Step 4  Enter the **Primary Data** and **Secondary Data** settings for the template.

See Credential Templates Settings Summary, page 8-22 for more information.

**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.

Step 5  Click **Save and Close** to save the template and close the window.
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 8-5 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.

To do this

Step 1  
Select Reader LED Profiles from the Doors menu, in the Templates sub-menu.

Step 2  
Create or edit the profile:

a. Click Add, or select an existing profile and click Edit.

Tip  
You can also right-click on an item to access the Add, Edit and Delete functions.

b. Enter the profile Name.

c. Enter the profile settings:

- **Command**: defines the state of the output when the profile is invoked (Output On or Output Off).
- **Duration**: specifies how long the output is turned on and off.
- **Repeat**: specifies the number of times the output is turned on and off.
- **On time (ms)** and **Off time (ms)**: specifies how long the output is ON or OFF, in milliseconds.

Step 3  
Click Save and Close to save the profile and close the window.
Duplicating Templates

- Duplicating Door, Device, and Credential Templates, page 8-27
- Duplicating Gateway Templates, page 8-28

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 8-6.

**Step 4** Enter a **New Name** for the template and click **OK**, as shown in Figure 8-7.

**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 8-10
- Configuring Device Templates, page 8-18
Duplicating Gateway Templates

- To create a template from a Gateway configuration, see Creating Custom Gateway Configurations and Templates, page 8-2.
- To create a clone of a Gateway configuration for one-time use, see Cloning a Gateway Configuration, page 7-33. 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 8-1 Door Properties

<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 11-8 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”. Note 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>

See Understanding Door Modes, Door Schedules, and the First Unlock Feature for more information.
### 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 (APB)
The action is taken by Gateway in case it cannot reach Cisco PAM. See the “Using Local (Gateway) Credentials if Network Communication is Lost” section on page 11-22.

### 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.

### Generic reader
Lists the generic readers associated to the door.

### Multifactor authentication timer (sec)
The number of seconds for the multifactor authentication to take place. The default time is 10 seconds.

---

**Table 8-1 Door Properties**

<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></td>
<td>- <strong>Open</strong>: the door is held open and the lock is in unlocked state.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Close</strong>: the door is physically closed and the lock is in unlocked state.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Lock</strong>: the door is physically closed and the lock is in Locked state.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Secure</strong>: the door is locked and the deadbolt is applied.</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 <strong>Server access timeout</strong>.</td>
</tr>
<tr>
<td>If server unreachable (APB)</td>
<td>The action is taken by Gateway in case it cannot reach Cisco PAM. See the “Using Local (Gateway) Credentials if Network Communication is Lost” section on page 11-22.</td>
</tr>
<tr>
<td>Server access timeout (sec)</td>
<td>The number of seconds before an action is taken based on <strong>Access decision on timeout</strong>.</td>
</tr>
<tr>
<td>ADA timespec multiplier</td>
<td>The multiplier used on <strong>Relock interval time</strong> if an ADA access occurs.</td>
</tr>
<tr>
<td>Door swing activation delay (sec)</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>
<tr>
<td>Generic reader</td>
<td>Lists the generic readers associated to the door.</td>
</tr>
<tr>
<td>Multifactor authentication timer (sec)</td>
<td>The number of seconds for the multifactor authentication to take place. The default time is 10 seconds.</td>
</tr>
</tbody>
</table>
Device Configuration Properties

This section summarizes the properties that can be configured on door devices.

- Understanding Normally Open (NO) vs. Normally Closed Devices, page 8-31
- Understanding Supervised vs. Unsupervised Input Devices, page 8-31
- Device Configuration Properties Summary, page 8-32

Understanding Normally Open (NO) vs. Normally Closed Devices

- 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.

Understanding Supervised vs. Unsupervised Input Devices

Door input devices can be supervised or unsupervised

- Unsupervised input devices have two states: active or inactive.
- Supervised input devices have four states: active, inactive, short, and open.

Unsupervised inputs have limited functionality. If a wire is cut or shorted between the input module and a normally open device. The server cannot determine the change and the device would remains in inactive state even when the switch is closed.

To make the input device supervised, use two 1K resistors in the circuit (Figure 8-8).

- In the inactive state, the circuit measures 2000 ohms.
- In the active state, the circuit measures 1000 ohms.
- In the short state the circuit measures 0 ohms
- In the open state the circuit measures infinite ohms.

Once the input device is supervised, CPAM can determine if a wire is cut or shorted.

Figure 8-8  Example of a Supervised Door Sensor
## Device Configuration Properties Summary

Table 8-2 describes device settings for common device types.

### Table 8-2  Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deadbolt</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>Door Swing</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>Trigger Time (sec)</strong>: The number of seconds that power is applied to operate the door swing.</td>
</tr>
<tr>
<td><strong>Door Sensor</strong></td>
<td>• <strong>Sensor input</strong>: 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>• <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>Duress Sensor</strong></td>
<td>• <strong>Sensor input</strong>: 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>• <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>Fire Sensor</strong></td>
<td>• <strong>Sensor input</strong>: 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>• <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 Input</strong></td>
<td>• <strong>Normal state</strong>: The type of device contact:</td>
</tr>
<tr>
<td><strong>Device</strong></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>• <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 8-2 Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic Output Device</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 <strong>Timed Activate Relay</strong> is invoked, this property defines the number of milliseconds the generic output is activated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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>Glass-Break</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>Lock</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>Note</strong> 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>Motion Sensor</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>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>
</tbody>
</table>
### Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Fail</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>Power fail state</strong>: The default state of the device.</td>
</tr>
<tr>
<td>REX</td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rex 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>Device state</strong>: The default state of the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supervised</strong>: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Push button</strong>: Indicates a push button type of REX.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Push button type</strong>: Indicates the kind of push button REX.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ADA enabled</strong>: 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>
## Table 8-2 Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
</table>
| Reader   | • Reader type:  
|          |   – Card Reader  
|          |   – Card and Keypad Reader  
|          |   – Keypad Reader  
|          | • Protocol: Only Wiegand is supported.  
|          | • Data format: Only Standard Wiegand is supported.  
|          | • Credential template: Set of credential templates to be used to validate the cards presented to this reader.  
|          | • Category: Entry or Exit reader.  
|          | • Reader connector: Type of connector Ten Wire/Five Wire  
|          | • 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.  
|          | • Credential order: If the reader is a Card and Keypad Reader this field specifies the credentials order.  
|          | • 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.  
|          | • 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.  
|          | • 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.  
|          | • Number of pin keys: If the reader has a keypad, this field specifies the length of the pin to expect.  
|          | • 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.  
| Tamper   | • Tamper input: 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.  
|          | • Tamper state: The default state of the device. |
Debounce Timer

Input devices like a door sensor can generate multiple spurious events (such as Door Forced Open events) within a short span of time under the following conditions:

- If the sensors are too sensitive
- Have faulty wiring
- Are incorrectly installed
- Are subject to vibrations

To prevent spurious events, a debounce timer can be used to mask events within a specified time interval. When the debounce timer is applied, a transition event is considered valid only if it does not change for at least debounce timer interval.

**Note**
The debounce timer applies only to events generated by input devices (sensors) such as INPUT_LOW/INPUT_HIGH. These events are not propagated to the Cisco PAM server, so there is no way of validating the debounce timer using Events Monitoring from the Cisco PAM server. Debounce timer validations can only be performed using the debugging logs on the Gateway module for the sensor. For example, see the bp_msg log.

The debounce timer is disabled by default (the default timer is zero seconds, meaning there is no event suppression). To enable the timer, configure each input interface with a maximum value of 500 milliseconds.

To determine the correct timer value, observe the events to ensure that valid events are not being suppressed. Valid events can be missed if the debounce timer value is too high. If valid events are suppressed, reduce the timer value.

**Note**
The debounce timer currently does not support Tamper and Powerfail devices.

**Procedure**
To configure the debounce timer, do the following:

**Step 1**
Create a new input device template.

a. Select **Doors > Templates > Device Templates**.

b. Configure the debounce timer value in the **Debounce Timer (ms)** field.
Step 2 Create a new input device for the Gateway.

a. Go to Doors -> Hardware.

b. Create a new input device for the Gateway.
c. Select the **Properties** tab.

d. Choose the corresponding device template.

e. Enter the debounce timer value in the appropriate field.
Tip

If the input device is already associated with the Gateway, right-click the interface, select **Edit** and enter the debounce timer value.

Note

The default value for debounce timer is zero.
CHAPTER 9

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 14, “System Integration”.

Contents

- Configuring Personnel, page 9-2
- Downloading Credential Changes to the Gateway Modules, page 9-11
- Viewing Audit Records and Events for Personnel Records, page 9-12
- Editing Organization and Department Lists, page 9-14
- Importing Personnel Records Using a Comma Separated Value (CSV) File, page 9-16
- Using a SnapShell License Scanner to Create Personnel Records, page 9-22
  - Install and Configure the SnapShell Scanner, page 9-22
  - Scan a License to Create a New Personnel Record, page 9-26
- Configuring Badges, page 9-28
  - Configuring Badge Templates, page 9-28
  - Badge Properties, page 9-30
  - Badge Authentication, page 9-36
  - Printing Badges, page 9-45
- Setting Up Image and Signature Options for Personnel Records, page 9-55
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 Select Personnel from the Users menu, as shown in Figure 9-2.

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 4-14 for more information.
- To disable a record, select the entry and choose Disable. This is equivalent to setting the Status to Inactive.

Figure 9-1 Personnel Module: Main Window

Tip

You can also scan a drivers license to create a new record with information on the card. See the “Using a SnapShell License Scanner to Create Personnel Records” section on page 9-22.

Step 3 Enter the information in the General tab, as shown in Figure 9-2. See Table 9-1 for field descriptions. The first name, last name, and SSN/FIN/ID fields are required.
Configuring Personnel

Figure 9-2    General

![Image of Personnel Record Interface]

Table 9-1    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>
<tr>
<td>SSN/ID#/FIN</td>
<td>(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.</td>
</tr>
<tr>
<td>Comments</td>
<td>(Optional) Any additional comments or notes about the personnel record.</td>
</tr>
<tr>
<td>Site</td>
<td>(Optional) The site associated with the personnel record.</td>
</tr>
<tr>
<td>Import...</td>
<td>(Optional) Click Import... to add an image to the record (select a JPEG image from a local drive and click OK).</td>
</tr>
</tbody>
</table>

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 9-55).
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 9-3. See Table 9-2 for field descriptions.

**Figure 9-3** Occupational Information

![Add Personnel Record](image)

**Table 9-2** 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 9-2 Personnel Module: Occupational Information Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personnel Type</strong></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><strong>Status</strong></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><strong>Organization</strong></td>
<td>The organization name to which the person belongs. Select a pre-defined value from the drop-down menu, or type a name in the field. To edit the pre-defined options, see Editing Organization and Department Lists, page 9-14.</td>
</tr>
<tr>
<td><strong>Department</strong></td>
<td>The department name within the organization to which the person belongs. Select a pre-defined department name from the drop-down menu, or enter a name in the field. To edit the pre-defined options, see Editing Organization and Department Lists, page 9-14.</td>
</tr>
<tr>
<td><strong>Date of hire</strong></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 9-4. See Table 9-3 for field descriptions.

*Figure 9-4 Contact Information*

![Add Personnel Record window]

*Table 9-3 Personnel Module: Contact Information Fields*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></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><strong>Phone numbers</strong></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><strong>Email address</strong></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.

d. Enter the Card # and PIN (required) in the badge properties window, as shown in Figure 9-5.

e. Modify the other badge fields, if necessary, as described in Badge Properties, page 9-30.

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 17-23 for more information.

To configure a badge without using a template, select None.

See Configuring Badge Templates, page 9-28 to create or modify the templates.
Configuring Personnel

Figure 9-5  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 9-6.
Chapter 9  Configuring Personnel and Badges

Configuring Personnel

Figure 9-6   Personnel Record: Logins Window

- Complete the General settings. For field descriptions, see Creating User Login Accounts and Assigning Profiles, page 5-8.
- Complete the Profiles fields to define the access privileges for the login. For field descriptions, see Creating User Login Accounts and Assigning Profiles, page 5-8.
- 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 9-7).
Step 11  Click **Save and Close** in the **Personnel Record** window to make the changes permanent.
Chapter 9 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**.

- Click the **Credential Download Status** tab in the Extended Status field, as shown in Figure 9-7.
- 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 9-8 Personnel Record: Custom Window](image_url)

---

OL-27703-01

Cisco Physical Access Manager User Guide

9-11
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 9-12
- Viewing Recent Events, page 9-14

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 9-9.
Step 4 Double-click an entry to view details for the item. Table 9-4 describes the audit record fields.
Figure 9-9  Personnel Audit Records Window

Table 9-4  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 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 View to display details for the device where the change was made, including the IP address of the workstation device.</td>
</tr>
<tr>
<td>Credential</td>
<td>The username used when the modification occurred. Click View to display and 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 associated with a personnel record at the time).</td>
</tr>
<tr>
<td>Data</td>
<td>Additional information about the modification.</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 9-2, Step 6).

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

Step 1  Select Organization from the Users menu, as shown in Figure 9-10.

### 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 9-5 describes the fields. Use the View, Report and Filter buttons for increased functionality.

<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 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>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>

### 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 9-2, Step 6).

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

**Step 1**  Select Organization from the Users menu, as shown in Figure 9-10.
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 9-11.

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 9-12).

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.
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 9-14 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 9-13).
c. Select the check box for **Use CVS personnel import wizard**.

d. Click **Save**.

e. Log out and log back in to the Cisco PAM application to activate the changes (select **Logout** from the Options menu).

**Step 2**  
Select **Personnel** from the User menu.

**Step 3**  
Select **CSV Import Wizard...** from the Add... button drop-down menu (Figure 9-14).

**Figure 9-14  CSV Import Wizard**

In the File Selection window, select the file to import into Cisco PAM, as shown in Figure 9-15.

a. Click the **Browse...** button and locate the CSV file.

b. Select the checkbox for **File has a header row** if the CVS file includes data for a header row.

c. Select a file for **Rejected records output file**.

d. Click **Next**.
Figure 9-15  CSV File Selection

![CSV Import Wizard](image)

File Selection
Browse for the CSV file to import.

- **Import File**
  - C:\Documents and Settings\egran\Desktop\test input.csv
  - File has header row

- **Rejected records output file**
  - C:\Documents and Settings\egran\Desktop\test output.csv

Buttons:
- Back
- Next
- Finish
- Cancel
Step 5  In the Column Configuration window (Figure 9-16), 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.

![Figure 9-16  CSV Import Column Selection](image)
Importing Personnel Records Using a Comma Separated Value (CSV) File

### Note

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 9-16). 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.

d. 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 9-17.
Figure 9-17   CSV Preview

- **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.
Using a SnapShell License Scanner to Create Personnel Records

Complete the following instructions to configure and use a SnapShell scanner to scan and import personnel information from a standard driver’s license.

- Install and Configure the SnapShell Scanner, page 9-22
- Scan a License to Create a New Personnel Record, page 9-26

Note
SnapShell scanner is supported only on a PC running Windows XP.

Install and Configure the SnapShell Scanner

Do not connect the scanner USB cable to the PC until the scanner installation and configuration is complete.

To install and configure the SnapShell scanner software and drivers on a client PC, do the following:

Procedure

Step 1
Download and install the SnapShell drivers.

a. Log on to the Cisco PAM Server Administration utility.
b. Select Downloads, and then click SnapShell Driver.
c. Save the SnapShell-Driver.exe file to a local drive.
d. Double-click the file on your local drive to run the installer.
e. Follow the on-screen instructions to complete the installation.

Click Run, Continue, OK, or Next when prompted to accept the default settings and options.
f. Restart the client PC.

Step 2
Download and install the SnapShell SDK software.

a. Log on to the Cisco PAM Server Administration utility.
b. Select Downloads, and then click Snap Shell SDK.
c. Save the SnapShell-SDK.exe file to a local drive.
d. Double-click the file on your local drive to run the installer.
e. Follow the on-screen instructions until you reach the Destination Location window (Figure 9-18).

Click Run, Continue, OK, or Next when prompted to accept the default settings and options.
a. In the Destination Location window (Figure 9-18), record the directory where the software is installed.

For example: C:\Program Files\Card Scanning Solutions\SDK
The installation directory path is used to update the Windows environmental variables to recognize the new scanner, as described in the following steps.

**Figure 9-18 SnapShell Scanner Destination Location**

If you choose a different destination folder, record the new directory path.

b. Select **Next** or **Install** to accept the remaining default install options and begin the installation process.

c. Click **Continue**, **Allow** or **OK** for any Windows security warnings.

d. Wait for the installation process to complete.

e. Click **Finish**.

**Step 3** Add the scanner destination folder to the Windows environmental variables.

This allows Windows to recognize the scanner. You must have the directory path, as shown in **Figure 9-18**.

a. Right click **My Computer**.

b. Select **Properties**.

c. Select **Advanced**.

d. Click the **Environmental Variables** button (**Figure 9-19**).
e. Select **Path** from the System Variables list (Figure 9-19).

f. Click **Edit** (Figure 9-19).

The Edit System Variables window appears (Figure 9-20).

g. Use the right arrow button on your keyboard to move the cursor to the end of the existing text that appears in the Variable Value field.

h. Enter a semi-colon (;).

i. Paste or type the full directory path after the semi-colon (;).

For example:

```
;C:\Program Files\Card Scanning Solutions\SDK
```

**Note**: Include the full directory path, including `\SDK`.

j. Click **OK** repeatedly to close the Windows Properties windows.

**Step 4** Connect the scanner USB cable to a PC USB port.
**Step 5** Enable the scanner in the Cisco PAM System Configuration.

a. Launch the Cisco PAM desktop client. See the “Logging in to Cisco PAM” section on page 4-3.

b. Select **Preferences** from the **Options** menu.

c. Select **Personnel Info Scanner** (Figure 9-21).

**Figure 9-21 Preferences for the Personnel Info Scanner**

![Preferences window](image)

d. Select **SnapShell Drivers License Reader** from the drop-down menu.

e. Select **Is present**. This indicates that the scanner is connected to the client PC.

f. Select an option for **Store License in**.
   - Select **ID#** to record the license number in the personnel record ID field.
   - Select **Do not store** if the license number should not be recorded.

**Note** If the license number is not recorded, you must manually enter a value in the new personnel record **ID#** field. This field is required.

g. Click **OK** to save the changes and close the window.

h. Log out and log back in to the Cisco PAM application to activate the changes (select **Logout** from the **Options** menu).
Scan a License to Create a New Personnel Record

Complete the following procedure to create a new personnel record by scanning drivers license.

**Procedure**

**Step 1**  Install and configure the personnel scanner, as described in the “Install and Configure the SnapShell Scanner” section on page 9-22.

**Step 2**  Log on to the Cisco PAM desktop client.

See the “Logging in to Cisco PAM” section on page 4-3.

**Step 3**  Select **Personnel** from the **Users** menu.

**Step 4**  Insert the license into the scanner with the information you want to scan flat against the scanner surface.

See the scanner documentation for more information.

**Step 5**  Select **Add** and then **Scan Wizard** (Figure 9-22).

*Figure 9-22  Scan Wizard in the Personnel Module*

---

**Note**  The Scan Wizard menu option only appears if the scanner was enabled. See the “Install and Configure the SnapShell Scanner” section on page 9-22.

**Step 6**  Select **Start Scan** (Figure 9-23).
Step 7 Wait for the scan to complete.

Step 8 Verify that the personnel record was created and the information from the scanned license is correct.

Step 9 If the scanner Preferences are set to not store the license ID, enter a value in the ID# field (required).

Step 10 Continue to the “Configuring Personnel” section on page 9-2 to complete the personnel record configuration.
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 9-28
- Badge Properties, page 9-30
- Badge Authentication, page 9-36
- Printing Badges, page 9-45

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

To do this

Step 1  Select **Badge Templates** from the User menu.

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

Step 3  
a. Enter the template name.
b. Click **Edit Template**.
To do this

Step 4

a. Enter the badge properties. See Badge Properties, page 9-30 for field descriptions.

b. Click OK.

Note  When a location restricted user reuses a badge template that has an unprivileged access policy associated to it, then the policy is not listed.

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 9-30
- Badges Module: Cisco Access Policy, page 9-32
- Badges Module: Advanced Gateway, page 9-33
- Badges Module: Audit Records, page 9-35
- Badges Module: Recent Events, page 9-35

Badges Module: General

The General tab includes basic information about the badge.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card # (Required)</td>
<td>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><strong>Tip</strong></td>
<td>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 <strong>Access denied: Card not in database</strong>. The Data field of the event displays the card number read from the card. See Viewing Audit Records and Events for Personnel Records, page 9-12.</td>
</tr>
<tr>
<td>PIN (Required)</td>
<td>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 (Optional)</td>
<td>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 (Optional)</td>
<td>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 (Optional)</td>
<td>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 (Optional)</td>
<td>The badge holder will be anti-passback exempt during the next reader use only.</td>
</tr>
</tbody>
</table>
### Table 9-6  Badges Module: General Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Badge Type</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>Assigned to</td>
<td>(Optional) The personnel record the badge is assigned to.</td>
</tr>
<tr>
<td>Validity</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>- <strong>Active</strong>: Must be set to this value for access to be granted.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Inactive</strong>: Access is denied for all access points in system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Lost</strong>: Access is denied for all access points in system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Stolen</strong>: Access is denied for all access points in system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Destroyed</strong>: Access is denied for all access points in system.</td>
</tr>
<tr>
<td>Effective</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>Expires</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>Site</td>
<td>(Optional) A site is a single instance of a Cisco PAM database.</td>
</tr>
<tr>
<td>Comments</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 11-2.

**Figure 9-24** Badges: Cisco Access Policy Selection

In Cisco PAM 1.4.1, when a user assigns access policies to a badge, the access policies up to the root of the location hierarchy of the logged in user as well as the policies in the location of the user is available for selection. This feature is applicable only if the profile enhancement feature is set in the configuration settings, see (Data Entry/Validation - Login, page 17-9)
Badges Module: Advanced Gateway

Table 9-7 describes the advanced settings for the Cisco Physical Access Gateway.

<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.</td>
</tr>
<tr>
<td></td>
<td>See Configuring Credential Templates, page 8-21 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</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, Temporary, Employee_full_time, Employee_part_time, Intern, Visitor or Other.</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>
Badges Module: HSPD-12 Badge Extension

Table 9-7 describes the HSPD-12 Smart Card badge extension settings.

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 9-8  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>
<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>
<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>
Chapter 9  Configuring Personnel and Badges

Configuring Badges

Badge Authentication

The **Authenticate Credential** door command is used to check if a specified badge ID will be authenticated at a future time.

**Procedure**

**Step 1**  Go to **Doors -> Hardware**.

**Step 2**  Right-click the door and select **Authenticate Credential**.

**Step 3**  Enter the badge ID and timestamp.

**Step 4**  Select the **Gateway** option to perform badge authentication at the Gateway. A Grant Access or Deny Access message is displayed. or

Select the **CPAM** option to perform badge authentication at the Cisco PAM server. A Grant Access or Deny Access message is displayed.

**Usage Notes**

- The **Authenticate Credential** command supports only a future date & time.
- Doors without an associated anti-passback (APB) policy can verify badge authentication at both the Cisco PAM server and the Gateway (one at a time).
- Doors configured with an APB policy can only verify badge authentication at the Cisco PAM server.
The **Authenticate Credential** command can be issued on APB doors only for APB exempt badges. If the APB rule is enforced for a badge, the command response is always “Access denied”.

- This command is not available for the doors configured under Two Door Policy.

**Limitations**

- The **Authenticate Credential** door command does not support facility code based authentication (if the door is configured based on facility code authentication).
- The command does not authenticate the badge based on a Badge ID and Pin Number combination.
- The command does not support Pin Exempt and ADA features.
- The command does not support any properties associated with the door (such as door schedules, door admin down, door admin up), its associated devices & its properties (such as Reader configurations) and door commands (except **Deactivate Access Levels and Activate Access Levels** commands).
- The **Authenticate Credential** door command does not validate based on APB entry/exit in the limitation field.

**Using the Badge Designer**

Use the **Badge Designer** to create and modify badge designs, as described in the following instructions.

**Step 1** Select **Badge Designer** from the **Admin** menu. The main window of the **Badge Designer** module displays all badge templates loaded into the system.

**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 3-44 for more information.
Figure 9-26    Badge Designer Main Window

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 9-27.
Figure 9-27  New Badge Format

![SVG Badge Format](image)

**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
   - IBM 59 x 82.5mm

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 9-28**.
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 9-29**.

**Figure 9-29    Badge Format Editor: Rectangle Tool**

![Image of Badge Format Editor](image)

- 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 9-30**.

d. Click and drag the logo to a desired location.

**Figure 9-30**  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 9-31**.

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.
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 9-32. 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 9-51 for more information.
Figure 9-32  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 9-32.

Figure 9-33  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 Badge Authentication, page 9-36).

After a design is assigned to the badge, 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 3-44 for instructions.
• To print multiple badges at once, you must also enable the batch printing feature. See Printing Multiple Badges, page 9-47 for instructions.

This section includes the following information:
• List of Recommended Badge Printers, page 9-45
• Printing Individual Badges, page 9-46
• Printing Multiple Badges, page 9-47
• Printing High Resolution Images, page 9-51
• Changing the Default Badge Printer, page 9-52
• System Configuration Settings for Badge Printing, page 9-53

List of Recommended Badge Printers

The following recommended printers have either been used with Cisco PAM or have been tested and verified as capable printers. To use these printers with Cisco PAM, you must correctly install the printer drivers prior to printing.

Note
Cisco PAM sends a simple command to the printer that allows the system to communicate with most printer manufacturers. Before purchasing a printer, verify the printer drivers work with the operating system for your client computer, and with Cisco PAM.

The recommended printers are:

**FARGO Printers**([www.fargo.com](http://www.fargo.com))
• HDP600 Card Printer
• HDP600 CR100 Card Printer
• DTC550 Card Printer
• DTC400e Card Printer
• DTC400 Card Printer
• Persona® C30e Card Printer
• Persona® C30 Card Printer

**Magic Card Printers**([www.ultramagicard.com](http://www.ultramagicard.com))
• Enduro Card Printer


- Rio2e Card Printer
- Tango 2e Card Printer
- Tango +L Card Printer
- Prima 3 Card Printer
- Alto Card Printer
- Avalon Card Printer
- Tempo Card Printer
- Opera Card Printer

**Evolis Printers**([www.evolis.com](http://www.evolis.com))
- Dualys 3
- Pebble 4
- Securion

### 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 3-44 for instructions.

**Step 2**  (Optional) Create the badge formats (designs), as described in *Using the Badge Designer*, page 9-37. 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 9-34.

**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 9-34.

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 in batch mode, do the following:

Step 1 Purchase and install the Badge Designer license to enable badge printing. See Obtaining and Installing Optional Feature Licenses, page 3-44 for instructions.

Step 2 (Optional) Create the badge formats (designs), as described in Using the Badge Designer, page 9-37. 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 9-35.
c. Uncheck the Disable batch badge printing box.
d. Log out and log back in to the Cisco PAM application to activate the changes (select Logout from the Options menu).

**Figure 9-35  Enabling Batch Badge Printing**

![System Configuration - Cisco Physical Access Manager](image)

**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 9-36).

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 9-36).
d. Click the **Badge Printing** tab and check the **Format** check box, as shown in Figure 9-37.

e. Select a format and click **OK**.

**Figure 9-37  Badge Printing Format for Multiple Badges**

---

**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 9-38).
Step 6  (Optional) Configure a default printer, as shown in Figure 9-34 on page 9-47. These steps only occur the first time you print a badge.

- Click Yes to configure the default printer. This defines the printer used to print Cisco PAM badges.
- In the Select print configuration window, select Create new configuration.
- In the Print window, select a printer, and click OK.
- In the Page Setup window, adjust the settings if necessary, and click OK.
- 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 9-52.

Step 7  Select a Batch Printing Option, as shown in Figure 9-39.

- 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 9-40**.

**Figure 9-40  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.

If the **State** of the print job is **Failed**, verify that a **Format** is assigned to every selected badge, as described in **Step 4**.

### 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 \((r_X, r_Y) = (w*\text{DPI}, h*\text{DPI})\) where:

- \((r_X, r_Y)\) is the resolution of the photo
- \(r_X\) is the number of pixels in width
- \(r_Y\) 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 9-41**.

**Figure 9-41 Removing the Default Badge Printer**

![Preferences window with Badge Printers tab selected](image)

**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 9-46 or **Printing Multiple Badges**, page 9-47. 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 9-42).

**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 9-47.</td>
</tr>
</tbody>
</table>
Chapter 9 Configuring Personnel and Badges

Configuring Badges

Step 4 Select the Miscellaneous tab (Figure 9-43).

Figure 9-43 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>Rasterize before printing</td>
<td>It converts the watermark into an image internally and prints it on the badge. <strong>Note</strong> Ensure that you do not enable this option unless there is an issue with printing the images on the badges.</td>
</tr>
</tbody>
</table>

Step 6 Click **Save** to save the changes.

Step 7 Log out and log back in to the Cisco PAM application to activate the changes (select **Logout** from the Options menu).
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 9-44.

Figure 9-44 Preferences: Image Capture

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.
Step 7  Click OK to save the settings.

The Capture button is activated in the Personnel module. See Configuring Personnel, page 9-2 for more information. Click the Capture button and verify that the TWAIN driver is selected and opens properly.

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 9-45.

Figure 9-45  System Configuration: Personnel Data Entry Window

![System Configuration - Cisco Physical Access Manager](image)

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  Log out and log back in to the Cisco PAM application to activate the changes (select Logout from the Options menu).

Note  You must log out and log back in for the Signature Capture menu to appear in the Preferences window.

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 9-46.
Figure 9-46  Preferences: Image Capture

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 9-2 for more information.
Multifactor Authentication

From 1.4.1 Release, the user can integrate additional access control devices like biometric devices to the Cisco PAM to ensure security. These devices are configured as Generic Readers in the Cisco PAM server. The Generic readers are associated with doors and finally configured to a specific gateway. Once configured, the gateway maps the data from the Generic Reader and matches it with the server. If matched, the events are triggered accordingly.

The Generic Readers are restricted by location hierarchy when the hierarchical location is set in the Data Entry/Validation - Login, page 17-9

Contents

- Configuring Generic Readers, page 10-2
- Associating Generic Reader with Doors, page 10-3
Configuring Generic Readers

To do this

Step 1
From the Doors menu, click **Generic Readers**.

Step 2
The Generic Reader window opens. Click **Add**.

Enter the following fields:
- Name (alpha-numeric characters)
- ID (numeric)

Select values in the following drop down lists:
- Generic reader type
- Generic reader category
- Hierarchical location

Select the ADA enabled radio button.

Tip
Ensure that Name and ID are similar.
Associating Generic Reader with Doors

**To do this**

**Step 1**
From the Doors menu, select **Hardware**. The gateway drivers, gateways and doors are displayed.

**Step 3**
Click **Save and Close**. The Reader information is listed in the Generic Reader window.

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
<th>Generic Reader Type</th>
<th>Generic Reader Co.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GR1</td>
<td>1</td>
<td>BIOMETRIC</td>
<td>ENTRY READER</td>
</tr>
<tr>
<td>GR2</td>
<td>2</td>
<td>FACE DETECTION</td>
<td>ENTRY READER</td>
</tr>
<tr>
<td>GR3</td>
<td>3</td>
<td>BIOMETRIC</td>
<td>ENTRY READER</td>
</tr>
<tr>
<td>GR4</td>
<td>4</td>
<td>FACE DETECTION</td>
<td>ENTRY READER</td>
</tr>
</tbody>
</table>

**Note** Only users with Admin rights are permitted to configure generic readers.
Step 2

Select the door and right click to view the drop down menu. Click **Associate Generic Reader**. An Associate Generic reader window opens.

**Note**

You can associate a maximum of six Generic Readers to a door.

Step 3

Select the Generic Reader from the list and click **OK**. The Generic Reader is configured to the door.
Chapter 10  Multifactor Authentication

Associating Generic Reader with Doors

To do this

**Step 4**  Click **Dissociate Generic Reader** to remove a reader from the door configuration.

**Step 5**  Right click the door and select Edit. The Edit Door window opens. Select Properties to view the Generic Readers added to the door and the Multifactor Authentication timer (sec). You can edit the timer and set the time.

*Note*  The drop down menu displays the list of generic readers assigned to the door.

*Note*  The default value of Multifactor Authentication timer (sec) is 10 seconds.
**Associating Generic Reader with Doors**

**Chapter 10 Multifactor Authentication**

**Note**
- The generic readers configured by the cpamadmin is not restricted to any hierarchical location.
- When a location-restricted user creates a generic reader, the hierarchical location field is auto-populated.
- The location-restricted users can access only devices (generic readers) of their location and the events for these devices alone is populated for them.

**Note**
These points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3).

**Additional Information**

Multifactor authentication depends on the external system to authenticate biometric or facial data that the Cisco PAM receives from the generic reader. The Cisco PAM does not claim support to authenticate the received data. The gateway authenticates the data based on the badge swipe by the user and HTTPS MFA requests it receives from external devices configured as generic readers in Cisco PAM.

The External system must send the following HTTPS request for establishing a session with GW

For example:

```plaintext
POST /fcgi/user.login?login HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/.msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: 10.78.179.95
Content-Length: 48
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-au
Cache-Control: no-cache

username=gwadmin&password=Cisco123&TRACKID=12345
```

The External system after authenticating the biometric data must send the following HTTPS request to GW

For example:

```plaintext
POST /fcgi/webmgr.ac?post_generic_rdr_event HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: 10.78.179.95
Content-Length: 59
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-au
Cache-Control: no-cache

hibadge=0&lobadge=34959&Generic_Reader_id=GR1&TRACKID=12345
```
where,

TRACKID — user defined cookie

hibadgeq—higher 32 bits of a badge (badge supports max of 64 bits)

lobadge—lower 32 bits of a badge

Generic_Reader_id—ID of the generic reader as configured under the Generic Reader Module.
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 11-2
- Access Policies in Cisco PAM 1.4.1, page 11-4
- Using the Schedule Manager, page 11-8
  - Schedule Manager in Cisco PAM 1.4.1, page 11-11
- Creating Anti-Passback Areas, page 11-19
  - Configuring Anti-Passback Areas, page 11-20
  - Using Local (Gateway) Credentials if Network Communication is Lost, page 11-22
  - Evicting a Badge from APB if the User Does Not Enter the APB Area, page 11-24
  - Monitoring Anti-Passback Events, page 11-26
  - Anti-Passback Events Displayed in the Events Module, page 11-26
- Two-Door Policies, page 11-27
  - Two-Door Policies in Cisco PAM 1.4.1, page 11-27
- Two-Door State Monitoring, page 11-29
Configuring Access Policies

This section describes how to create an access policy and assign it to a user badge.

To do this

Step 1 Select Access Policy from the Doors menu, under the Access Policies sub-menu.

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

Tip To remove a policy, highlight the entry and click Delete. 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.
To do this

Step 3
Enter the general information for the policy:

a. **Name**: Enter a descriptive name for the policy.

b. **Hierarchical location**: Select the location.

c. **Description**: Enter a description of the purpose or usage of the policy.

d. **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.

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 7, “Configuring Doors” to add doors.
     – Door Groups allow you to create groups of doors, such as all lobby doors. See Configuring Device Groups, page 7-34.

b. Select a **Schedule**. To create a new schedule, click the **New Schedule** button. See Using the Schedule Manager, page 11-8 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.
To do this

**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 9, “Configuring Personnel and Badges” for more information.

---

### Access Policies in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings (Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The location-restricted user can view only doors/door groups of their assigned location. They are allowed to create access policies only with these listed doors/door groups.

- The location-restricted user can re-use the access policies created up to the root level of the location hierarchy.

- The cpamadmin can view/edit/use the access policies created by the location-restricted users.

**Note** By default, the cpamadmin can view all doors in ‘Add Policy’ page because their login is not restricted by hierarchical locations.

- The **Name** field in Add Policy page is a mandatory field while creating an access policy.

- When a location-restricted user logs in, the **Schedule** field displays the following details:
  - The schedules created by the profile user
  - The schedules created by cpamadmin
The schedules created (by other location-restricted users) up to the root level of the logged in user’s location.

- The door groups of the location-restricted user’s location alone are displayed in ‘Add Policy’ page.

Note

These points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise, the Cisco PAM appliance retains its behavior as in the previous version (1.3).

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 11-1  Reactivating Access Control Policies

<table>
<thead>
<tr>
<th>Command or action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Access Level</td>
<td>Right-click a door and select the <strong>Activate Access Level</strong> to activate a policy and select <strong>Deactivate Access Level</strong> to deactivate the access policy.</td>
</tr>
<tr>
<td>Reset Gateway</td>
<td>Right-click a Gateway icon and select the <strong>Reset Gateway</strong> 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 <strong>Reload Gateway Configuration</strong> 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

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).
To do this

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.

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 11-5 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 11-2 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, 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. See the “Understanding Door Modes, Door Schedules, and the First Unlock Feature” section on page 6-27 and the “Configuring Doors” section on page 7-2 for more information.

To add or edit schedules, do the following:

**To do this**

**Step 1**  
Select Schedules from the Doors menu, in the Schedule Manager sub-menu.

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

To remove a schedule, highlight the entry and click Delete.

**Note**  
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.
To do this

Step 3
Enter the Name, Hierarchical location and description for the schedule.

Step 4
Select a Schedule Type:

- **Door Policy**: door schedules appear in the door Properties window under the menu: **Door enable schedule**. See **Step 6, page 8-14** in **Configuring Door Templates** for more information.

- **Access Policy**: access policy schedules define the schedule for user badge access. See **Configuring Access Policies, page 11-2** for more information.
To do this

**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 11-13.

- 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.

![Time Entry Collection](image)

**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**.

![Use Schedule Mode](image)

**Note** The option **Default Mode** enables the default door mode defined in the door Properties window. See **Step 6, page 8-14** in Configuring Door Templates for more information.
To do this

Step 7  Select a Time Range for the schedule.

Step 8  Click Add to add the entry to the list of defined schedules.

Step 9  

a. Repeat Step 5 to Step 9 to add additional schedules, if necessary.

b. Click Save and Close.

Step 10  To apply schedules to an access policy, see Configuring Access Policies, page 11-2.

To apply a schedule to a door configuration, see Configuring Door Templates, page 8-10 and Configuring Doors, page 7-2. Door schedules are selected in the Properties window, in the Use Schedule Mode menu.

Schedule Manager in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings(Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The schedules can be added by users only for locations or sub-locations assigned to their user profile.
The Time entry collections and Time ranges available for selection within a schedule is also based on the user’s hierarchical location. Consequently, the time entry collections and time ranges of other locations are not valid.

The location-restricted users have read-write access to schedules in the sub-tree of their location and read-only access to schedules in the ancestral path.

**Figure 11-1 Schedule based in Hierarchical location**

- When a location-restricted user logs in the ‘Add Schedule’ page, the **Hierarchical Location** field (by default, takes the location of the logged in user) is auto-populated.
- The location-restricted user can reuse all schedules created by the cpamadmin and other profile users up to the root level of the current logged in profile user. (This includes the location-restricted user’s own schedules too.)
- The location-restricted users cannot view any unprivileged child schedules in/below their location.

Tip If the cpamadmin assigns a door policy from an unprivileged location to the logged in location-restricted user, the policy continues to work but it is not auto-populated to the logged in location-restricted user. This observation is seen across all modules. Hence it is recommended to use legitimate policies for seamless working of the profile enhancement feature.
Chapter 11 Configuring Cisco Access Policies

Using the Schedule Manager

Note

The above points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3).

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 11-2).

Figure 11-2 Schedule Manager Menu

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 11-8 for more information.

Note

If the profile enhancement feature is set in the system configuration settings, then the location-restricted user can reuse all Schedules, Work weeks, Holiday, Time ranges and Special cases created by the cpamadmin and other location-restricted users up to the root level of the current logged in location-restricted user.

Follow the steps below to modify Work Weeks/Holidays/Time Ranges/Special Cases/Time Entry Collections:

- Modifying Work Weeks, page 11-14
- Modifying Holidays, page 11-14
- Modifying Time Ranges, page 11-16
- Modifying Special Cases, page 11-16
- Modifying Time Entry Collections, page 11-18
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.
Step 4  Enter a short text description.
Step 5  Select the Hierarchical location.
Step 6  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 7  Click Save and Close when you are done.

Note  In Cisco PAM 1.4.1, Work Weeks can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. See (Data Entry/Validation - Login, page 17-9).

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 of the value.

Step 4: Enter a short text description.

Step 5: Select the Hierarchical location.

Step 6: 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 7: For a holiday that is one day, select the same day for both the beginning and end dates.

Step 8: Click the **Today** button to reset the calendar to the current date.

Step 9: Click **Save and Close** when you are done.

---

**Note**

In Cisco PAM 1.4.1, Holidays can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. See (Data Entry/Validation - Login, page 17-9).
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  Enter the Name of the value.
Step 4  Select the Hierarchical location.
Step 5  Enter a short text description.
Step 6  Enter a start and end time in 24 hour format. For example, enter 13:00 for 1 p.m.
Step 7  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 8  To remove a range, highlight the entry and select Remove.
Step 9  Click Save and Close when you are done.

Note  In Cisco PAM 1.4.1, Time Ranges can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. See (Data Entry/Validation - Login, page 17-9).

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.

Step 4  Enter a short text description.

Step 5  Select the Hierarchical location.

Step 6  Select the **Recurrence**. For example, Every Year.

Step 7  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 8  Select the options for **Week** or **Day of month**.

Step 9  Click **Save and Close** when you are done.

---

**Note**

In Cisco PAM 1.4.1, Special Cases can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. See (Data Entry/Validation - Login, page 17-9).
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.

Step 4
Select the Hierarchical location.

Step 5
Enter a short text description.

Step 6
Select the **Type**. For example, Holiday, Work Week, or Special Case.

Step 7
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 8
Select a **Time Range**. For example, **Default Time Range Group**. To create a new time range, click **New** to open the Add window.

Step 9
If you select month, select the specific month for the schedule, or select **Every Month**.

Step 10
Click **Add** to add the entry.
Creating Anti-Passback Areas

An anti-passback area is a secure area where you want to prevent someone from badging in and then passing their badge back to another person who can use it again to gain access.

To create an anti-passback area, configure a door with two readers: one as an entry reader (to gain entry into the anti-passback area) and one as an exit reader (to leave the anti-passback area). Once a badge is inside the anti-passback area, it must be used to exit the anti-passback area before it can be used to enter the area again.

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.

Related Documentation

See the following sections for more information:

- Anti-Passback areas in Cisco PAM 1.4.1, page 11-19
- Configuring Anti-Passback Areas, page 11-20
- Using Local (Gateway) Credentials if Network Communication is Lost, page 11-22
- Evicting a Badge from APB if the User Does Not Enter the APB Area, page 11-24
- Monitoring Anti-Passback Events, page 11-26
- Anti-Passback Events Displayed in the Events Module, page 11-26

Anti-Passback areas in Cisco PAM 1.4.1

In Cisco PAM 1.4.1, if the profile enhancement feature is set in the system configuration settings (Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The user can create anti pass-back areas for doors assigned to their hierarchical location only. The doors of other locations are not displayed. For example: if a user profile is assigned to location ‘San Jose’ the doors associated with this location alone is displayed. See Figure 11-5. If the user wishes to view all doors then the system configuration settings should be set accordingly.
Creating Anti-Passback Areas

Procedure
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 11-4.

- 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**.
Step 2

Complete the following fields in the detail window (see Figure 11-5).

a. **Name**: Enter a descriptive name for the area.

b. **Anti-Passback Area Number**: Read only.

c. **Comments**: Enter a description of area.

d. **Hierarchical Location**: enter the location.

e. **Site**: Read-only.

f. **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.

g. **Anti-passback delay**: Enter the delay time, in seconds, used for the **Timed** anti-passback mode.
Step 3 Click **Save and Close** to save the settings and close the detail window.

Step 4 Add an entry door and exit door to the Anti-Passback area (see Figure 11-4):

a. Choose a door from the left column.
b. Choose Entry or Exit for an Anti-Passback area in the right column.
c. Click the arrows to add or remove the door for an entry or exit point.

### Using Local (Gateway) Credentials if Network Communication is Lost

If network communication is lost between the Access Control Gateways and the Cisco PAM appliance, the entry and exit doors will fail to grant access to users since the user credentials cannot be verified. To prevent this scenario, you can configure the doors to authenticate user credentials locally (using credential data stored on the door’s Gateway module).

**Usage Notes**

- Allowing local Gateway authentication as described in this section means that the badge can be used multiple times (potentially by different users) at the entry Gateway. Use the local authentication option only if necessary. APB areas are only fully effective when stable network communication exists between the Gateway modules and the Cisco PAM appliance.
- We recommend using the **Soft (grant access)** anti-passback mode when local Gateway credentials are used. See the “Configuring Anti-Passback Areas” section on page 11-20.
- A **Gateway authenticated APB Grant Access** event is generated when an APB Gateway authenticates a badge locally.
  - Once network communication is reestablished between the Gateway and the Cisco PAM appliance, any **Gateway authenticated APB Grant Access** events are synchronized with the appliance.
  - The appliance uses the events to determine the APB status of badges. For example, if a Gateway used local credentials to grant access to a badge at the entry door while the network was down, the badge will be added to the APB area by the Cisco PAM appliance when the network communication is reestablished. When the user swipes their badge at the exit door, the Cisco PAM appliance evicts the badge from the APB area.
• If the entry and exit doors are configured to use two different Gateway modules, it is possible that a user can become trapped in an APB area. This can occur under if the user is granted access to the APB area using local credentials stored on the entry Gateway, and network communication is restored between Cisco PAM and the (second) exit door Gateway while the user is still in the APB area (before they access the exit door Gateway). This occurs because there is no record on the Cisco PAM appliance that the user entered the APB area (the record only exists on the entry Gateway). To prevent this scenario, we recommend the following:
  – Configure all APB area doors on a single Gateway. To support more than two doors on a single Gateway, a Reader module is required.
  – Install working phones that can reach the CPAM administrator within the APB area. A badge can be modified to allow one free APB pass for the trapped user.

Procedure
To configure local authentication of user credentials (using data stored on the local Gateway module and not the Cisco PAM appliance), do the following:

Step 1
Use either the Hardware or Locations & Door module to edit the door or door template configuration.
  • For example, choose Hardware from the Doors menu, expand the hardware tree, right-click on the door name, and select Edit. You can also double-click the device name to open the edit window.
  • To change the setting for a single door, see the “Modifying Door Configurations” section on page 7-18.
  • To change the setting for a door template, see the “Configuring Door Templates” section on page 8-10 and the “Door Configuration Properties” section on page 8-29.

Step 2
Select the Properties tab (Figure 11-6).

Figure 11-6 Authenticating Credentials Locally (at the Gateway)

Step 3
Uncheck the box for If server unreachable (APB). This allows you to edit the setting.
Step 4  Choose **Authenticate locally** from the menu.
Step 5  Click **Save and Close**.
Step 6  Download the configuration change.

See the “Applying Configuration Changes to Gateways” section on page 7-22.

### Evicting a Badge from APB if the User Does Not Enter the APB Area

If a user presents their badge and is granted access to an Anti-Passback Area, but decides not to enter the door, then a *Door Not Used* event is generated by the door’s Gateway module. To prevent the badge from being added to the Anti-Passback monitoring list, enable the System Configuration setting for **Evict most recent badge from APB area when door not used**.

#### Usage Notes
- This setting is only effective when the user presents their badge and then walks away without physically opening the door. If the user physically opens the door but then walks away without actually entering the APB area, the *Door Not Used* event is NOT generated and the badge is added to the APB area for monitoring. If this occurs, you must manually evict the badge from the APB area using the **Anti-Passback Monitoring** module.
- If a user presents their badge at the exit door of an APB area, the badge is evicted from the APB area. However, if the user does not open the door, and a *Door Not Used* event occurs, the badge is re-added to the APB monitoring area. In this scenario, the exit door name will be used as the new entry door (as opposed to the original entry door name).
- If a badge is evicted from the APB area after a *Door Not Used* event, as described above, and then later added back to the APB area when the user accesses the door again, then the entry door is not displayed in the **Anti-Passback Monitoring** module. The exit door is displayed instead.
- We recommend using the *Soft (grant access)* anti-passback mode when local Gateway credentials are used. See the “Configuring Anti-Passback Areas” section on page 11-20.

#### Procedure
To evict badges from an APB area when a *Door Not Used* event is generated by the door’s Gateway, do the following:

**Step 1**  Select **System Configuration** from the Admin menu.
**Step 2**  Click the **Cisco Settings** tab (**Figure 11-7**)
**Step 3**  Select the check box for **Evict most recent badge from APB area when door not used**.
Figure 11-7  Cisco Settings

Step 4  Restart the Cisco PAM appliance to activate the change. See the Using the Web Admin Menus, Commands and Options, page 3-17 for more information, or ask your system administrator for assistance.
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 11-8. 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 11-8 shows the main window.
- To reset the state of a badge, select an entry and click the Reset button.

Table 11-1 Anti-Passback Monitoring Properties

<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 Creating Anti-Passback Areas, page 11-19 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 Creating Anti-Passback Areas, page 11-19 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 12-4.

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”.

Figure 11-8 Anti-Passback Monitoring Window
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.

Two-Door Policies in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings (Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The Two-Door Policy displays doors in the user’s assigned location only. The user can view and edit doors accordingly.
- The Hierarchical location field is auto-populated for a profile when a new policy is created.
- When a location-restricted user selects the doors for the Two-Door policy, only doors within the user’s location are listed for selection.
- The cpamadmin should assign appropriate locations for the Two-Door Policy and its corresponding doors with that of the logged in user for the existing Two-Door policy to avoid any behavior discrepancy.
- The Two-Door policy monitoring page displays all badges but the location-restricted user can reset badges which are only related to the location-restricted user’s location.

| Note | These points are applicable only when the profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3.2). |

Configuring Two-Door Policies

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 11-9).

- 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.
Step 2  Complete the fields in the detail window, as shown in the following Figure 11-10:

**Figure 11-10  Two-Door Policy Detail Window**

- **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 11-11). 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.

**Note**  The doors are filtered and displayed based on the user’s assigned location.

**Figure 11-11  Select Door 1 Window**

Step 3  Click Save and Close to save the changes and close the detail window.

**Tip**  While configuring a Two-Door policy it is required to have all the entities that is the policy location and the door in the policy in the location of the logged in user.
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 11-12).

**Step 2**
To display details for the event, highlight an entry and click **Edit...**

**Figure 11-12  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 11-2  Two-Door State Monitoring Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 two-door policy. See <strong>Two-Door Policies</strong>, page 11-27 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>

**Step 3**
Click **Close** to close the detail window.
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 13, “Configuring Automated Tasks”. To view live and recorded video for events and alarms, see Chapter 15, “Video Monitoring”.

Contents

- Viewing Events, Alarms and Audit Trail Records, page 12-3
  - Events and Alarms in Cisco PAM 1.4.1, page 12-3
  - Viewing Events, page 12-4
  - Viewing Alarms, page 12-8
  - Viewing Audit Trail Records, page 12-13
  - Viewing Recent Events for a Device, Driver, or Location, page 12-15
- Viewing Events Using Personnel Photos, page 12-17
  - Viewing Event Photos, page 12-17
  - Adding a Color Border to Event Photos (Credential Watch), page 12-18
  - Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 12-21
- Recording External Events, page 12-25
- Viewing Workstation Activity, page 12-28
- Configuring Events and Alarms, page 12-29
  - Modifying Default Event Policies, page 12-29
- Event Policy Manager in Cisco PAM 1.4.1, page 12-30
- Automatically Open the Alarm Window, page 12-34
- Configuring Time Schedules, page 12-34
- Configuring Alert Sounds, page 12-37
- Setting Event and Alarm Priorities, page 12-38
- Defining User Privileges for Editing Events, page 12-38

- Using Graphic Maps, page 12-40
  - Graphic Maps in Cisco PAM 1.4.1, page 12-40
  - Graphic Maps Viewer, page 12-41
  - Graphic Map Editor, page 12-44

- Backing Up and Archiving Events, page 12-50
  - Including Events In System Backups, page 12-50
  - Pruning and Archiving Old Events, page 12-50
  - Creating Reports from Pruned Events, page 12-51
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. Alarms are critical or important events. Audit trails are events initiated by users.

This section includes the following:

- Understanding Live and Archived Events, page 12-3
- Understanding Event Timestamps, page 12-4
- Viewing Events, page 12-4
- Viewing Alarms, page 12-8
  - Alarm States, page 12-9
  - Alarm Detail Window, page 12-9
- Viewing Audit Trail Records, page 12-13

Tip

See Configuring Events and Alarms, page 12-29 to define or modify event types. To copy or move events to a historical events archive, see Backing Up and Archiving Events, page 12-50.

Events and Alarms in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings(Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The events and alarms are displayed to users based on hierarchical location assigned to their user profiles. For example: if a location-restricted user “campusadmin” is assigned to a location “San Jose Campus”, the user can view events and alarms related to this location and its sub locations only.
- The location-restricted user cannot view events of the following drivers and modules:
  - Driver level commands
  - Cleared Alarms event
  - Device commands
  - Workstation
  - Audit Trail

Note

These points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version(1.3.2).

Understanding Live and Archived Events

- You can include or exclude events from system backups. Excluding events reduces the size of the backup file.
The Event Monitoring window includes all live events in the system. Live events can be pruned to remove them from the main database to improve system performance. Pruned events are not displayed in the Event Monitoring window. Old events can also be archived and backed up to a remote server.

See the “Backing Up and Archiving Events” section on page 12-50 for more information.

Understanding Event Timestamps

Beginning with Release 1.3.0, events display the timestamp of the Cisco PAM PC workstation used to view the events. In previous releases, events displayed the Cisco PAM appliance timestamp.

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 12-1) shows the most recent events in the access-control system.

**Figure 12-1 Events Module Main Window**

Beginning with Release 1.3.0, events display the timestamp of the Cisco PAM PC workstation used to view the events. In previous releases, events displayed the Cisco PAM appliance timestamp.

**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 12-2). 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 4-10.

• **Columns...**: Define the columns displayed and their order. See Revising the Column Display, page 4-14.

• **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 4-12.

• **Search**: See Search, page 4-15.

**Step 3**
Select a record and click **View...** to open the detail window (Figure 12-2). You can also double-click the record.

![Events Module Detail Window](#)

**Figure 12-2  Events Module Detail Window**

**Step 4**
Review the properties and actions for the record. See Table 12-1 for field descriptions.

**Note**
Event fields available vary depending on the type of event. The following example is for a door event.
### Table 12-1  Event Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>The time and date when the event occurred.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Beginning with Release 1.3.0, events display the timestamp of the Cisco PAM PC workstation used to view the events. In previous releases, events displayed the Cisco PAM appliance timestamp.</td>
</tr>
<tr>
<td><strong>Time received</strong></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><strong>Site</strong></td>
<td>A site is a single instance of a Cisco PAM database.</td>
</tr>
<tr>
<td><strong>Type</strong></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><strong>Log Code</strong></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 12-29.</td>
</tr>
<tr>
<td><strong>Priority</strong></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 12-38.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A description of the event.</td>
</tr>
<tr>
<td><strong>Device</strong></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 12-41.</td>
</tr>
<tr>
<td><strong>Credential</strong></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>
</tbody>
</table>
Table 12-1  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>• 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>camera</td>
<td>The camera associated with the device.</td>
</tr>
<tr>
<td></td>
<td>• Live Video: opens the video player to view live video from the camera associated with the device.</td>
</tr>
<tr>
<td></td>
<td>• Event Video: displays archived video associated with the event, if available.</td>
</tr>
<tr>
<td></td>
<td>• Live and Event Video: opens both live and archived video windows.</td>
</tr>
<tr>
<td></td>
<td>• Arrangement: displays all camera arrangement that includes the camera associated with the event.</td>
</tr>
</tbody>
</table>

See Chapter 15, “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 12-34.

This section includes the following:
- Main Alarm Window, page 12-8
- Alarm States, page 12-9
- Alarm Detail Window, page 12-9
- Alarm Properties, page 12-10

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 12-3) shows the most recent 500 uncleared alarms.

![Figure 12-3 Alarms 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.
- **Report...**: View the selected alarms in a separate window, or save the information in a file. See Creating Reports, page 4-10.
- **Columns...**: Define the columns displayed and their order. See Revising the Column Display, page 4-14.
• **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 4-12.

**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 12-4 on page 12-10). You can also double-click the record. See Alarm Properties, page 12-10 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>
<thead>
<tr>
<th>Table 12-2 Alarm States</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
</tr>
<tr>
<td>Active</td>
</tr>
<tr>
<td>Acknowledged</td>
</tr>
<tr>
<td>Cleared</td>
</tr>
</tbody>
</table>

**Alarm Detail Window**

The detail window (Figure 12-4) 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 12-10 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 12-3  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 12-29.</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 12-38.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the alarm.</td>
</tr>
</tbody>
</table>
### Table 12-3  Alarm Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>The device associated with the alarm, 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 12-41.</td>
</tr>
<tr>
<td>Credential</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>• <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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit...</strong>: Revise the credential watch level associated with the badge.</td>
</tr>
<tr>
<td>Address</td>
<td>The address of the device.</td>
</tr>
<tr>
<td>Personnel Record</td>
<td>If a personnel record is associated with the alarm, 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, this field contains the card number.</td>
</tr>
<tr>
<td>Count</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>Alarm State</td>
<td>The state of the alarm.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ack...</strong>: 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>• <strong>Clear...</strong>: 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>• <strong>Comment...</strong>: 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>• <strong>View Instructions...</strong>: Opens a detail window with instructions for dealing with the type of alarm, if any.</td>
</tr>
</tbody>
</table>
### Table 12-3  Alarm Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target device</strong></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><strong>camera</strong></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>
<tr>
<td></td>
<td>See Chapter 15, “Video Monitoring” for more information.</td>
</tr>
</tbody>
</table>
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 12-5) shows the most recent audit records.

**Figure 12-5 Audit Trail Main Window**

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
<th>Device</th>
<th>Personnel Record</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>31/12/2009 05:26:44.960</td>
<td>Automation rule updated</td>
<td>0x0e-8768901b</td>
<td>0x0e-8768901b</td>
<td>LOCAL_FILE_POST_Cameras</td>
</tr>
<tr>
<td>31/12/2009 05:26:46.960</td>
<td>Automation rule updated</td>
<td>0x0e-8768901b</td>
<td>0x0e-8768901b</td>
<td>LOCAL_FILE_POST_Cameras</td>
</tr>
<tr>
<td>31/12/2009 05:27:03.960</td>
<td>Device record updated</td>
<td>0x0e-8768901b</td>
<td>0x0e-8768901b</td>
<td>Cisco AccessPoint04</td>
</tr>
</tbody>
</table>
```

**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 4-14.
- **Filter**: See Using Filters, page 4-12.

**Step 3** Select a record and click View... to open the detail window (Figure 12-6). You can also double-click the record.

**Step 4** Review the properties and actions for the record. See Table 12-4 for field descriptions.
Chapter 12  Events & Alarms

Viewing Events, Alarms and Audit Trail Records

Figure 12-6  Audit Trail Detail Window

Table 12-4  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 12-29.</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 12-38.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the event.</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 4-10.
Step 3  
Right-click the device or driver, and select **View Recent Events** from the drop-down menu, as shown in Figure 12-7.

**Figure 12-7  View Recent Events Menu**

Step 4  
Double-click an event to view event details, as shown in Figure 12-8.

**Figure 12-8  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 12-17
• Adding a Color Border to Event Photos (Credential Watch), page 12-18
• Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 12-21

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 12-9).

**Figure 12-9   Event Photos Window**

---

**Note**
The screen appears blank (without fields or data) until a photo event is available for display.

**Step 3**
From the main window, you can perform the following actions:

• **Filter**: Filter to display specific types of events (see Using Filters, page 4-12 and Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 12-21).

• **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.
  – **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.
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:

**To do this**

**Step 1**

Enable Credential Watch Levels menu:

a. Select System Configuration from the Admin menu.

b. Select the Miscellaneous tab.

c. Select the Enable credential watch levels check-box.

d. Click Save.

e. Log out and log back in to Cisco PAM to activate the changes (select Log Out from the Options menu).
To do this

**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 5, “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**.
To do this

**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**.
Viewing Events Using Personnel Photos

To do this

Step 5
Open the Event Photos module: select Event Photos from the Events & Alarms menu, in the Monitoring sub-menu.

Step 6
Present the badge to the door card reader to display the associated badge photo in Event Photos. In this example, a dark blue border is displayed and the watch level is “New Employee”.

Note
The screen appears blank (without fields or data) until a photo event is available for display.

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 12-10).
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.
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 12-11).
Figure 12-11  Filter Log Code

Cisco Physical Access Manager User Guide

Chapter 12  Events & Alarms
b. Select the events to be displayed in Event Photos, as shown in Figure 12-12. For example, select Door Grant Access.

Figure 12-12   Select the Log Code

![Image of Select the Log Code dialog box]

- 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 12-25. This file also defines the categories for the log codes.
2. Create a Text File to Define the Event Names in Cisco PAM, page 12-26.
3. Import the Files into Cisco PAM, page 12-26.
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: `SampleExtEventDefns.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.

To do this

Step 1
Select External Events from the Events & Alarms menu.

Step 2
Click Import.
To do this

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 12-25
   • Create a Text File to Define the Event Names in Cisco PAM, page 12-26

Step 4

(Optional) Preview the settings.

Click Finish to save the changes

Click Back to select a different file.

Step 5

The new log codes are displayed in the main External Events window.

Step 6

Add external events and alarms to Cisco PAM using the recordExtEvent API, as described in the Cisco Physical Access Control API Reference Guide.
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 12-13) shows the most recent events in the access-control system.

**Figure 12-13  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 behavior 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.

*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.

**Contents**

- Modifying Default Event Policies, page 12-29
- Event Policy Manager in Cisco PAM 1.4.1, page 12-30
- Automatically Open the Alarm Window, page 12-34
- Configuring Alert Sounds, page 12-37
- Setting Event and Alarm Priorities, page 12-38
- Defining User Privileges for Editing Events, page 12-38

*Tip*

To automatically trigger actions when an event occurs, see Chapter 13, “Configuring Automated Tasks”.

### 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.

Event Policy Manager in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings(Data Entry/Validation - Login, page 17-9), you need to remember the following points while creating/editing event policies:

- A location-restricted user will not be able to edit default event policy rules.
- When a location-restricted user creates a new rule, by default the Hierarchical location field is auto-populated.
- The new rule will be applied only to devices belonging to the user’s location.
- When a location-restricted user creates an event policy it also applies to the unprivileged child locations under the location-restricted user.
• Location-restricted users cannot filter devices of their location while creating an event policy.

**Note**

These points are applicable only when the profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3).

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 12-14) shows all event policies defined within the system.

**Figure 12-14  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 12-15. You can also double-click the entry.
- Click **Add...** to open the detail window (Figure 12-15) and add a new event policy.
- Select an entry and click **Delete** to delete the selected event policy.

Each field is described in Table 12-5 on page 12-32.
Figure 12-15  Event Policy Manager Detail Window

Event Policy Properties

An event policy has the following properties:

Table 12-5  Event Policy 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>
## Table 12-5  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 7-34.</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><strong>Time schedule</strong></td>
<td>Specifies the time schedule used for event policies. See Configuring Time Schedules, page 12-34 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><strong>Priority</strong></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><strong>Alert Sound</strong></td>
<td>The sound to be played, if <strong>Is Alarm</strong> is checked. Available alert sounds are managed in Configuring Alert Sounds, page 12-37. Click <strong>Play</strong> to preview the alarm sound.</td>
</tr>
<tr>
<td><strong>Background color</strong></td>
<td>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><strong>Foreground color</strong></td>
<td>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 12-16).

**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 5-2.

![Figure 12-16 Profile: General Tab](image)

Configuring Time Schedules

Time schedules define when events and automated rules will run. See **Configuring Events and Alarms**, page 12-29 and **Configuring Global I/O Automated Rules**, page 13-18 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 12-17**.
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 12-18.

**Figure 12-17**  **Time Schedule: Main Window**

![Time Schedule: Main Window](image)

**Figure 12-18**  **Time Schedule: Detail Window**

![Time Schedule: Detail Window](image)

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 12-18.
c. Enter the **Start** and **End** time in hour and minute format (h:h: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 12-18**).
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 12-29.

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 12-20) 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 12-20  Alert Sound Module Main Window**

![Alert Sound Module Main Window](image)

**Step 3** Edit a new or existing alert sound using the detail window (Figure 12-21):

**Figure 12-21  Alert Sounds Module Detail Window**

![Alert Sounds Module Detail Window](image)

- Click Import WAV File and select a sound file from a local drive. Click Play WAV File... to preview the alert sound.
- Enter a name for the alert sound.
- 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 12-22).

![Figure 12-22 Event Policy Window](image)

**Figure 12-22 Event Policy Window**

**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 12-29.

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 12-23).

**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 12-23  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.

Graphic Maps in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings(Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The graphic maps are displayed to users based on hierarchical location assigned to their user profiles. For example: if a user profile “campusadmin” is assigned to a location “BVVC”, the user can view maps related to this location and its sub locations only. If the user tries to view any other location maps, an error is displayed. See Figure 12-24.

- When location-restricted users create a new map, the users can select from a list of devices that are populated based on the location to which they are assigned.

- All device groups up to the root of the location-restricted user are visible and the user can reuse these device groups provided at least one device is present in the location-restricted user’s assigned location.

- The maps created by cpamadmin are not restricted by any hierarchical location.

- The location-restricted user is restricted from viewing maps created by the cpamadmin.

- The hierarchical location is auto populated for a location-restricted user while creating maps.
When the cpamadmin removes a location from the location-restricted user’s hierarchy, all devices of that location is removed automatically. However if any device commands relating to these devices are present, then it requires manual removal, so the cpamadmin should ensure that they remove all associated devices/commands (manually) along with the location.

Note

These points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version(1.3)

The followings sections describes the map viewer, and the editor used to create the maps:

- Graphic Maps Viewer, page 12-41
- Graphic Map Editor, page 12-44

Graphic Maps Viewer

Select Graphic Maps Viewer in the Events & Alarms menu (in the Monitoring submenu).

Figure 12-25 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 12-25   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.
- *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.

<table>
<thead>
<tr>
<th>Inside Color</th>
<th>Outside Color</th>
<th>Device Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td></td>
<td>Alarm(s)</td>
</tr>
<tr>
<td>Orange</td>
<td></td>
<td>Acknowledged alarm(s)</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td>No alarms</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>Unknown, fault or active state</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td>Armed and inactive state</td>
</tr>
<tr>
<td>Light Blue</td>
<td></td>
<td>Disarmed and active state</td>
</tr>
<tr>
<td>Dark Blue</td>
<td></td>
<td>Disarmed and inactive state</td>
</tr>
</tbody>
</table>

**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>
</tbody>
</table>
Table 12-6 Toolbar and Navigation Controls (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Graphic Maps Viewer. 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 Reset, or right-click the map and click Reset View.</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:

To do this

Step 1
Select Graphic Map Editor from the Admin menu.

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.
### Chapter 12  Events & Alarms

#### Using Graphic Maps

**To do this**

**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.

**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.
To do this

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.

Step 6  
Add devices or doors to the appropriate location on the map.

The device will report real-time status in the Graphic Maps Viewer.

a. Click the **Devices** tab to view the Gateways, doors and drivers.

b. 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 7-34 for more information.
To do this

Step 7
Add locations to the map.

The device will report real-time status in the Graphic Maps Viewer.

a. Click the Locations tab.

b. 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).

Step 8
Add commands to the map. Users can click on command icons in Graphic Maps Viewer to invoke the command.

a. Click the Commands tab to view the commands available for the selected device.

b. Drag a command to the map. The Device Command window opens.

c. Click OK to accept the selected command and add it to the map.
To do this

Step 9 (Optional) To select a different device and command combination using the Device Command window, do the following:

a. 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. 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.

b. Select a command for the device(s): click Choose and select a command from the list.

c. (Optional) Click Choose to select the Parameters for the command, if required.

![Device Command Window](image)

**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.

d. Click OK.

Step 10 (Optional) Add automated rules to the map.

a. Click the **Devices** tab and select the **Automation Driver**.

b. Click the **Command** stab and drag the icon for **Invoke Automation Rule** to the map. The Device Command window appears.

![Device Command Window](image)

**Note** In the Device Command window, the selected device is **Automation Driver**, and the selected command is **Invoke Automation Rule**.

c. To select the rule, click **Choose** in the Parameters field and select the rule.

![Device Command Window](image)

To do this

Step 11  (Optional) Create multiple views of the map.

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 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.

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.
Back Up and Archiving Events

You can include or exclude events from system backups. You can also prune and archive old events to remove them from the main database. The following topics provide more information:

- “Including Events In System Backups” section on page 12-50
- “Pruning and Archiving Old Events” section on page 12-50
- “Creating Reports from Pruned Events” section on page 12-51

Including Events In System Backups

Events can either be included or excluded from system backups, as described in the “Backing up the Cisco PAM Database” section on page A-1. Including events allows you to restore those events along with other data and configurations. However, the backup process will take longer and the backup file will be larger.

Excluding events from a system backup reduces the size of the backup file, and the time required to complete the backup process.

Pruning and Archiving Old Events

As an alternative to backing up all events, you can prune and archive old events.

- Pruned events are removed from the live database table and placed in a separate database table, allowing you to reduce the size of the main database while keeping them accessible on the Cisco PAM system. Pruned events are not visible in Events & Alarms, but are included in reports. Pruned events are also included in system backups.

- Archived events are removed from all Cisco PAM database tables and copied to a compressed file. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archived events are not visible in the Events & Alarms listings or Reports, and are not included in system backups.

Archiving historic events improves system performance and simplifies monitoring since only the latest, most relevant, events and alarms are displayed. System backup file sizes are also reduced. 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.

Archived event files can be restored to the Cisco PAM database, if necessary, or used by other applications to view old events or run reports. See the “Creating Reports from Pruned Events” section on page 12-51.

See the “Archiving Historical Events” section on page 3-24 for more information.
Creating Reports from Pruned Events

To run reports on historical events that were copied to the historical events database, create a filter-based report in the Report Manager.

To do this

Step 1
Select Report Manager from the Reports menu.

Step 2
Click Add and select Add Filter-based Report Template.

Step 3
Select the template settings:

- **Name**: the name of the report.
- **Max results**: the number of results displayed in the report. -1 is unlimited results.
- **Item type**: select Events (Historical).
- **Edit Filter**: the filter setting, similar to filters available in the toolbar. See Using Filters, page 4-12.
- **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 4-10.
- **Variable Parameters**: information the user is be prompted to provide when the report is run.
- **Edit Columns**: the columns used in the report. Use the Up and Down buttons to reorder the columns for the report.

Step 4
Click Save and Close.
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 13-2
  - Creating a Button, page 13-2
  - Creating a Button That Runs An Automated Rule, page 13-7
  - Creating Panels (Windows) of Related Buttons, page 13-7
  - Restricting User Access to Button Panels, page 13-8
- Configuring Edge Policies, page 13-9
- Configuring Device I/O Rules, page 13-15
- Configuring Global I/O Automated Rules, page 13-18
  - Enabling the Automation Driver, page 13-19
  - Configuring Automated Tasks Using Global I/O, page 13-21
  - Example: Automated Weekly Report, page 13-31
- Automation Rules in Cisco PAM 1.4.1, page 13-35
- Defining Reports (Report Manager), page 13-39
  - Using the Report Manager, page 13-40
  - Filter-based Report Template, page 13-41
  - SQL-Based Report Template, page 13-43
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 13-2
- Creating a Button That Runs An Automated Rule, page 13-7
- Creating Panels (Windows) of Related Buttons, page 13-7
- Restricting User Access to Button Panels, page 13-8

Creating a Button

To do this

Step 1 Select **Quick Launch** from the Events & Alarms menu, in the Monitoring sub-menu. The Quick Launch window opens.

![Quick Launch Window](image)

**Note** The Quick Launch window appears blank on first use since no Quick Launch icons have been created.

Step 2 Select **Add Widget**.

![Add Widget](image)

Step 3 Select a widget type to create a Quick Launch button.

The widget types include:

- **Open Module**: creates a button that opens a Cisco PAM module window.
- **Device Command**: creates a button that executes a command for a door or device. For example, grant access to a door.
- **Label**: Creates a text label used to organize Quick Launch buttons into rows and columns.
To do this

Step 4  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.

![Image of Location tab]

**Note**  If another button already exists in that location, the existing button location automatically shifts to the right.

Step 5  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

To do this

**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**.

**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 Configuring Device Groups, page 7-34.
     - **Monitor Point**
     - **Monitor Point Group**
To do this

**Step 8** Select a command for the door or device(s):

   a. Select *Choose*.

   b. Select a command from the list. For example, **Deactivate Access Levels**.

   c. Click **OK**.

**Tip** See **Device and Driver Commands, page 7-41** and **Door Modes and Commands, page 7-46** for command descriptions.

**Step 9**

   a. Click **Choose** to select the Parameters for the command, if required.

      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.

   b. Click **OK**. The new button appears on the main Quick Launch page.
Creating Quick Launch Buttons

**To do this**

**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.


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.
Creating Quick Launch Buttons

Step 4
Click OK.

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.

Step 1
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.

a. Open the Profiles module.
b. Click Add or Edit to create or modify a profile.
c. Click the Module tab.
d. Click Quick Launch.
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 5, “Configuring User Access for the Cisco PAM Desktop Client”.

Step 2
Assign the profile to the user login.

a. Open the Login module.
b. Click Add or Edit to create or modify a user login.
c. Select Profiles.
d. Select the profile that includes the required access privileges.
Configuring Edge Policies

Use **Edge Policies** to create event based actions that are stored and executed on specific Gateway modules. These policies can trigger URL Actions that perform tasks in external devices. For example, when a user swipes their badge at a reader device, a URL action can be sent to the Cisco VSM system to start recording surveillance video for that location.

**Differences Between Edge Policies and Global I/O Triggered URL Actions**

- Edge Policies are stored on the Gateway module, and are triggered immediately when an event occurs, even if network communication with the CPAM server is delayed or lost.
- Global I/O rules may not execute immediately due to network delays, rules processing, communication between Cisco PAM and the Gateways, or other factors.
- Global I/O rules, however, offer additional options for automation rule triggers and subsequent actions. In addition, URL Actions for an Edge Policy are limited to the subset of events that can be triggered by the Gateway.

See **Configuring Global I/O Automated Rules, page 13-18** instructions to create global automation rules.

**Procedure**

Complete the following instructions to create or modify Edge Policies:

This example assumes that the Gateways, readers, doors, personnel accounts, and other components are installed, configured, and working properly. For instructions, see the other chapters in this guide, including Chapter 7, “Configuring Doors” and Chapter 9, “Configuring Personnel and Badges”.

e. Click **Save and Close**.
**To do this**

**Step 1** Enable the Edge Policy menu.

a. Select **System Configuration** from the Admin menu.
b. Select the **Cisco Setting** tab.
c. Select the check box **Enable “Edge Policies” Module**.
d. Click **Save**.
e. Log out and log back in to the Cisco PAM application to activate the changes (select **Logout** from the Options menu).

**Step 2** Select **Doors > Edge Policies > Edge Policy**.

**Step 3** Click **Add**, or select an existing rule and click **Edit**.
To do this

Step 4  Enter a name and description for the rule.

Tip  Select or de-select Enabled to activate or deactivate the policy.

Step 5  Define the Trigger type.

The trigger defines the event (such as Door Grant Access) and the devices (such as a Gateway) for the trigger. When the specified event occurs on the specified device, the Edge Policy action is triggered. Release 1.3 supports event triggers only.

a. Match—Select Any trigger.

b. Type—Select Event.
To do this

Step 6  Define the Trigger.

The trigger defines an event that occurs on a device. When this trigger occurs, the action for the Edge Policy is invoked.

a. Click Add New to select the event and device(s) used to trigger the rule.

Tip  You can also use the Add available button to choose a previously defined trigger (condition). To create, edit or delete the saved triggers, select Doors > Edge Policies >Conditions.

b. Enter the General properties:
   - Name—enter a meaningful name. For example, Access Lobby Door.
   - Description—enter the trigger description. For example, Access door event at lobby door.

c. Select Event and select the event for the trigger.
   - Select an available event from the left column.
   - Click the arrow to move the event to the right column.

d. Select Devices and select the devices that the event must occur on.
   - Filter by—select the device. For example, Gateway.
   - Device Type—shows the available device types. For example, Door.
   - Select—highlight a device in the Available column, and click the arrow to move it to the Selected column.
   - Device(s)—click Choose and select an available device (such as a Door) and move it to the Selected field.

e. Verify that the selected device name appears in the Devices field.

f. Select Save and Close.
To do this

**Step 7**  Select the **Action** that occurs when the condition(s) are met.  
- **URL Action**—select a URL Action that will occur when the conditions are met. See the “Configuring URL Actions” section on page 14-2. The URL action must be an Edge action type.

**Note**  For Cisco VSM video recording, use create a soft trigger event in VSM to generate the URL used to record video. Enter that URL in the URL action.

**Step 8**  Click **Save and Close** to save the changes. The new or revised policy is displayed in the main window.

**Tip**  Click the **Enabled** check box to activate or deactivate the policy.
To do this

Step 9  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 7-22 for more information.
Configuring Device I/O 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 13-18 instructions to create global rules.

Complete the following instructions to create or modify Device IO Rules:

---

**To do this**

**Step 1** Select Device IO Rules from the Doors menu.

**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.
To do this

**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.
To do this

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.

A Global I/O rule is comprised of a trigger and an action.

The **trigger** can be one of 3 types:
- **Periodic**
  - Monthly—the day of the month and time the action occurs
  - Weekly—the day of the week and time the action occurs
  - Daily—the time of the day the action occurs
- **Manual**
  - The action only occurs when manually invoked by a user.
- **Event**
  - The action occurs only when specified criteria are met.

The **action** occurs when the trigger conditions are met. The options are to generate a report or issue a device command.

Create automated tasks using the Global I/O module, as described in the following sections.
- **Enabling the Automation Driver, page 13-19**
- **Configuring Automated Tasks Using Global I/O, page 13-21**
- **Example: Automated Weekly Report, page 13-31**
Enabling the Automation Driver

To enable automated tasks, the Automation Driver must be created and configured in the Hardware window. The driver is 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 6-3 for a description of the various system drivers.

To do this

Step 1  Select Hardware from the Doors menu.

Step 2  Right-click the Driver Manager and select New Automation Driver....
To do this

Step 3  Enter the driver settings:

- Click the **General** tab and enter a **Name** for the **Automation Driver**.
- If e-mail notification is needed, click the **SMTP Server Settings** tab and enter the SMTP server settings.
- Click **Save and Close** to close the configuration window and create the Automation Driver.

Step 4  Right-click the **Automation Driver** and select **Start**.

This enables the driver and activates any automated rules.
Chapter 13 Configuring Automated Tasks

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.

To do this

Step 1 Select Global I/O from the Events & Alarms menu. The Automates Rules window lists the currently defined rules.

The main window includes the following columns.

- **Name**: The name of the automated task.
- **Enabled**: Yes if the task is enabled. No if the task is disabled.
- **Trigger**: Operator-defined events, and or time schedules that execute an action or notification.
- **Action**: Reporting or device commands executed on devices.
- **Notification**: The notification type. For example: E-mail, FTP, or Syslog notification.

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

Tip You can also right click to select an option.

Step 3 Enter a Name for the rule and select or deselect the Enabled checkbox.
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.
  - 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 12-34** 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.
To do this

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 or organization data. The file must be located on an FTP server or CPAM 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 13-25 for descriptions of the fields and settings for each option.
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 13-19.

- **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.
Chapter 13      Configuring Automated Tasks

Configuring Global I/O Automated Rules

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 or CPAM server. The file can contain personnel or organization data.
- **Group Edit**: Edits multiple personnel or badge records.
- **Sanity Report Action**: Provides a snapshot of the specified system status.
- **URL Action**: performs a pre-defined URL action.

Create or edit an automated rule as described in Configuring Automated Tasks Using Global I/O, page 13-21. In the Actions section, click Add to create a new action, or select an existing action and click Edit.
Create or edit an automated rule as described in Configuring Automated Tasks Using Global I/O, page 13-21. 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 13-39.

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**.
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 7-34.
   - **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 13-22 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**, page 7-41 and **Door Modes and Commands**, page 7-46 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 file from a directory located on the CPAM Server or a FTP server.

- The properties import file must be named `csv.import.properties`.
- 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.
- 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.

a. Select the Action type **CSV Import**.
b. Select the data **Type**: Personnel or Organizations.
c. **For CSV import from CPAM server** enter the file settings as:
   - **Directory Path**: The directory path of the CSV file location in CPAM server.
   - **Configuration file**: (read only) the import configuration file having import mapping settings must be named `csv.import.properties`.

   **Note** Here the CSV file and `csv.import.properties` should be placed in any of the CPAM server directories like `/tmp` or `/directory` that has root level permissions. Ensure that both files are in the same directory path.

d. Click **Save and Close**.
e. **For CSV import from folder/directory located on a FTP server**, enter the server and file settings as:
   - **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 configuration file having import mapping settings, must be named as `csv.import.properties`.

   **Note** The `.csv` and `csv.import.properties` files should be placed in the location specified in the Directory path.

f. Click **Save and Close**.

For CSV import for personnel records from local client machine desktop, See Importing Personnel Records Using a Comma Separated Value (CSV) File, page 9-16
Group Edit
Edits multiple personnel or badge records.

a. Select the Action type **Group Edit**.
b. Select the Item Type: for example, **Badges**.
c. (Optional) Click **Edit Filter** to apply the changes to a subset of badges or records. Use the filter window to define the filter settings.
d. Click **Group Edit** to enter the changes that will apply to all specified personnel or badge records.
e. 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 6-18** 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 14-2 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 Configuring Quick Launch Buttons, page 13-2).
Example: Automated Weekly Report

The following sample shows how to configure an automated rule that runs a report on a weekly basis.

To do this

Step 1  Select Global I/O in the Events & Alarms menu.

Step 2  Create a new rule and enter the General settings:

a. Click Add... to open the Automation Rule window.

b. Name: Enter a descriptive name for the rule. For example: Daily Gateway Report (output).

c. Enabled: Verify that the Enabled checkbox is selected.

Step 3  Select the periodic Trigger to have the report sent at a regular scheduled time:

a. From the Trigger row, click the New... button.

b. Select Periodic from the drop-down menu.

c. Select OK.
To do this

Step 4 Select the days and times for the periodic Trigger:
   a. Interval: Options include: Monthly, Weekly and Daily.
   b. Day of Week/Month: If you select Monthly or Weekly, select the day of the month or week.
   c. Time of day: 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.
   d. Select OK.

Step 5 Select the action to generate a report file:
   a. In the Action section, click the Add... button.
   b. Select Report from the drop-down menu.
To do this

Step 6  Define the type of report and the format of the output:

a. From the Report window, click **Choose...**. The **Choose Report** window displays all reports defined in the system.

- Select a report from the list.
- Click **OK** to close the **Choose Report** window.

![Choose Report Window](Image)

b. From the Report window, click **Settings** to open the **Report Generation** window.

- **Title**: Enter a Title for the report.
- **Format**: Select if the report should be in **Record-style** or **Table-style**.
- **Output**: Select the type of file to output. For example: PDF document or Excel spreadsheet.
- Click **OK** to close the **Report Generation** window.

c. Click **Save and Close** to save the **Action** settings and close the **Report** window.

d. Repeat these steps to create additional **Actions** for the automated rule, if necessary.

**Tip**  To create or edit reports, see [Defining Reports (Report Manager), page 13-39](#).
To do this

Step 7 Select the Notification method. For example, send the report file by e-mail:
   a. From the Notification row, click the New... button. Notification options are: E-mail, FTP or Syslog.
   b. Select E-mail from the notification drop-down and configure valid e-mail addresses as displayed in the following step.
   c. Click OK.

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.
To do this

**Step 9**

a. Verify that all configurations are correct.

b. Click **Save and Close** to save the Automated Rule and close the window.

**Step 10** Add the Automation driver as described in **Enabling the Automation Driver**, page 13-19.

**Note** This step is only necessary if the Automation Driver is not already added.

**Automation Rules in Cisco PAM 1.4.1**

If the profile enhancement feature is set in the system configuration settings (**Data Entry/Validation - Login**, page 17-9), the following changes are impacted in this module:

- The location-restricted users can create automation rules in the Global I/O interface in their set of accessible locations only. The user is allowed to add trigger conditions and actions only on devices within their assigned hierarchical location. See (Figure 12-1)
The location-restricted user has to select the Hierarchical Location while adding an ‘Automation rule’ unlike other modules where the hierarchical location of the location-restricted user is auto-populated.

When a location is assigned to a global I/O rule of trigger type periodic and event, the rule is applied only for the location it was created to and its child nodes, if any.

If the trigger type is manual then the rule is applied to the locations that are common between the locations assigned to the location-restricted user and the location(with its child nodes) in which the global I/O was created.

If the location-restricted user wishes to invoke a Global I/O manually, the automation driver has to be present in the Hardware View of the location-restricted user. To achieve this, the cpamadmin can populate the automation driver in the hierarchical location of the location-restricted user by modifying the profile of the user.

To populate automation driver, do the following:

**Step 1** Go to Profile > Edit > General > Assign to Login.
Step 2 Select the **Ignore hierarchical location restriction for device matching filter** checkbox.

Step 3 Click **Filter**. The Filter Device window appears.

Step 4 Select Automation Driver from the Type drop down list.
Step 5  Click OK to save the changes. The automation driver is populated.

**Note**  The drawback of populating the automation driver is that the automation driver events of other locations that are not under the purview of the location-restricted user also become visible.

- All automation rules created up to the root of the hierarchy of the location-restricted user is visible to the user. The location restricted user can invoke these rules provided there are any devices (at least one) pertaining to their location in these rules.
- All device groups up to the root of the location-restricted user are visible and the user can reuse these device groups provided at least one device is present from the location restricted user’s assigned location in these device groups. When these device groups are reused, the commands are applied to the devices belonging to the location restricted user’s location.
- When the cpamadmin removes a location from the location restricted user’s hierarchy, all devices of that location is removed automatically. However if any automation rules relating to these devices are present, then it requires manual removal, so the cpamadmin should ensure that they remove all associated automation rules (manually) along with the location.

**Note**  These points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3).
Defining Reports (Report Manager)

The Report Manager comprises of predefined set of Reports to retrieve data. You can use the Report Manager to view, run, add or modify reports. Further these reports can be 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. In 1.4.1 Release, Filter based reports are generated to an user based on the hierarchical location to which the user belongs to. This is due to the configuration settings. 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 13-18 for instructions to assign reports to automated tasks.

This section includes the following information:

- Report Manager in Cisco PAM 1.4.1, page 13-39
- Using the Report Manager, page 13-40
- Filter-based Report Template, page 13-41
- Object SQL-based Report Template, page 13-42
- SQL-Based Report Template, page 13-43

Report Manager in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings (Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- A location-restricted user can view and reuse default reports up to their root level location.
- The cpamadmin should restrict access of SQL based Reports to location-restricted users in the Profiles module. This action prevents the location-restricted users from accessing SQL based reports.

Note
These points are applicable only when the profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3.2).
Chapter 13      Configuring Automated Tasks

Defining Reports (Report Manager)

Using the Report Manager

Step 1  Select Report Manager from the Reports menu. The main window appears, as shown in Figure 13-5.

Figure 13-5  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 13-41
- SQL-Based Report Template, page 13-43

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 13-6 shows the detail window for a Filter-based Report Template. Complete the fields according to the descriptions in Table 13-1.

Figure 13-6 Filter-based Report Template

<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. &quot;-1&quot; retrieves 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 Using Filters, page 4-12.</td>
</tr>
</tbody>
</table>
### Defining Reports (Report Manager)

In Cisco PAM 1.4.1, the filter based reports have an additional field, **Hierarchical Location** that allows the user to retrieve reports on the devices or events in the user’s assigned location only. See (Figure 13-7). This is based on the system configuration settings. See (Data Entry/Validation - Login, page 17-9).

#### Table 13-1  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 4-10.</td>
</tr>
<tr>
<td>Variable Parameters...</td>
<td>Lists parameters for the report. The selected parameters will prompt the user to provide values for them when the report is run. Based on the parameter values data will be retrieved.</td>
</tr>
<tr>
<td>Edit Columns...</td>
<td>Select the columns used in the report. Use the Up and Down buttons to reorder the columns for the report.</td>
</tr>
</tbody>
</table>

In Cisco PAM 1.4.1, the filter based reports have an additional field, **Hierarchical Location** that allows the user to retrieve reports on the devices or events in the user’s assigned location only. See (Figure 13-7). This is based on the system configuration settings. See (Data Entry/Validation - Login, page 17-9).

#### Figure 13-7  Filter based Report with hierarchical Location

![Image](add_filter_based_report_template.png)

**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 13-8* shows the detail window for a Object SQL-based Report Template. Complete the fields according to the descriptions in Table 13-2.
Defining Reports (Report Manager)

Figure 13-8  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 13-9 shows the detail window for a SQL-based Report Template. Complete the fields according to the descriptions in Table 13-2.

Table 13-2  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. &quot;-1&quot; retrieves 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 Item type drop-down menu.</td>
</tr>
<tr>
<td>Report Settings...</td>
<td>Report generation options. For more information on report settings see Creating Reports, page 4-10).</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>

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 13-9 shows the detail window for a SQL-based Report Template. Complete the fields according to the descriptions in Table 13-2.
Defining Reports (Report Manager)

Chapter 13      Configuring Automated Tasks

Defining Reports (Report Manager)

Figure 13-9  SQL-based Report Template

![Image of SQL-based Report Template]

**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. &quot;-1&quot; retrieves unlimited results.</td>
</tr>
<tr>
<td>SQL</td>
<td>The SQL query to be executed. It returns all the column data defined in the SQL.</td>
</tr>
<tr>
<td>Report Settings...</td>
<td>Report generation options. For more information on report settings see Creating Reports, page 4-10.</td>
</tr>
<tr>
<td>Variable Parameters...</td>
<td>Dynamic parameters can be added through this option with a name and a type to match with any of the field columns defined in the sql query. The previously added parameters could be viewed and edited. Parameters configured will prompt the user to provide values for them when the report is run and based on that data will be retrieved. The parameter values replace question marks in the SQL query, in order. The number of parameters must match the number of question marks in the query. Tip: A sample SQL based report template defined with variable parameters will have the sql query part like &quot;select evt_time from vx_evt where evt_time &lt; (?) ;&quot;</td>
</tr>
</tbody>
</table>

**Additional Information**

- To avoid Non-Admin (other than Administrators profile) users from running and editing the SQL Based Reports to retrieve information beyond their access levels, unselect ‘Allow execution of SQL-based Reports’ option in Users > Profiles > Add Profile/Edit Profile > Modules > Report Manager.
- SQL based reports can also be invoked from the Global I/O module through event or periodic trigger.
- Default sanity reports returns unprivileged data.
- Contact Support Team for any high level ERD of database/assistance in writing complex SQL based queries to meet individual requirements.
This chapter describes how to integrate the Cisco PAM data and actions with enterprise or third-party systems.

Contents

- Configuring URL Actions, page 14-2
  - Creating or Modifying URL Actions, page 14-3
  - Creating Automated Rules for URL Actions, page 14-7
  - Viewing URL Events, Alarms, and Logs, page 14-12
- Synchronizing Data Using Enterprise Data Integration (EDI), page 14-16
  - Before You Begin, page 14-16
  - Understanding Photo File Compression When Importing Personnel Records, page 14-17
  - Installing the EDI Licence and Desktop Application, page 14-18
  - Creating Active Directory Database Integration Projects Using EDI Studio, page 14-20
  - Creating SQL and Oracle Database Integration Projects Using EDI Studio, page 14-33
  - Importing, Starting, and Monitoring EDI Projects in Cisco PAM, page 14-41
- Accessing the SQL Database, page 14-49

Note

See also the Cisco Physical Access Control API Reference Guide for information on Web Services support.
Configuring URL Actions

URL actions allow you to trigger actions in external systems when alarms or events occur in CPAM. For example, URL actions can trigger the following in other systems:

- **Cisco Energywise:** 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 14-1).

**Figure 14-1  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 14-3
- Creating Automated Rules for URL Actions, page 14-7
- Viewing URL Events, Alarms, and Logs, page 14-12
Creating or Modifying URL Actions

To add or modify URL actions, complete the following instructions:

To do this

**Step 1** Select **URL Actions** from the Admin menu.

![URL Actions Menu]

**Step 2** Click **Add** to create a new action, or select an existing action and click **Edit**.

![URL Actions Table]
To do this

Step 3 Enter the basic properties in the URL Action window:

a. Name: enter a descriptive name.
b. Description: enter a short description of the rule.
c. Post / Get: select the method the listening server will implement.
d. Http / Https: Select the connection method. The Cisco PAM default for secure connections is to present a client certificate, and accept all secure certificates.
e. Enter the URL base.
   This is the URL of the system that will be triggered.
   For example: http://www.cisco.com
f. Select Enabled to enable or disable the action.

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. Enter the URL 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.
To do this

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>
Chapter 14      System Integration

Configuring URL Actions

To do this

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=text_sample & Event Attr=text_sample & EventAttr=text_sample & Device Address
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.

To do this

**Step 1** Select Global I/O from the Events & Alarms menu.

**Step 2** Click Add.
Chapter 14  System Integration

To do this

Step 3  
Enter a Name for the rule and select or deselect the Enabled checkbox.

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 occurs. Select Event and then click Edit Filter to select the event log code.

- **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.
Chapter 14  System Integration

Configuring URL Actions

To do this

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 14-2 for more information.

e. Click Save and Close.
Configure URL Actions

To do this

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 13-19.

- **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.
Chapter 14  System Integration

Configuring URL Actions

To do this

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**.
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 14-12
- Viewing Alarms for Failed URL Action, page 14-13
- Event and Alarm Response Codes for URL Actions, page 14-13
- Viewing Logs for URL Action Output, page 14-14
- URL Action Failure Due to Invalid Security Certificate, page 14-15

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 12-4 for more information.

Figure 14-2 URL Action Events
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 12-8 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 3-2.

**Step 2**
Select the Monitoring tab, and then select URL Log. Figure 14-4 shows the menu and sample log.

**Figure 14-4  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):

```java
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 Using the Web Admin Menus, Commands and Options, page 3-17 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 Using the Web Admin Menus, Commands and Options, page 3-17 for instructions to restart the server.
Synchronizing Data Using Enterprise Data Integration (EDI)

EDI is used to synchronize data from Active Directory, Microsoft SQL Server, MySQL and Oracle 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 14-16
- **Understanding Photo File Compression When Importing Personnel Records**, page 14-17
- **Installing the EDI Licence and Desktop Application**, page 14-18
- **Creating Active Directory Database Integration Projects Using EDI Studio**, page 14-20
- **Creating SQL and Oracle Database Integration Projects Using EDI Studio**, page 14-33
- **Importing, Starting, and Monitoring EDI Projects in Cisco PAM**, page 14-41
  - **Importing and Starting EDI Projects**, page 14-41
  - **Verifying EDI Projects (EDI Monitoring)**, page 14-43
  - **Modifying a Running EDI Project**, page 14-45
  - **Restarting a Failed EDI Project**, page 14-47
  - **Summary of EDI Administration Functions**, page 14-47

**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 3-44 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.
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 14-47 and Managing the Camera Inventory, page 15-28.

Stop any running EDI projects before upgrading the Cisco PAM appliance software. After the upgrade, you can restart the projects. See Importing and Starting EDI Projects, page 14-41 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.

Note: If upgrading from Release 1.0 or Release 1.1, you must also recreate the EDI projects using the EDI Studio application.

Note: Only personnel photos in the JPEG or JPG format are supported for import. In addition, the photos must be in RGB format. Other image formats are ignored when importing personnel data.

Understanding Photo File Compression When Importing Personnel Records

Photo files that are imported into the Cisco PAM personnel database can be a maximum of 750 kb per image. If a photo is larger than the defined maximum, the file is automatically compressed by Cisco PAM.

You can define the maximum file size for imported photo files using the System Configuration module. For example, if you enter a maximum file size of 500 kb, then any files larger than 500 kb will be automatically compressed when the personnel record is imported.

Note: Only personnel photos in the .jpg format are supported for import.

To set the maximum file size limit, do the following:

Step 1 Select System Configuration from the Admin menu.
Step 2 Select Cisco Settings on the left (Figure 14-5).
Step 3 In the field EDI personnel’s photo size limit, enter the maximum file size for the imported file.

- Enter a value, in kb, between 50 and 750.
- The default value is 250 kb.

Note: Any photo file larger than the specified size will be automatically compressed during the EDI import operation. A small loss of image quality may be noticeable in the compressed image.
Synchronizing Data Using Enterprise Data Integration (EDI)

Figure 14-5    Cisco Settings

Step 4  Click Save to save the changes.

Step 5  Log out and log back in to the Cisco PAM application to activate the changes (select Logout from the Options menu).

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.

Figure 14-6    Cisco PAM Licenses

Step 1  Install the EDI license on the Cisco PAM server. Figure 14-6 Shows the EDI license installed on a Cisco PAM server. See Using the Web Admin Menus, Commands and Options, page 3-17 for information to view the installed licenses or purchase and install new 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 14-7).

![EDI Driver]

**Figure 14-7**   EDI Driver

---

### Step 3

**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 14-8. You do not need to log on to the utility to download the software. The required version of Java is also installed, if necessary.

![Download EDI Studio]

**Figure 14-8**   Download EDI Studio

---

You can also log in to the Cisco PAM Server Administration utility and select **Cisco EDI Studio (JRE Required)** from the **Downloads** menu. See Using the Web Admin Menus, Commands and Options, page 3-17.

---

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.
f. Select **Cisco EDI Studio** from the shortcut on your desktop or from your Windows *Programs* menu.

---

**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 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.

---

**To do this**

**Step 1**

Select **Cisco EDI Studio** on your Windows PC. The Cisco Enterprise Data Integration window opens.

---

**Step 2**

Create a new Workspace.

a. Select **New Workspace** from the File menu. You can also right-click **Root** and select **New Workspace**.

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.
Chapter 14      System Integration

Synchronizing Data Using Enterprise Data Integration (EDI)

To do this

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**.

![New Project Template dialog box](image)
Synchronizing Data Using Enterprise Data Integration (EDI)

To do this

Step 5  Enter the Active Directory database parameters:

a. **Host name**: enter the IP address of the database server.

   Note  The Active Directory Hostname must be accessible from the Cisco PAM appliance network. For example, both systems should be on the same network.

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.

![Active Directory Source Parameters](image)

Note  The fields Search base, Login name, and Password are provided by your Active Directory administrator.

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.

![Test connection failed](image)

**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.
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).
   - Map emp_status to the appropriate AD attribute. For example, active or inactive. Consult your Active directory Admin for more info on this attribute.

   See also Notes for Mapping the AD and Cisco PAM User Attribute Names, page 14-24.

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 \textit{sn} for the last name, and another attribute \textit{givenName} for the first name. For example: of Mike Smith would include:

- \textit{sn}=Smith
- \textit{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 \textbf{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 \textit{cpam} user allows the Cisco PAM server to log in to the AD database. The \textit{sn} attribute defines the lastname, and the \textit{givenName} attribute defines the first name.

In addition, the Active Directory attribute \textit{department} is defined. This attribute is mapped to the Cisco PAM field \textit{govt_id}.
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.
To do this

Step 8

Define the Active Directory default database values.

For example, enter the following 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.

c. Enter the AD attribute used by your organization for each of the emp_status fields. For example, enter I for emp_status (inactive) or R for emp_status (retired) employees. CPAM supports status for active, inactive, on leave, retired, and terminated.

d. Click Next to continue.
To do this

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.
To do this

**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.
To do this

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.
Creating Custom Employee Status Values

The employee status (emp_status) attribute defines if a user is active or inactive. The fields supported by default are:

- emp_status (active)—the user account is active.
- emp_status (inactive)—the user account is inactive.
- emp_status (on leave)—the user account is inactive.
- emp_status (retired)—the user account is inactive.
- emp_status (terminated)—the user account is inactive.

If necessary, you can create additional employee status values. Each identifies the user account as either active or inactive. For example, an organization uses the value of 512 for Active and 514 for Inactive, but they also use an additional value 544 for an active user with an expired password. You can create this new active user status in cpam, and then enter the definition in EDI.

Procedure

Step 1

Enable the Employee Statuses module (disabled by default).

a. Select Profiles from the Users menu.

b. Double-click the user profile for the user who administers EDI projects.

You can also select the profile name and click Edit.

c. In the Edit - Profile window, select the Modules tab (Figure 14-9).

d. Expand the Advanced category.

e. Select Employee Statuses to highlight it.

f. Select the Allow access to module check box.

g. Click Save and Close.
Step 2  To display the new menu, logout of Cisco PAM and log back in.
   a. Choose Logout from the Options menu.
   b. Enter a username and password for a user assigned to the profile you just modified.
   c. Select Login.

Step 3  Select Employee Statuses from the Admin menu (Figure 14-10).
Step 4 Create a new employee status entry.
  
  a. Click **Add**.
  
  b. Enter the name of the new entry (Figure 14-11).
  
  c. Select **Active** if user accounts with this status should be active. Deselect **Active** if the user accounts should be inactive.
  
  d. Click **Save and Close**.

  **Figure 14-11 Employee Statuses Window**

  ![Employee Statuses Window](image)

  e. Verify that the new status appears and that the Active setting is true or false (Figure 14-10).
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 versions 10g and 11g
- 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 14-12.

Figure 14-12  EDI Studio: Cisco Enterprise Data Integration Window

Step 2  Create a 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.
Step 4  
Select a Project Template, as shown in Figure 14-15.

**Figure 14-15  EDI Studio: Choose Project Template**

![New Project dialog box](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 14-16.

Figure 14-16  EDI Studio: Enter Parameters for the Source Database

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 14-1**.
Table 14-1 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>&lt;br&gt;• <em>name</em>: (primary key) Name of the organization.&lt;br&gt;<strong>Department Data</strong>&lt;br&gt;• <em>name</em>: (primary key) Name of the department.&lt;br&gt;• <em>orgName</em>: (primary key) Organization name</td>
</tr>
</tbody>
</table>
Table 14-1 Required Fields for Data Mapping

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Required Fields</th>
</tr>
</thead>
<tbody>
<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</td>
</tr>
<tr>
<td></td>
<td>are: 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,</td>
</tr>
<tr>
<td></td>
<td>on_leave, retired, and terminated. If your organization has additional</td>
</tr>
<tr>
<td></td>
<td>employee status codes, such as Active Password Expired, you can manually</td>
</tr>
<tr>
<td></td>
<td>add those codes to the bottom of the list: enter the CPAM Value in the left</td>
</tr>
<tr>
<td></td>
<td>column (it must be one of the 5 supported emp_status attributes, as shown),</td>
</tr>
<tr>
<td></td>
<td>and then enter your organization’s code in the right column.</td>
</tr>
<tr>
<td></td>
<td>• The emp_type is not required, but has the following valid values: contractor,</td>
</tr>
<tr>
<td></td>
<td>employee, employee_full_time, employee_part_time, intern, other, vendor, and</td>
</tr>
<tr>
<td></td>
<td>visitor. emp_type is a type of employee.</td>
</tr>
<tr>
<td></td>
<td>Note The Region and Nationality fields be values already defined in system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Credential (Badge Records)</th>
<th>Note</th>
<th>The primary keys are badgeId and facilityCode.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• badgeId: (primary key) The badge ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• credTemplateId: Use this field to assign the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>parameters from a badge template in Cisco PAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to imported badges. This option is used when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>importing badges into Cisco PAM for the first</td>
</tr>
<tr>
<td></td>
<td></td>
<td>time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, create or edit a badge template in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco PAM as described in Configuring Badge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Templates, page 9-28. This template can contain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>settings for fields such as access policy,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>facility code, badge type, watch level, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>effective date. Enter the name of the badge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>template in the Source Attribute Value column</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for credTemplateId. For example: KeyPad_BCD4,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>26BitWiegandCT, 26BitWiegandKeyPadCT, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• facilityCode: (primary key) The facility code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• activationDate: Activation date for the badge.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• expirationDate: Date the badge expires. This</td>
</tr>
<tr>
<td></td>
<td></td>
<td>date must be greater than the activation date.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• validity: The valid values are: active, inactive, destroyed, lost, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stolen.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• role: The user’s role in the organization. The</td>
</tr>
<tr>
<td></td>
<td></td>
<td>valid values are: employee, contractor, vendor,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 14-17).

**Figure 14-17  EDI Studio: EDI Extension**

![EDI Extension File Selection](image)

Step 9  Choose a schedule to specify how often data will be synchronized, as shown in Figure 14-18.

**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 14-12 on page 14-33).

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 14-41.
Importing, Starting, and Monitoring EDI Projects in Cisco PAM

This section includes the following information:

- Importing and Starting EDI Projects, page 14-41
- Verifying EDI Projects (EDI Monitoring), page 14-43
- Modifying a Running EDI Project, page 14-45
- Restarting a Failed EDI Project, page 14-47
- Summary of EDI Administration Functions, page 14-47

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

**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\
To do this

Step 3

Once the file is uploaded, click **Start**.

Step 4

Select the start time:

- 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.

**Note**  Active Directory EDI projects restart when the Cisco PAM appliance is stopped and restarted. All other projects will run on their normally scheduled time. If you do not want Active Directory projects to run after a server restart, stop the project(s) before restarting the server.

Step 5

Verify that the project is started.

**Note**  Active Directory EDI projects restart when the Cisco PAM appliance is stopped and restarted. All other projects will run on their normally scheduled time. If you do not want Active Directory projects to run after a server restart, stop the project(s) before restarting the server.
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 14-19).

![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 14-20):

- **Interface**: this occurs when the Cisco PAM server connects to the remote data source 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.
Synchronizing Data Using Enterprise Data Integration (EDI)

Figure 14-20  EDI Monitoring Window

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 14-20 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 14-21).

Figure 14-21  EDI Error Monitoring Menu

Step 4  The Error Monitoring window displays entries for each failed record, as shown in Figure 14-22. 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.

Figure 14-22  EDI Error Monitoring
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 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.

**Step 5** Once the cause of the error is determined, modify the project. See Modifying a Running EDI Project, page 14-45. If an EDI data integration project fails, identify and resolve the problem, and then complete the instructions in Restarting a Failed EDI Project, page 14-47.

---

**Modifying a Running EDI Project**

To modify an EDI project that is running, do the following:

**Step 1** Stop the project:

  a. Select EDI Administration from the Admin menu.
  b. Select the project and click Stop.

**Step 2** Click Export to save the .jar project file. Save the file in the in the default EDI project directory on your PC:

   C:\Program Files\Cisco Systems\EDI Studio\workspaces\Project_Folder\projects\.

**Step 3** Edit the project in EDI Studio:

  a. Open the EDI Studio application on your PC.
  b. Select the project from the left window, and click Edit at the bottom of the detail window.
  c. Edit the settings as necessary and click Save.

**Tip** For field descriptions, refer to Creating Active Directory Database Integration Projects Using EDI Studio, page 14-20.
*Figure 14-23  Editing EDI Projects*

![Image of Cisco Enterprise Data Integration interface]

**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 14-24*):

*Figure 14-24  EDI Project Start Time*

![Image of EDI Project Start Time window]

- 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 14-47**.

**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 9-14** for more information.

- The project mapping is incorrect. See **Modifying a Running EDI Project, page 14-45** 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 14-41**.

**Summary of EDI Administration Functions**

- **Column Descriptions**
- **EDI Administration Functions, page 14-48**

**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>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recent Start Time</td>
<td>The most recent time that data integration began for the project.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies if the project is running, stopped, or scheduled.</td>
</tr>
<tr>
<td>Last Run Date</td>
<td>The date of project was last executed (successful and unsuccessful attempts).</td>
</tr>
<tr>
<td>Run Count</td>
<td>The number of times the project has been run (successful and unsuccessful attempts).</td>
</tr>
<tr>
<td>Success Run Count</td>
<td>The number of times the project has been successfully run.</td>
</tr>
</tbody>
</table>

### EDI Administration Functions

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>Active Directory EDI projects restart when the Cisco PAM appliance is stopped and restarted. All other projects will run on their normally scheduled time. If you do not want Active Directory 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

The CPAM SQL database can be accessed by 3rd party Time and Attendance (T&A) systems to view personnel, time and attendance, and user tracking data.

The database views are not visible by default. Use the MySQL Query browser to display the database views.

Caution
Do not modify the SQL tables. Use the following instructions to browse the tables only. Changing the tables or data can result in CPAM errors or system failures.

To view the CPAM SQL database, complete the following procedure:

Step 1
Contact Cisco technical support to obtain the database username, password, host and schema, if necessary.

Step 2
Install and launch the MySQL Query Browser, and enter the server and login information supplied by Cisco technical support.

Step 3
In the Schemata pane (right column), expand the vxdb entry and scroll down to the bottom of the list to display the entries for personnel_vw, time_attendance_vw, and user_tracking_vw (Figure 14-25).

Figure 14-25 MySQL Query Browser

Step 4
To view the database entries:
   a.  Double-click on the table name to enter a query in the Query field.
   b.  Click the Execute button
The data is shown in the browsing area.
See the following for examples of the SQL data views:

- Personnel, page 14-50
- Time and Attendance, page 14-51
- User Tracking Data, page 14-52

### Personnel

The Personnel view (Figure 14-26) provides personnel information such as first name, last name, user id, personnel id, photo image, and the image type.

**Figure 14-26  Personnel**
Time and Attendance

The Time and Attendance view (Figure 14-27) provides information on user entry and exit through 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 14-27  Time and Attendance
User Tracking Data

The User Tracking view (Figure 14-28) 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 14-28  User Tracking
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 archived 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 an archived 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.

Camera Manager in Cisco PAM 1.4.1

If the profile enhancement feature is set in the system configuration settings (Data Entry/Validation - Login, page 17-9), the following changes are impacted in this module:

- The camera drivers present in the user’s hierarchical location alone is displayed.
- The location-restricted users can view all cameras in the camera manager, but can access cameras of their location only.
- The cpamadmin assigns the location of the cameras to a location-restricted user.
- When a 7X camera driver is associated to a specific location, as a location-restricted user you will be able to view your set of privileged cameras under the System driver that is populated only in your location i.e other location-restricted users cannot view the System driver.
- You can install Cisco VSM Camera Driver either 6X or 7X version. Both versions are supported in Cisco PAM 1.4.1. However, you can configure and associate the camera devices to only one of them at a time. The following are the differences between the 6X and the 7X versions:

<table>
<thead>
<tr>
<th>Changes</th>
<th>New Cisco VSM Camera Driver 7X</th>
<th>New Cisco VSM Camera Driver 6X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Changes</td>
<td>To Setup Cisco VSM the server name, username and password is given.</td>
<td>To Setup Cisco VSM the server name, username and password is not given</td>
</tr>
<tr>
<td>Architectural changes</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
In 7X version, if a camera is removed from the VSM configuration then it is deleted completely from Cisco PAM provided the camera is not associated with any devices/map/CCTV Camera Arrangements/uncleared Alarms.

In addition, both the 6X and 7X Camera Manager versions can display multiple live video streams in a grid arrangement, allowing a user to monitor multiple cameras at once.

Tip

In 6X version 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 15-28.

For more information on Cisco Video Surveillance Manager, go to the Cisco Network-Centric Video Surveillance Products website.

If you wish to switch to any of the VSM versions, ensure that you have removed all camera devices and drivers from the Cisco PAM.

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 15-4
  - Configuring the Camera Driver, page 15-4
  - Associating Cameras with Doors and Devices, page 15-8
  - Installing the Cisco VSOM Video Client Desktop Application, page 15-11
- Viewing Video, page 15-13
  - Viewing Live Video in a Grid Arrangement -VSM 7X, page 15-17
  - Viewing Video for an Event, page 15-19
  - Viewing Event on a VSM Camera Driver 6X, page 15-20
  - Viewing Event on a VSM Camera Driver 7X, page 15-24
- Managing the Camera Inventory, page 15-28
- Updating the Camera Inventory, page 15-28
• Deleting the Cisco VSM Cameras, page 15-30
• Deleting Individual Cameras, page 15-35
• Recording Motion Events from Cisco VSM Cameras, page 15-37
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 15-4
- Associating Cameras with Doors and Devices, page 15-8
- PC Workstation Requirements for Live Video Viewing, page 15-11
- Installing the Cisco VSOM Video Client Desktop Application, page 15-11

Configuring the Camera Driver

To Add the VSM Camera Driver to enable video sharing and playback with the Cisco VSM system:

To do this

Step 1  Select **Hardware** from the Doors menu.

Step 2  Right-click the **Driver Manager** and select the appropriate camera driver version:

- New Cisco VSM Camera Driver
- New Cisco VSM Camera Driver 7X
To do this

Step 3  Enter the driver name in the properties window. For example: Cisco VSM Camera Driver7x.

Note  Verify that the Enabled checkbox is selected (default).

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 15-11.
- **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.

Tip  If it is 7x version, the Maximum player instances number should be from 1 to 4.

Step 5  Click Save and Close to close the window.
Enabling Video Monitoring

**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**.

**Step 7**
If you are using VSM Camera Driver 7x, do the following:

a. Right-click the **Cisco VSM Camera Driver 7X** and select **Setup Cisco VSM**.

**Tip**
These fields are disabled if the camera driver was previously set up and includes cameras.

b. Enter the **Server Name**, **Username** and **Password** in the VSM Config screen.

c. Click **OK** to save the changes and close the window.
To do this

Step 8 If you are using VSM Camera Driver 6X, do the following:

a. Right-click the Cisco VSM Camera Driver and select Setup Cisco VSM.

   **Note** Do not change the database name or port number once they are configured.

b. Enter the **Database name**: the name of the Cisco VSM database. The default is bas.

c. Enter the **Server name**: the name or IP Address of the Cisco VSM database server.

d. Enter the **Port number**: the port number for the Cisco VSM database server. The default is 3306.

e. Click OK to save the changes and close the window.

![Cisco VSM Configuration Parameters](image)

Step 9 Right-click the VSM Camera Driver and select **Synchronize with Cisco VSM** to populate Cisco PAM with the Cisco VSM cameras.

**Note** For 7x version follow the same step to populate the Cisco PAM with the Cisco VSM cameras.
Chapter 15  Video Monitoring

Enabling Video Monitoring

To do this

Step 10 Verify that the Cisco VSM cameras appear as children of the Camera Driver.

NOTE

The Cisco PAM client must run on Windows 7 platform to view video from the cameras under the 7X driver.

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.

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.

NOTE

The Cisco PAM client must run on Windows 7 platform to view video from the cameras under the 7X driver.
To associate a camera with a door or device, do the following:

**To do this**

**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 be associated to more than one 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 15-28.
Enabling Video Monitoring

**To do this**

**Step 3** (Optional) You can also associate cameras with devices by editing the camera properties.

a. Double-click the camera in the Video or Hardware windows.
   
The **Edit - Camera** window opens.

b. Select the **Devices in View** tab.

c. Check the devices to be associated with the camera.
   
   Associated cameras are listed in the far-right table.

d. 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** 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.

**Note** Follow the same steps to associate cameras with devices if you have launched a 7X camera driver.
For more information about configuring Cisco VSM cameras, see the Cisco Video Surveillance Manager User Guide.

**PC Workstation Requirements for Live Video Viewing**

Table 15-1 describes the recommended baseline configuration for a monitoring workstation that displays video from Cisco Video Surveillance Manager (VSM) 6.3. A workstation with this configuration was used to determine the recommended maximum video loads. This configuration assumes that the workstation is dedicated to video. Running other software, such as firewalls, antivirus applications, CD/DVD burning utilities, and general-purpose applications will reduce the quality of the user experience.

<table>
<thead>
<tr>
<th>Workstation Attribute</th>
<th>Baseline Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Windows 7 64-bit, SP3</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel 950 i7 Core - 3.07 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>6 GB DDR3</td>
</tr>
<tr>
<td>Graphics</td>
<td>NVIDIA GeForce GTX260 896MB PCIe</td>
</tr>
<tr>
<td>Cisco VSOM configuration</td>
<td>VMR mode enabled</td>
</tr>
<tr>
<td>Browser</td>
<td>Microsoft Internet Explorer 7</td>
</tr>
<tr>
<td>Network connection</td>
<td>Gigabit Ethernet (GigE) network connection required</td>
</tr>
<tr>
<td>Display configuration</td>
<td>Single monitor</td>
</tr>
</tbody>
</table>

For related information, see Video Surveillance Monitoring Workstation Recommended Baseline Specification, which is available here:


**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 15-11.

**Step 2** Configure the VSM Camera Driver, as described in Configuring the Camera Driver, page 15-4.

**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 archived 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 Video for an Event, page 15-19

Viewing Live Video in a Grid Arrangement -VSM 6X

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.

To do this

Step 1
Select Camera Manager from the Events & Alarms menu, in the Video sub-menu.

Step 2
Click the Layouts menu and select a layout that includes the number of cameras you want to view.
To do this

**Step 3**  
(Optional) You can also select a pre-defined arrangement.

**Step 4**  
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.
To do this

**Step 5** (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**.
To do this

**Step 6**  
(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.

**Step 7**  
(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.
Chapter 15  Video Monitoring

Viewing Video

Viewing Live Video in a Grid Arrangement - VSM 7X

To view live video in a grid arrangement while using VSM Camera Driver 7X, do the following:

To do this

Step 1

Select Camera Manager 7X from the Events & Alarms menu, in the Video sub-menu.
To do this

**Step 2** Click the **Layouts** menu and select a layout that includes the number of cameras you want to view.

![Layout Menu](image1)

**Step 3** Select the cameras and click **Submit** to view the videos of the selected cameras.

![Camera Selection](image2)

**Note** Based on the system configuration settings (see Data Entry/Validation - Login, page 17-9), only cameras that are assigned to your user profile, location, and sub location will be listed for selection.
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 archive video for the event (if an archive feed has been configured for the camera). To define how much video to display before and after events occur, see the “Defining the Duration of Event Video Recording” section on page 15-27. For example, video event archives can begin 30 seconds before the event occurred, and continue 20 seconds after the event occurred. If the archive is not available, an error message appears (for example, if the event video occurred previous to the archive window).

You can also view live video from the camera that captured the event.

Event video includes the following options:

- **View Live Video**—view live video from the camera associated with the event.
- **View Event Video**—view the video archive for the event.
- **View Live and Event Video**—open both live and archive video windows.
- **Show Camera Arrangement**—displays all camera arrangements that include the camera associated with the event. If the camera is not included in any camera arrangements, then this option is disabled (grayed out).

**Usage Notes**

- 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.

- Beginning with Release 1.3.0, you can assign cameras to a location. The camera location allows you to configure event policies for a group of cameras based on location. For example, you can suppress event and alarm notifications of motion events from cameras in a high traffic area during normal business hours. To assign a location to a camera:
  - Select **Camera Manager** from the **Events & Alarms** menu, in the **Video** sub-menu.
  - Right-click a camera name.
  - Click the **Location** tab.
  - Select a location from the Hierarchical Location menu.
  - Click **Save and Close**.

---

**Tip**

You can also edit the camera location using the Hardware module. Right-click a camera name and choose **Edit**. Select the Location tab and choose a Hierarchical Location from the drop-down menu.
Viewing Event on a VSM Camera Driver 6X

To view event on a VSM camera driver 6X, do the following

**To do this**

**Step 1**
Select Events from the Events & Alarms menu.

**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.
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 a view option:
  - **View Live Video**—view live video from the camera associated with the event.
  - **View Event Video**—view the video archive for the event.
  - **View Live and Event Video**—open both live and archive video windows.
  - **Show Camera Arrangement**—displays all camera arrangements that include the camera associated with the event. If the camera is not included in any camera arrangements, then this option is disabled (grayed out).

---

**Tip** The video and camera options appear only if video is available for that event.
To do this

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 a viewing option: View Live Video, View Event Video, View Live and Event Video, or Show Camera Arrangement.

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

**Step 6**  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**.

**Tip**  The commands are the same commands available by right-clicking the device in the Hardware module.

**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.
Viewing Event on a VSM Camera Driver 7X

To view events on a VSM Camera Driver 7X, do the following:

To do this

**Step 1** Right-click the camera and select View Live Video.

**Step 2** The live video window opens.
To do this

Step 3
Alternatively you can also view Live video from Events and Alarms->Monitoring->Events and click any camera event.

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 a view option:

- **View Live Video**—view live video from the camera associated with the event.
- **View Event Video**—view the video archive for the event.
- **View Live and Event Video**—open both live and archive video windows.
- **Show Camera Arrangement**—displays all camera arrangements that include the camera associated with the event. If the camera is not included in any camera arrangements, then this option is disabled (grayed out).

**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 a viewing option: **Live Video**, **Event Video**, **Live and Event Video**, or **Arrangement**.

**Tip** The video and camera options appear only if video is available for that event.
To do this

**Step 5** When viewing recorded event video, use the controls under the video display to fast forward, rewind, pause, or play the clip.

<table>
<thead>
<tr>
<th>Tip</th>
<th>Press the Rewind or Forward buttons multiple times to increase the speed. You can playback or rewind video at 1x, 2x, 3x, or 4x.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip</td>
<td>If it is an event video, a time bar is displayed.</td>
</tr>
</tbody>
</table>
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 15-1 System Configuration Events/Alarm Window*

**Step 2** Enter the following:

<table>
<thead>
<tr>
<th>Length of video to display pre-event</th>
<th>The number of seconds of video that are included before the event occurred.</th>
</tr>
</thead>
<tbody>
<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** Log out and log back in to the Cisco PAM application to activate the changes (select **Logout** from the Options menu).
Managing the Camera Inventory

- Updating the Camera Inventory, page 15-28
- Deleting the Cisco VSM Cameras, page 15-30
- Deleting Individual Cameras, page 15-35

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, regardless of the configured run frequency. It may take up to a minute to synchronize the inventory. 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

**Step 1**

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.

Tip

These fields are disabled if the camera driver was previously set up and includes cameras.
To do this

Step 2 Right-click the Cisco VSM Camera Driver and select Synchronize with Cisco VSM. This command manually synchronizes Cisco PAM with the Cisco VSM inventory.

Step 3 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

Step 4 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 15-28.

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**

**Step 1** Remove all camera references from the Camera Manager layout arrangements, and from any Graphic Map.

a. Select Camera Manager from the Events & Alarms menu, in the Video sub-menu.

b. Select each arrangement, and click and drag the title bar of each camera off the grid.

tip You can also delete the arrangement to remove the camera references.

c. Click Save.

d. Select Graphic Map Editor from the Admin menu.

e. Select any maps that include cameras.

f. Right-click each camera icon and select Remove Device Icon.

tip You can also delete the entire map to remove the camera references.

g. Click Save.

For more information, see the following:

- Graphic Map Editor, page 12-44.
Managing the Camera Inventory

To do this

**Step 2**

a. Enable the **Delete All Cameras** command and the **Allow deletion of devices with events** option in the System Configuration settings.

b. The **Delete All Cameras** command only appears after you enable it in the System Configuration window.

c. The **Delete All Cameras** command will fail to complete if you do not enable the **Allow deletion of devices with events** option.

d. Select **System Configuration** from the Admin menu.

e. Select the **Cisco Settings** sub-menu.

f. Select the check-box for **Display Delete All Cameras command on the camera driver**.

g. Select the **Miscellaneous** sub-menu.

h. Select the check-box for **Allow deletion of devices with events**. This allows cameras with associated events to be deleted from Cisco PAM.

i. Click **Save**.

j. To activate the change, stop and then restart the Cisco PAM server. See Using the Web Admin Menus, Commands and Options, page 3-17 for instructions.
To do this

Step 3
Delete the cameras from Cisco PAM:

a. Open the Hardware module.

b. Right-click the Cisco VSM Camera Driver.

c. Select the **Delete All Cameras** command.

d. Click **OK** when the warning message appears. All events, alarms and audit messages for the cameras will be deleted.

Step 4
Verify that the deletion was successful.

- 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**.

- If the action fails, some cameras are still displayed under the camera driver. If this occurs, do the following:
  a. View the event **Description** and **Data** fields to locate the issue.
  
     — The event is: “Cisco VSM Camera Driver command failed: Reset Cameras”.
  
     — Open the event to view the event **Data** and identify the camera(s).
  
     For example:
  
     “References found; Analog Camera - WV-CP484- Graphic Maps: map1-256map5-2.6MB,B10-3, map4,B28-1, Analog Camera - WV-CP484- Camera Arrangements: one.”

  b. Locate and delete the remaining camera references from Camera Manager and the graphic maps (see **Step 1**).

  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.

  d. Invoke the **Delete All Cameras** command again, as described in **Step 3**.
To do this

Step 5

After the **Delete Cameras** command is successful, restart the camera driver: right-click the **Cisco VSM Camera Driver** and select **Restart**.

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
Deleting Individual Cameras

To delete individual cameras, do the following:

**Tip**  See Deleting the Cisco VSM Cameras, page 15-30 for information on a single command to delete all cameras.

**Step 1**  Remove the camera associations (for the camera to be deleted) from the Camera Manager arrangements, and from any Graphic Map.

**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.

  g.  Select the **Miscellaneous** sub-menu.

  a.  Select the check-box for **Allow deletion of devices with events**. This allows cameras with associated events to be deleted from Cisco PAM.
b. Log out and log back in to the Cisco PAM application to activate the changes (select Logout from the Options menu).

**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.

**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 7-25 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.

Tip
See the Cisco Video Surveillance Manager User Guide for more information.

Procedure

Step 1
Configure the Camera Driver as described in Configuring the Camera Driver, page 15-4. Skip to Step 2 if the camera driver is already configured.

Step 2
Install the 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 3-44.
- Skip to Step 3 if the API license is already installed.

Step 3
Verify that Cisco PAM Web Services are enabled:

Note
Skip to Step 4 if Cisco PAM Web Services are already enabled.

a. 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 3-2.

b. Select the Monitoring tab and then select Status.

Note
The Status window appears by default. This window also appears when you first log on.
c. Verify that the Web Service API service is Enabled (Figure 15-2).

**Figure 15-2  Web Service API Status**

![Cisco PAM Server Administration](image)

The message Web Services license not applied appears if the API license is not installed. You must purchase and install the API license to record start motion and stop motion events. See Step 2.
Step 4  (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 15-3.

   Figure 15-3  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 5  Identify and record the Camera ID, as shown in Figure 15-4.
The Camera ID is used in the URL used to call the event, as described in Step 6.
   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 6 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 15-5).

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:
   
   - **cpam-ip-addr**: the IP address of the Cisco PAM server.
   - **number**: the **cameraId** number recorded in Step 5. For example: 65.
   - **type**: the **eventType**. For example: `CB.MOTION_START` or `CB_MOTION_STOP`
   - **time_value**: the **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.

**Figure 15-5**  **Enable URL Notification in the Cisco VSOM Events Configuration Page**

---

**Step 7** 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 12-4.
Figure 15-6 shows an example of a **Camera Motion Start** event. Double-click the event entry for additional details.

*Figure 15-6  Camera Events in Cisco PAM*
Triggering Camera Actions and Video Recording in Cisco VSM

Events in Cisco VSM can use a *soft trigger* to perform an action (such as adjusting a camera PTZ setting). The soft trigger is activated when Cisco VSM receives a URL from an external system, such as CPAM.

For example, when a door is forced open, a Door Forced Open event is generated and a URL is sent to Cisco VSM. Cisco VSM then executes actions based on that URL, such as panning the camera and sending and creating an archive. The process works as follows:

1. Create a event in Cisco VSM, and choose the *Enable Soft Trigger* option. A URL used to trigger the event is automatically generated and displayed.
2. In CPAM, create a URL action using the Cisco VSM URL that was automatically generated when you created the VSM soft trigger.
3. In CPAM, create an automation rule (Global I/O rule) that triggers the URL action when a *door forced open* event occurs.
4. CPAM sends the URL to Cisco VSM.
5. When Cisco VSM receives the URL, the camera pans and a video archive is created.

*Figure 15-7* illustrates this example.

**Figure 15-7  Soft Trigger Event in Cisco VSM**

> **Tip**

See the *Cisco Video Surveillance Manager User Guide* for instructions to create Cisco VSM soft triggers.
VoIP Integration

The integration of VoIP phone to Cisco PAM enables users to grant access to doors through the VoIP phone. This new feature of Cisco PAM allows the entry of personnel without badges. The VoIP integration does not require any configuration on the Cisco PAM. The Cisco PAM user receives the access request from the personnel/employees, enquires the credentials and grants them access through the VoIP phone.

VoIP phone integration to Cisco PAM is achieved by the following processes:

- Creating a phone service in Cisco Unified Call Manager (CUCM) and
- Subscribing a service to a VoIP phone.

Contents

- Creating a phone service in CUCM, page 16-2
- Subscribing a service to a VoIP Phone, page 16-5
Creating a phone service in CUCM

By creating a service in CUCM, you establish a link between the Cisco PAM and CUCM. The Cisco PAM IP is given while creating the service. The services can be created for single door or multiple doors in Cisco PAM. You need to ensure that the URL is validated before creating a service.

For example, if you paste the below URL in your browser to list all doors,

http://10.78.177.196/IPPhoneManager.jsp?UserName=cpamadmin&pass=cisco&method=authenticate

The following page with the URL is displayed in your screen, else the URL is incorrect.

![Validating the URL](image)

**Procedure**

To create a phone service, do the following:

1. **Go to the CUCM administration page.**
2. **Choose Device -> Device Settings -> Phone services.**
Step 3  Click Add New to create a new service.
  - You can also modify existing services.

Step 4  Enter the details in the IP Phone Services Configuration window.

Note  Enter the Cisco PAM IP in the The Service URL field. You can give an url to display all doors or a static url that will display specific doors. Ensure that you add the unique id of the door in the url if it is for static door configuration.

Tip  To configure for a single door, use the following url:
http://ip_address_of_cpam/QuickUnlock.jsp?UserName=<cpamadmin>&pass=<password_for_cpamadmin>&method=authenticate&resourceId=<Door_Unique_ID>&resourceType=door
Creating a phone service in CUCM

Step 5  Click Save. The service is created.

Additional Information

Cisco PAM supports three different URL's. You can configure any one of the below URLs based on your requirement.

**URL 1: Just the URL**

http://<ip_address_of_cpam>/IPPhoneManager.jsp

Use the above URL to create a service without username and password to display all doors. Once configured, the user is requested for the user credentials for each access.

**URL 2: URL with Username and Password:**

http://<ip_address_of_cpam>/IPPhoneManager.jsp?method=authenticate&UserName=<cpamadmin>&pass=<password_for_cpamadmin>

Use the above URL to create a service with username and password to display all doors. Once configured, the user can select a door and grant access without giving the user credentials each time.

Use case example for URL 2: For a receptionist in a busy school/university, if the number of keystrokes necessary to unlock a door at the phone are too many, then you can pre-configure the URL with their (receptionist) Username and the Password.

**URL 3: Quick unlock: Just one click to unlock/grant access to the door:**

http://<ip_address_of_cpam>/QuickUnlock.jsp?method=authenticate&UserName=<cpamadmin>&pass=<password_for_cpamadmin>&resourceId=<Door_Unique_ID>&resourceType=door
More Information on the URL’s

For quick unlock of a door:
http://ip_address_of_cpam/QuickUnlock.jsp?UserName=<cpamadmin>&pass=<password_for_cpamadmin>&method=authenticate&resourceId=<Door_Unique_ID>&resourceType=door

Configure the above URL as a service and name it “Door name to be unlocked”. Select the Service and the door will unlock, you will see the user friendly message on the phone.

To retrieve Resource ID:
http://ip_address_of_cpam/IPPhoneManager.jsp?method=authenticate&UserName=cpamadmin&pass=cpam

Go to the above URL to see the list of doors and select the door to configure as the individual door.

To authenticate username and password:
http://ip_address_of_cpam/IPPhoneManager.jsp?method=authenticate&UserName=cpamadmin&pass=cpam

Subscribing a service to a VoIP Phone

These steps enable you to subscribe a service to the VoIP phone. Once subscribed, the doors are displayed on the Phone UI. The user can now grant access to doors displayed on the phone UI

Note
To Configure VoIP phone to CUCM contact the CUCM Admin.

Procedure

Step 1  Go to Device->Phone in the CUCM admin Page. The Find and List Phones window appears.

Step 2  Select and click a specific VoIP phone from the list. The Phone configuration window appears.

Figure 16-4  Selecting a VoIP Phone

Step 3  Choose Subscribe/Unsubscribe Services from Related Links and click GO.
Chapter 16  VoIP Integration

Subscribing a service to a VoIP Phone

**Figure 16-5  Subscribed/Unsubscribed Services**

**Step 4**  Select a Service from the drop down list. Click **Next**.

**Figure 16-6  Select a service**

**Step 5**  Click **Subscribe**. The service is now subscribed to the phone and is listed under **Subscribed Services**.
Chapter 16  VoIP Integration

Figure 16-7  Service Subscribed

To subscribe for more services, Click **Subscribe a New Service** link in the subscribed services.

**Step 6**
Click **Save** and close the window. The service is subscribed now.

To Display the service on the VoIP phone, follow the steps below:

**Step 7**
Click **Add a new SURL** under Associate Information in the Phone Configuration window.

Figure 16-8  Add a new SURL
Step 8 Select the service to configure the service URL button.

Figure 16-9 Configure Service URL button

Step 9 Click Save. The service is listed in the VoIP phone.

Step 10 In the VoIP phone, click the button next to the service. The user credentials are requested.

Step 11 Enter the **Username** and **Password** and click **Submit** to display the door(s).

Figure 16-10 User Name and Password

Step 12 Press the button next to the selected door.

- The services are displayed based on user profile. Only doors assigned to the user login will be displayed.
For an admin user eg: Cisco PAM admin, all doors will be displayed.

**Step 13**

If the credentials are true, the following message is displayed.
- Successfully granted access on Door_8(name of the door).
If the credentials are false, the following message is displayed.
- Authentication failed.

**Note**
- If you have configured a list of doors to a service, you have to select the door from the list displayed on the phone.
- The VoIP phone displays the list of doors in the alphabetic order. The doors are displayed in any of the states like “UNKNOWN, UP, DOWN, MISMATCH”

**Step 14**
The events are displayed in Cisco PAM under **Events and Alarms->Monitoring->Events**.

### Limitations
- A VoIP phone can support up to display of 100 doors. If a server has more than 100 doors then you need to configure the remaining doors as a static URL.
- A disabled door will not be available in the list of doors displayed on the VoIP phone.
System Configuration Settings

This chapter describes the system-wide site settings available in the System Configuration module. In Cisco Physical Access Manager 1.4.1 release, the System Configuration module includes additional settings through which an user profile can be associated to a location hierarchy. This feature allows users to control or execute actions on locations and sub-locations mapped to their user profile. See Data Entry/Validation - Login, page 17-9

Note
We recommend restricting access to the System Configuration module to administrators only.

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 17-1).
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 Log out and log back in to the Cisco PAM application (select Logout from the Options menu).

Note
Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select Logout from the Options menu). For some settings in the Cisco Settings window, you must restart the Cisco PAM appliance. See the “Cisco Settings” section on page 17-23 for more information.

Contents

- LDAP Settings, page 17-3
- Event/Alarms Settings, page 17-5
- Data Entry/Validation - Personnel Settings, page 17-6
- Data Entry/Validation - Badge Settings, page 17-8
- Data Entry/Validation - Login, page 17-9
- Password Policy Settings, page 17-11
- Custom Device Fields Settings, page 17-13
- Custom Badge Fields, page 17-14
- Personnel ID Number Generator, page 17-16
- PIN Generator, page 17-17
- Card Number Generator, page 17-18
- Support Contact Information, page 17-19
- Miscellaneous Settings, page 17-20
- Cisco Settings, page 17-23
LDAP Settings

The LDAP options (Figure 17-1) include login validation settings required to use the Lightweight Directory Access Protocol. See Table 17-1 for field descriptions.

For more information, see Configuring LDAP User Authentication, page 5-12.

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 17-1 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:// Example: ldap://192.168.1.1</td>
</tr>
</tbody>
</table>
### LDAP Settings

Note

Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

#### Table 17-1  System Configuration LDAP Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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: <code>cn=Users,dc=my-domain,dc=com</code>.</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: <code>dc=my-domain,dc=com</code>.</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 <strong>simple</strong>.</td>
</tr>
<tr>
<td>JNDI factory</td>
<td>Advanced setting that generally should be left unchanged as <code>com.sun.jndi.ldap.LdapCtxFactory</code>.</td>
</tr>
</tbody>
</table>
Event/Alarms Settings

Use the Events/Alarms tab (Figure 17-2) to define how alarms are managed by the system, and how much video is recorded for events.

Figure 17-2   Events/Alarm Settings

Table 17-2 describes the Event and Alarms settings.

Table 17-2   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>
</tbody>
</table>
**Table 17-2  System Configuration Alarm Fields (continued)**

<table>
<thead>
<tr>
<th>Field</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>
<tr>
<td>Repeat alert sounds</td>
<td>Defines if alarms sounds are played only once, or repeated.</td>
</tr>
<tr>
<td>Show audit records in events</td>
<td>Lists the audit records of events.</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).

**Data Entry/Validation - Personnel Settings**

**Figure 17-3  Personnel Data Entry Settings**
Table 17-3 describes the Data Entry/Validation - Personnel settings.

Table 17-3   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 9-56.</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>
<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>
<tr>
<td>Use CSV personnel import wizard</td>
<td>Enable the CSV import wizard in the personnel module. The CSV import wizard allows operators to add personnel to Cisco Physical Access Manager using a CSV file. See Importing Personnel Records Using a Comma Separated Value (CSV) File, page 9-16.</td>
</tr>
</tbody>
</table>

Note

Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select Logout from the Options menu).
Data Entry/Validation - Badge Settings

Figure 17-4  Badge Data Entry Settings

Table 17-4 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>
</tbody>
</table>
Data Entry/Validation - Login

The profile enhancement feature is set in this page. This configuration setting facilitates the administrator to link a user profile to hierarchical location.

Table 17-4 Data Entry/Validation - Badge Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 9-47.</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 - Login

The profile enhancement feature is set in this page. This configuration setting facilitates the administrator to link a user profile to hierarchical location.

Figure 17-5 Data Entry/Validation - Login Settings

Table 17-5 describes the Data entry Validation - Login Settings
Table 17-5  Data entry Validation - Login Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login may not have a profile from a different partition</td>
<td>Not supported in this version</td>
</tr>
<tr>
<td>Profile may not restrict by hierarchial location</td>
<td>select this check box if you do not want user profiles to be restricted by hierarchial locations</td>
</tr>
<tr>
<td>Allow profile to be bound to hierarchial locations per assignment</td>
<td>select this check box if you want user profiles to be restricted by hierarchial locations</td>
</tr>
</tbody>
</table>

On setting these changes, the system configuration settings changes i.e a user is able to associate a location to a login thereby granting privileges to the login user for devices in that location. Also a user can be associated to several profiles and the one with higher privileges is applied to the login user.

Tip  You must select both Profile may not restrict by hierarchial location and Allow profile to be bound to hierarchial locations per assignment to associate profiles to hierarchial location.

Note  If the user does not select the fields that associate profiles to locations, the user profile actions are not restricted to the locations or sub locations that they belong to. The configuration settings would then reflect the Cisco Physical Access Manager 1.3 release.
Password Policy Settings

The Password Policy options (Figure 17-6) determine password expiration and strength requirements.

Figure 17-6 Password Policy Settings

Table 17-6 System Configuration Password Policy Fields

<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>

Table 17-6 describes the Password Policy settings.

Note

Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select Logout from the Options menu).
Custom Personnel Fields Settings

The Custom Personnel Fields defines the custom fields available in the personnel detail window.

**Figure 17-7  Custom Personnel Fields**

Table 17-7 describes the Custom Personnel Fields settings.

**Table 17-7  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 the a sentence, for example: Driver's license number.</td>
</tr>
</tbody>
</table>
Note
Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select Logout from the Options menu).

Custom Device Fields Settings

Configures which the custom fields which are available in the device detail window.

Figure 17-8  Custom Device Fields

Table 17-8 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>
</tbody>
</table>
Chapter 17  System Configuration Settings

Custom Badge Fields

Configures which the custom fields which are available in the badge detail window.

Table 17-8  Custom Device Fields Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column header</td>
<td>Change 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>Change 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 you log out and log back in to the Cisco PAM application (select Logout from the Options menu).
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 you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).
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 17-10  Personnel ID Number Generator Settings

Table 17-10  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.

**Table 17-11  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 you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).
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 17-12  Card Number Generator Settings

Table 17-12  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 you log out and log back in to the Cisco PAM application (select Logout from the Options menu).
Support Contact Information

Customer contact 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 17-13   Support Contact Information Settings

Table 17-13   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 you log out and log back in to the Cisco PAM application (select Logout from the Options menu).
Miscellaneous Settings

Figure 17-14 includes a variety of settings, as described in Table 17-14.

Figure 17-14  Miscellaneous Settings

Table 17-14  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>
</tbody>
</table>
### Table 17-14  Miscellaneous Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Restrict new devices to wizards only</td>
<td>All new devices added to the Hardware 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 Adding a Color Border to Event Photos (Credential Watch), page 12-18.</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>
<tr>
<td>Logged in workstations assume partition of login’s profile</td>
<td>not supported in this version.(1.4.1)</td>
</tr>
<tr>
<td>Partition-restricted workstations only use explicitly assigned license items</td>
<td>not supported in this version.(1.4.1)</td>
</tr>
<tr>
<td>Rasterize before printing</td>
<td>It converts the watermark into an image internally and prints it on the badge. Note: Ensure that you do not enable this option unless there is an issue with printing the images on the badges.</td>
</tr>
</tbody>
</table>
Note

Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select Logout from the Options menu).
Cisco Settings

Figure 17-15 includes the settings described in Table 17-14.

Figure 17-15 Cisco Settings

To activate changes made to Cisco settings, you must either log out and log back in, or restart the Cisco PAM appliance, as described in the following table. To restart the appliance, see Using the Web Admin Menus, Commands and Options, page 3-17, or ask your system administrator for assistance.

Table 17-15 Cisco Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>To Activate Changes</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>
<td>Restart the Cisco PAM appliance.</td>
</tr>
</tbody>
</table>
| Credential download frequency (mins) | Defines how often (in minutes) credential information is downloaded to the Gateways.  
Note 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 9-2 for more information. | Restart the Cisco PAM appliance.     |
| NTP Server                         | Defines a default NTP server when updating multiple Gateways. See the “Changing the NTP Setting for Multiple Gateway Modules” section on page C-7. | Log out and log in.                  |
### Table 17-15 Cisco Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>To Activate Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDI personnel’s photo size limit</td>
<td>Defines the maximum file size for imported photo files using the System Configuration module. For example, if you enter a maximum file size of 500 kb, then any files larger than 500 kb will be automatically compressed when the personnel record is imported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter a value, in kb, between 50 and 750.</td>
<td>Log out and log in.</td>
</tr>
<tr>
<td></td>
<td>• The default value is 250 kb.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See the “Understanding Photo File Compression When Importing Personnel Records” section on page 14-17.</td>
<td></td>
</tr>
<tr>
<td>Display soft commands on default module</td>
<td>Displays the soft commands for the default m01 (Gateway) module.</td>
<td>Log out and log in.</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.</td>
<td>Log out and log in.</td>
</tr>
<tr>
<td></td>
<td>See Deleting the Cisco VSM Cameras, page 15-30.</td>
<td></td>
</tr>
<tr>
<td>Evict most recent badge from APB area when door not used</td>
<td>If a user presents their badge and is granted access to an Anti-Passback Area, but decides not to enter the door, then a Door Not Used event is generated by the door’s Gateway module. To prevent the badge from being added to the Anti-Passback monitoring list, enable the System Configuration setting for Evict most recent badge from APB area when door not used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See the “Evicting a Badge from APB if the User Does Not Enter the APB Area” section on page 11-24</td>
<td>Restart the Cisco PAM appliance.</td>
</tr>
</tbody>
</table>
Backing 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-23 for more information.

Contents

- Backing up the Cisco PAM Database, page A-1
  - Backup Usage Notes, page A-2
  - Scheduling Automatic Backups, page A-2
  - Disabling Automatic Backups, page A-5
  - Performing a One-Time Manual Backup, page A-6
- Archiving the Historical Events Database, page A-8
- Restoring a Server Backup File, page A-8

Backing up the Cisco PAM Database

Use the backup option in the Cisco PAM Server Administration utility to back up all Cisco PAM data and configurations. 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.

The following backup options are available:

- Backup all data, including live and historical events.
- Backup all data but exclude all events (do not back up events).
- Define an automatic backup schedule.
• Copy the automatic backups to a remote server.
• Perform a one-time manual backup.

Refer to the following topics:
• Backup Usage Notes, page A-2
• Scheduling Automatic Backups, page A-2
• Disabling Automatic Backups, page A-5
• Performing a One-Time Manual Backup, page A-6

Backup Usage Notes

• The maximum size for a backup file is 1 gigabyte (GB) of data. An error occurs if the backup file will be larger than 1 GB, and the backup will fail.
• To reduce the size of the backup, do one or both of the following:
  – Exclude events from the backup operation. See the automatic and manual backup instructions in this section for more information.
  – Remove historical events from the database to reduce the size of the backup file. See the “Archiving the Historical Events Database” section on page A-8 for more information. See the “Archiving Historical Events” section on page 3-24 for instructions.
• The backup password is used to restore the backup file, if necessary. Record this password in a safe location.
• Manual backups are enabled only if automatic backups are disabled.
• 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 restore a backup, stop both servers in an HA configuration. The backup can be restored to either server.

Scheduling Automatic Backups

This section describes how to define automatic backups, including how to automatically save the backup files to a remote FTP or SFTP sever. Figure A-1 shows the Automatic backup window.
Appendix A      Backing Up and Restoring Data

Figure A-1  Backup Window in the Cisco PAM Server Administration Utility

The three most recent backup files are listed at the top of the page. When a fourth backup file is added, the oldest file is deleted. You can right click a filename to save it to a local or network drive, or use the option in the following procedure to automatically copy the backup files to a remote server. The saved file includes the date (mm/dd/year) the backup occurred, the Cisco PAM version number, and other information. For example: bak-02062011-1422251.3.0_0.3.25.cpam-132.

Procedure
To define automatic backups of 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 3-2.
Step 2  Select Setup and then Backup, as shown in Figure A-1.
Step 3  Select the Automatic backup check box.
Step 4  Enter and re-enter a password for the backup file.
   This password must be entered when the backup file is used to restore the data.
Step 5  (Optional) Select the Exclude Events box to exclude events from the backup.
   •  Events will not be backed up and cannot be restored.
   •  To remove historical events from the main database and reduce the size of the backup file, review the “Archiving the Historical Events Database” section on page A-8.
• For instructions to prune old events from the main database, or to remove them from the database by creating an archive of historical events, see the “Archiving Historical Events” section on page 3-24.

Step 6 Define the automatic backup schedule.
   a. 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.
   b. 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.

Step 7 (Optional) Automatically copy the backups to a remote FTP or SFTP 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 8 Click Update to save the changes. Backups will occur according to 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 backup name includes the date and the server software version number. For example: February 06, 2011 02:22:25 PM 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 7.
If the remote server settings are incorrect or the directory path does not exist, the file is not copied and an error message is displayed.

The backup is still saved to the Cisco PAM server even if the remote server is unavailable.

Disabling Automatic Backups

To disable automatic backups, deselect the Automatic backup check box (Figure A-2).

**Figure A-2  Disabling Automatic Backups**

![Cisco PAM Server Administration](image)

**Procedure**

**Step 1** Log on to the Cisco PAM appliance as described in Logging on to the Cisco PAM Server Administration Utility, page 3-2.

**Step 2** Select **Setup** and then **Backup**, as shown in Figure A-2.

**Step 3** Select the **Automatic** tab.

**Step 4** De-select the **Automatic backup** check box.

**Step 5** Click Update.

**Step 6** (Optional) Perform a manual backup, if necessary. See the “Performing a One-Time Manual Backup” section on page A-6.
Performing a One-Time Manual Backup

This section describes how to perform a one-time manual backup, including how to save the backup file to a remote FTP or SFTP server. Figure A-3 shows the manual backup window.

Tip

Manual backups are enabled only if automatic backups are disabled. See the “Disabling Automatic Backups” section on page A-5.

Figure A-3    Manual Backup Window

The three most recent backup files are listed at the top of the page. When a fourth backup file is added, the oldest file is deleted. You can right click a filename to save it to a local or network drive, or use the option in the following procedure to automatically copy the backup files to a remote server. The saved file includes the date (mm/dd/year) the backup occurred, the Cisco PAM version number, and other information. For example: bak-02062011-1422251.3.0_0.3.25.cpam-132.

Procedure

To define automatic backups, 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 3-2.

Step 2    Select Setup and then Backup.

Step 3    Select the Manual tab, as shown in Figure A-3.

Note    Manual backups are enabled only if automatic backups are disabled. See the “Disabling Automatic Backups” section on page A-5.

Step 4    Enter and re-enter a password for the backup file.
Step 5  (Optional) Select the **Exclude Events** box to exclude events from the backup.

- Events will not be backed up and cannot be restored.
- To remove historical events from the main database and reduce the size of the backup file, review the “Archiving the Historical Events Database” section on page A-8.
- For instructions to prune old events from the main database, or to remove them from the database by creating an archive of historical events, see the “Archiving Historical Events” section on page 3-24.

Step 6  (Optional) Automatically copy the backup to a remote server.

Use this option to automatically copy the backup file to a remote FTP or SFTP server.

a. Check the **Copy to remote server** check box.

The **remote server** settings appear, as shown in Figure A-3.

b. Select the server protocol:
   - **FTP**: for standard File Transfer Protocol servers.
   - **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 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 7  Click **Backup Now** to begin the backup process and create a new .zip backup file.

- When the backup is complete, the new backup file is added to the top of the screen, as shown in Figure A-3.

  - 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 6.

  - If the remote server settings are incorrect or the directory path does not exist, the file is not copied and an error message is displayed.

  - The backup is still saved to the Cisco PAM server even if the remote server is unavailable.
Archiving the Historical Events Database

When you copy and prune old events (as described in “Archiving Historical Events” section on page 3-24) the events are moved to a separate Cisco PAM database. Although the events are no longer displayed in Events and Alarms, they can still be included in system backups (see the “Understanding Live, Pruned and Archived Events” section on page 3-24).

Archiving these historical events removes them from the database and saves them to .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.

You can right click a filename to save it to a local or network drive, or automatically copy the archive files to a remote FTP or SFTP server.

The historical event management settings are entered during the initial server setup. See the “Initial Setup Instructions” section on page 3-7 for instructions.

To modify these settings, use the Cisco PAM Server Administration utility, as described in the “Archiving Historical Events” section on page 3-24.

Restoring a Server Backup File

Complete the procedure in this section to restore data from a backup file, or from an archive file.

Note the following when restoring data or archives:

- Data can be restored only when the server is stopped.
- Both servers must be stopped in an HA configuration. The backup can be restored to either server.
- 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.
- Backup files include the Cisco PAM configuration and other data.
- Archive files include only historical events that were removed from the database using the Archive function. You can view historical events recovered from an archive file using Reports, but they cannot be viewed in the Events and Alarms module. See Archiving the Historical Events Database, page A-8 for more information.
- If an archive from release 1.2.0 or earlier is restored, you will automatically be redirected to the Events configuration page of the Cisco PAM Server Administration utility. Use this page to enter the required setting to prune and archive old events. See the “Archiving Historical Events” section on page 3-24 for information and instructions. You cannot start the server or perform other activities until the event archiving is successfully configured.

Procedure

To restore the data from a backup or archive file, do the following:

**Step 1** Verify that you have the correct backup file from either the Active or Standby server.

See Backing up the Cisco PAM Database, page A-1.

**Step 2** Stop the Standby server, if installed.
A. Log on to the Standby Cisco PAM appliance.

b. Select Monitoring and then select Status.

c. In the Admin State Entry, click Stop.

d. Verify that the Admin State is Down, as shown in Figure A-4.

Step 3
Stop the Active server.

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.

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 Monitoring and then select Status.

c. In the Admin State Entry, click Stop.

d. Verify that the Admin State is Down, as shown in Figure A-4.

Step 4
On the Active server, select the Setup tab, and then select Restore, as shown in Figure A-5.
Figure A-5  
*Restore Window in the Cisco PAM Server Administration Utility*

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-1.

Step 6  
Click **Browse** to locate and select the .zip backup file.

For example: `bak-02102011-1141001.3.0_0.3.25.cpam-supermicro-116`

Step 7  
If the file is an archive file, select the **Is Archived File** checkbox.

See Archiving the Historical Events Database, page A-8 for more information.

Step 8  
Click **Restore** and wait for the restore process to complete.

Step 9  
Wait for the 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  
If restoring a backup from Release 1.2.0 or earlier to Release 1.3.0 or higher, you must enter the event pruning and archive settings, as shown in Figure A-6.

**Note**  
If you are upgrading from release 1.3.0 or higher, skip to Step 11.

- Pruned Events are removed from the main database table and placed in a separate database, allowing you to reduce the size of the main database date while keeping them accessible on the Cisco PAM system. Pruned events are not visible in Events & Alarms, but are included in reports. Pruned events are also included in system backups.

- Archived events are removed from all Cisco PAM database tables and copied to a compressed file. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archived events are not visible in the Events & Alarms listings or Reports, and are not included in system backups.

**Tip**  
These settings are only required if restoring a backup from Release 1.2.0 or earlier. After the restore is complete, you can make additional changes. See the “Archiving Historical Events” section on page 3-24 for more information.
a. Select the **Pruning** tab (Figure A-6), and enter the following settings:

- **Live Events Window (days)**—Enter a value between 0 and 500 (inclusive). This is the number of days of events that will be available on live view. All the events older than the specified days will be removed at the pruning schedule time. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are subject to pruning and archiving (depending on the schedule defined in the following steps).

- **Schedule**—define the time and frequency when events should pruned.
  - **Date**—To schedule pruning for one day per month, select **Date** and then select a day of the month. For example: 15.
  - **Weekday**—To schedule pruning once per week, select **Weekday** and then select a day of the week. For example: Tuesday.
  - **Daily**—To run pruning every day, select **Daily**.
  - **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run pruning at 2 p.m., enter **14:00:00**. To run pruning at 1 a.m., enter **01:00:00**.

- **Note**
  - To ensure that events are regularly pruned, we recommend entering 60 days or less in the **Live Events Window** field. Entering a value greater than 60 can cause an excessive number of event entries to accumulate in the main database and negatively impact system performance.
  - The number is rounded to midnight of the last day.
b. Select the **Archive** tab (Figure A-7) and enter the following settings:

**Tip**

The archive settings are required during the initial setup. After a successful restore, you can disable auto-archiving if necessary. See the “Archiving Historical Events” section on page 3-24.

- Enter and re-enter the administrator **Password**. This password is used to restore the archive file (similar to backup files).

- **Historic Events Window (days)**—Enter the number of days that events will be available for reports. After the minimum number of days the events will be archived to a compressed file. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are subject to archiving (depending on the schedule defined in the following steps).

- Enter a **Schedule** when the historic events will be removed from the pruned database and placed into a compressed archive file (archived files are listed above the entry fields).
  - **Date**—To schedule archiving for one day per month, select **Date** and then select a day of the month. For example: 15.
  - **Weekday**—To schedule archiving once per week, select **Weekday** and then select a day of the week. For example: Tuesday.
  - **Daily**—To run archiving every day, select **Daily**.
  - **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run archiving at 2 p.m., enter 14:00:00. To run archiving at 1 a.m., enter 01:00:00.

- (Optional) Select **Copy to remote server** to automatically copy the archived event files to a remote FTP or SFTP location.
Only the three most recent archive files are saved. If you do not save the archive file manually or by copying it to a remote server, then the oldest file will be permanently deleted when the fourth file is created.

- **FTP**: for standard File Transfer Protocol servers.
- **SFTP**: for secure file transfers using the Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).
- **Address**—the IP address or hostname of the remote server.
- **Username**—the username required to log in to the server.
- **Password**—the login password for the remote server.
- **Path**—the directory path where the compressed archive will be copied. The path must exist on the remote server. If the directory is not available, the archive will fail.

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

**Step 11** 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-8.

c. Verify the following:
   - The Admin State is **Up**.
   - The Server Mode is **Active**.

**Figure A-8** **Server Admin State (Up) for the Active Server**

![Server Admin State (Up) for the Active Server](image)

**Step 12** If the Status is **Down**, click **Start** to manually restart the server and then verify that the Admin State is **Up**.

**Step 13** 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 the Server Software

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 1.4.1, page B-2
- Obtaining Software Images, page B-8
- Obtaining Release Notes and Other Related Documentation, page B-9
- Upgrading the Cisco PAM Desktop Software, page B-10
- Upgrading the Cisco PAM Server Software, page B-11
- Replacing an Appliance, page B-18
  - Replacing a Stand-Alone (Non-Redundant) Appliance, page B-18
  - Replacing Both Appliances in an HA Configuration, page B-19
- Reinstalling the Cisco PAM Server Software from a Recovery CD, page B-23
Upgrade Notes for Release 1.4.1

- Event Archive Settings Are Required, page B-3
- Localization Feature Requires Database Upgrade, page B-4
- Gateway Module Firmware Must Be the Same Version as Cisco PAM, page B-4
- Credential Download Frequency Must be 60 Minutes or Higher, page B-4
- The Door Groups Feature Added to Device Groups, page B-5
- Enabling the Password Recovery Feature, page B-5
- Upgrading From Release 1.0.3 to Release 1.4.1, page B-5
- Split Holiday Schedule Configurations By Month, page B-5
- Select the Following Options When Upgrading Gateway Firmware, page B-6
- Generic Output Devices Installed Prior to Release 1.1.0 Must Be Rewired, page B-6
- Generic Output Device Command and Event Name Changes, page B-6
- Browser Time-out, page B-7
- Upgrade the Cisco PAM Desktop Client Software, page B-7
- Java Requirements, page B-7
- Stop EDI Projects Before Upgrading Cisco PAM, page B-7
- Change the Database Password Message, page B-7
- Event Archive Settings Are Required, page B-3
- Localization Feature Requires Database Upgrade, page B-4
- Gateway Module Firmware Must Be the Same Version as Cisco PAM, page B-4
- Credential Download Frequency Must be 60 Minutes or Higher, page B-4
- Enabling the Password Recovery Feature, page B-5
- Upgrading From Release 1.0.3 to Release 1.4.1, page B-5
- Split Holiday Schedule Configurations By Month, page B-5
- Browser Time-out, page B-7
- Upgrade the Cisco PAM Desktop Client Software, page B-7
- Java Requirements, page B-7
- Stop EDI Projects Before Upgrading Cisco PAM, page B-7
- Change the Database Password Message, page B-7
Event Archive Settings Are Required

If upgrading from Release 1.3 or earlier, you are automatically redirected to the Events configuration page of the Cisco PAM Server Administration utility (Figure B-1).

**Figure B-1 Initial Setup: Event Pruning and Archiving**

![Cisco PAM Server Administration](image)

Use this page to enter the required event pruning and archive settings. You cannot start the server or perform other activities until event archiving is successfully configured.

The following additional conditions apply:

- If you are upgrading redundant HA servers, the historical event archive settings are only required on the primary appliance.
- If the appliance being upgraded has existing automation rules configured for historical events, the following occurs during the upgrade:
  - Commands to copy, prune or archive events are removed. If the automation rule only includes these commands, then the entire rule is removed. The system will use the new event pruning and archiving settings you are prompted to enter during the upgrade.
  - If the automation rule also includes action to create reports, the automation rule is upgraded and the reports rules are saved in the upgraded system.

For instructions and more information, see the “Archiving Historical Events” section on page 3-24.
Localization Feature Requires Database Upgrade

If you upgrade the Cisco PAM appliance from release 1.3.0 or lower to release 1.4.1 or higher, you must also upgrade the system database to support localization. This is a one-time process performed by clicking an Enable Localization button the first time you access the localization feature (Figure B-2).

**Figure B-2  Enabling Localization**

- This procedure is also required if you restore a data backup from release 1.2.0 or lower to release 1.3.0 or higher.
- This process can take up to one hour (or more) to complete for large databases.
- For more information, see the “Installing and Revising Language Packs” section on page 3-29.

Gateway Module Firmware Must Be the Same Version as Cisco PAM

Gateway modules must have the same firmware version as the Cisco PAM appliance server software. This includes the major version, minor version, maintenance version, and the build number. If any difference in versions exists between the Gateway and the appliance, then only a restricted set of operations (such as image upgrade) can be performed.

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 17-23.
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-5 for instructions.

Upgrading From Release 1.0.3 to Release 1.4.1

To upgrade to Cisco PAM Release 1.4.1 from Release 1.0.3, you must first upgrade to Cisco PAM Release 1.1.0. For more information see the caveat CSCte56355.

Post Upgrade:

- The doors without any location will be moved to the Gateway/Expansion module location during the upgrade.
- Doors with a different location than that of its parent GW/expansion module location will now remain in the same location. After upgrade, while editing these doors the user cannot save if the door’s location is different from Gateway expansion module location, hence the user has to ensure that both the door and gateway are in the same location.
- Expansion Modules that are created under the GW will be assigned to the GW Location independent of whether the module is assigned to any location before upgrade.

Fresh Installation:

- The Modules will be assigned to the Gateway location by default and the location value will be read-only.(both Default and Expansion Modules)
- Newly created doors will be assigned to the Gateway location by default, independent of whether it is created either using Default Module or Expansion Module or both.

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 1.4.1 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 C-12 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, 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 4-2.

**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 14-41 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**

After an upgrade, if the server is started using the Start command in the Commands menu of the Cisco PAM Server Administration utility, a message appears asking if you want to change the database password. Click Cancel. This password is a security measure used for troubleshooting and technical support. It does not impact user operation.
Obtaining Software Images

To access the self-service portal and obtain software, documents, and tools, do the following:

**Step 1**
Go to the following URL:

**Tip**
You can also log in to the Cisco Support Center at http://www.cisco.com/support/.

**Step 2**
Enter your username and password.
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.

**Step 3**
Click the **Download Software** link (Figure B-3).

**Figure B-3  Download Cisco PAM Software Updates**

**Step 4**
Click the link for the correct release, or use the search function to locate the software release (Figure B-4).
Figure B-4   Select and Download a Software Release

Step 5  Click Download Now.

Step 6  Follow the on-screen instructions to save the download file to a local or network drive:
   a. Verify the download details.
   b. Click Proceed With Download.
   c. Accept the End User License Agreement.
   d. Select a download option (Java or non-Java).
   e. Select a location to save the file.
   f. Wait for the download to complete.

Step 7  Locate and extract the compressed .zip file on your drive.
        For example: cpam-cam25-1.4.1_0.3.6.upgrade.zip.

Step 8  Open the directory and verify that the file is correct.
        The filename includes the release number and other details. For example:
        cpam-cam25-1.4.1_0.3.6.upgrade.bin.

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
        – Cisco Physical Access Manager Documentation

Step 2  Click the link for the appropriate guide.
For example: **Install and Upgrade Guides** or **End-User Guides**.

**Step 3** Use these publications to learn how to install, upgrade and use the Cisco Physical Access Control hardware and software.

**Tip** Release Notes are also included with software downloads, or you can access the release notes while downloading software updates. See the “Obtaining Software Images” section on page B-8.

---

**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 4-2 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.
  - If upgrading two redundant appliances (HA configuration), complete the upgrade on one appliance before beginning the upgrade on the second appliance. If the second appliance is upgraded before the first appliance upgrade is complete, unrecoverable conditions may occur, forcing a restore from a backup file.
  - Software downgrades are not supported.
- Review all Upgrade Notes for Release 1.4.1, page B-2
- Obtain the correct software image. See Obtaining Software Images, page B-8.

**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 and Upgrade Notes for Release 1.4.1, page B-2

**Step 2**
Backup either the Active or Standby server, as described in Backing up the Cisco PAM Database, page A-1. This backup is not required, but ensures the latest system data is preserved in case an error occurs.

**Step 3**
Save the backup file to a local drive.

**Step 4**
Stop the Standby server, if configured:
- Log on to the Standby appliance, as described in Logging on to the Cisco PAM Server Administration Utility, page 3-2.
- Click the Monitoring tab and verify the Server Mode is Standby (Figure B-5).
- Select the Stop button in the Admin entry.
- Verify that the Admin State is Down.
Upgrading the Cisco PAM Server Software

Step 5  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-5).

c.  In the Admin State entry, select Stop.

d.  Verify that the Admin State is Down.

Step 6  On the Active server, select the Setup tab, and then select Upgrade, as shown in Figure B-6.

Figure B-6  Upgrade Window in the Cisco PAM Server Administration Utility

Step 7  Click Browse to locate and select the upgrade image.

See the “Obtaining Software Images” section on page B-8 to download the upgrade software, if necessary.

For example: cpam-cam25-1.4.1_0.3.6.upgrade.bin

Step 8  Click the Upgrade button.

- A message appears informing you that the upgrade is starting and the web page will refresh.
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 9**
The log in page appears when the upgrade is complete.

**Step 10**
Enter your existing username and password to log into the appliance.

**Step 11**
If upgrading from Release 1.2.0 or earlier to Release 1.3.0 or higher, you must enter the event pruning and archive settings, as shown in Figure B-7.

**Note**
If you are upgrading from release 1.3.0 or higher, skip to **Step 12**.

- Pruned Events are removed from the main database table and placed in a separate events database, allowing you to reduce the size of the main database while keeping them accessible on the Cisco PAM system. Pruned events are not visible in Events & Alarms, but are included in reports. Pruned events are also included in system backups.

- Archived events are removed from all Cisco PAM database tables and copied to a compressed file. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archived events are not visible in the Events & Alarms listings or Reports, and are not included in system backups.

**Tip**
These settings are only required if upgrading from Release 1.2.0 or earlier. After the upgrade is complete, you can make additional changes. See the “Archiving Historical Events” section on page 3-24 for more information.

---

**Figure B-7**  Initial Setup: Event Pruning and Archiving

![Pruning and Archiving Settings](image)

- **Live Events Window (days)**—Enter a value between 0 and 500 (inclusive). This is the number of days of events that will be available on live view. All the events older than the specified days will be removed at the pruning schedule time. For example, enter **30** to keep events in the live view for 30 days. After midnight on day 30, the events are subject to pruning and archiving (depending on the schedule defined in the following steps).
Appendix B      Upgrading the Server Software

To ensure that events are regularly pruned, we recommend entering 30 days or less in the **Live Events Window** field. Entering a value greater than 30 can cause an excessive number of event entries to accumulate in the main database and negatively impact system performance.

The number is rounded to midnight of the last day.

**Schedule**—define the time and frequency when events should be pruned.

- **Date**—To schedule pruning for one day per month, select **Date** and then select a day of the month. For example: 15.
- **Weekday**—To schedule pruning once per week, select **Weekday** and then select a day of the week. For example: Tuesday.
- **Daily**—To run pruning every day, select **Daily**.
- **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run pruning at 2 p.m., enter 14:00:00. To run pruning at 1 a.m., enter 01:00:00.

**Pruning Hours**—This field is enabled only if Daily is selected in Schedule. The default value is 1.

**Figure B-8       Archiving Events**

b. Select the **Archive** tab (Figure B-8) and enter the following settings:

**Tip**

The archive settings are required during the initial setup. After a successful restore, you can disable auto-archiving if necessary. See the “Archiving Historical Events” section on page 3-24.
Appendix B  Upgrading the Server Software

Upgrading the Cisco PAM Server Software

- Enter and re-enter the administrator **Password**. This password is used to restore the archive file (similar to backup files).

- **Historic Events Window (days)**—Enter the number of days that events will be available for reports. After the minimum number of days the events will be archived to a compressed file. For example, enter **30** to keep events in the live view for 30 days. After midnight on day 30, the events are subject to archiving (depending on the schedule defined in the following steps).

- Enter a **Schedule** when the historic events will be removed from the pruned database and placed into a compressed archive file (archived files are listed above the entry fields).
  - **Date**—To schedule archiving for one day per month, select **Date** and then select a day of the month. For example: **15**.
  - **Weekday**—To schedule archiving once per week, select **Weekday** and then select a day of the week. For example: **Tuesday**.
  - **Daily**—To run archiving every day, select **Daily**.
  - **Time**—Enter the time in 24 hour format (hh:mm:ss). For example, to run archiving at 2 p.m., enter **14:00:00**. To run archiving at 1 a.m., enter **01:00:00**.

- **(Optional)** Select **Copy to remote server** to automatically copy the archived event files to a remote FTP or SFTP location.

**Note** Only the three most recent archive files are saved. If you do not save the archive file manually or by copying it to a remote server, then the oldest file will be permanently deleted when the fourth file is created.

- **FTP**: for standard File Transfer Protocol servers.
- **SFTP**: for secure file transfers using the Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).
- **Address**—the IP address or hostname of the remote server.
- **Username**—the username required to log in to the server.
- **Password**—the login password for the remote server.
- **Path**—the directory path where the compressed archive will be copied. The path must exist on the remote server. If the directory is not available, the archive will fail.

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

**Step 12** 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: **1.4.1**

d. Verify the Admin State is **Down**.

e. Verify the Server Mode is **N/A**.
Appendix B      Upgrading the Server Software

Upgrading the Cisco PAM Server Software

Figure B-9  Server Admin State for the Active Server

Step 13  (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 12. If a Standby server is not installed, skip to Step 14.

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-9
d. Select the Setup tab, and then select Upgrade.
e. Click Browse to locate and select the upgrade image, as shown in Figure B-6 on page B-12.
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 14  Restart the Active server.
a. Log on to the Active Cisco PAM appliance, if necessary.
b. Select Monitoring and then Status.
c. In the Admin State entry, select Start.
d. Wait for the Admin State to change to Up.

Note  When the server restarts, a message may appear 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,
e. Select the Monitoring tab and then select Status, as shown in Figure B-10.
f. Verify the following:
   - Verify the Server Version is correct. For example: 1.3.0
   - Verify the Admin State is Up.
   - Verify the Server Mode is Active.

Figure B-10  Server Admin State (Up) for the Active Server

Step 15  (HA configurations only) Start the Standby server.

Note  Only start the Standby server after the Active server is Up, as described in Step 14.

a. Log on to the Active Cisco PAM appliance.
b. Select Monitoring and then Status.
c. In the Admin State entry, select Start.
d. Wait for the Admin State to change to Up.
e. Click Cancel or OK if a database password message appears.
f. 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: 1.3.0
   - Verify the Admin State is Up.
   - Verify the Server Mode is Standby.

Step 16  Restore your data backup, if necessary. See the “Restoring a Server Backup File” section on page A-8.

Step 17  Upgrade the Cisco PAM desktop client, as described in Installing or Updating the Cisco PAM Desktop Software, page 4-2. If the versions are not the same, an error will occur when launching the desktop client.
Replacing an Appliance

To replace an existing appliance with a Cisco Multi Services Platform (MSP) appliance, refer to the following procedures:

- Replacing a Stand-Alone (Non-Redundant) Appliance, page B-18
- Replacing Both Appliances in an HA Configuration, page B-19
- Replacing a Single Appliance in an HA Configuration, page B-21

Replacing a Stand-Alone (Non-Redundant) Appliance

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>Step 1</td>
<td>Backup the old appliance, as described in Backing up the Cisco PAM Database, page A-1. This backup is used to restore the system data to the new appliance.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Copy the backup file to a local disk, as described in Backing up the Cisco PAM Database, page A-1.</td>
</tr>
</tbody>
</table>
| Step 3 | Stop the appliance.  
  a. Log on to the appliance, as described in Logging on to the Cisco PAM Server Administration Utility, page 3-2.  
  b. Select Monitoring and then select Status (Figure B-11).  
  c. In the Admin State Entry, click Stop.  
  d. Verify that the Admin State is Down. |
| Step 4 | Power off the old appliance and physically install the new appliance, as described in the Cisco Physical Security Multi Services Platform User Guide. |
| Step 5 | Boot the new server and complete the setup instructions in Initial Setup Instructions, page 3-7. |
| Step 6 | Obtain and install new Cisco PAM licenses. See Obtaining and Installing Optional Feature Licenses, page 3-44 for more information. |
| Step 7 | Restore the backup file to the new server, as described in Restoring a Server Backup File, page A-8. |
Replacing Both Appliances in an HA Configuration

To replace both appliances in a redundant HA configuration, complete the following procedure:

⚠️ **Caution**

This procedure results in system downtime.

**Procedure**

**Step 1** Back up the Active or Standby server.

The backup file is used to restore the system data on the new server.

a. Log in to the Active or Standby appliance.

b. Backup the system data, as described in [Backing up the Cisco PAM Database](#), page A-1.

c. Copy the backup file to a local disk.

**Step 2** Stop the Active appliance.

a. Log on to the Active appliance, as described in [Logging on to the Cisco PAM Server Administration Utility](#), page 3-2.

b. Select **Monitoring** and then select **Status** (Figure B-11).

c. Verify the Server Mode is **Active**.

d. In the Admin State Entry, click **Stop**.

e. Verify that the Admin State is **Down** and the Server Mode is **N/A**, as shown in Figure B-11.

![Figure B-11](image.png)

**Step 3** Stop the Standby appliance.
Replacing an Appliance

Note

Stopping the second appliance results in system downtime since both appliances are offline.

a. Log on to the appliance, as described in Logging on to the Cisco PAM Server Administration Utility, page 3-2.

b. In the Admin State Entry, click Stop.

Step 4 Power down and physically remove the old appliances.

Step 5 Install the new appliances, as described in the Cisco Physical Security Multi Services Platform User Guide.

Step 6 Boot the new Active appliance and complete the initial configuration for an Active server, as described in Initial Setup Instructions, page 3-7.

- Enter a Shared IP Address.
- Obtain and install new Cisco PAM licenses, including the HA license. All optional licenses are installed on the Active server only. See Obtaining and Installing Optional Feature Licenses, page 3-44 for more information.

Step 7 Boot the new standby appliance and complete the initial configuration for a Standby server.

- Enter a Shared IP Address, as described in Initial Setup Instructions, page 3-7.
- Obtain and reinstall the HA license on the Standby server. See Obtaining and Installing Optional Feature Licenses, page 3-44 for more information.

Step 8 Verify that the redundant servers are in sync.

a. Log in to each server.

b. Open the Monitoring > Status window.

c. Verify that there are entries for Peer Address, Hostname, and Sync Status (Figure B-12).

   If the HA servers are not in sync, see the “Monitoring” section on page 3-20 for a description of the HA messages that may appear.

![Figure B-12 HA Status: Peer Address, Hostname and Sync Status](image-url)
Recovering a Single Appliance in an HA Configuration

To replace a single appliance in a HA configuration, put the appliance in Admin Down state. This transfers the Active server status to the other appliance. System data is maintained and access control functionality remains available. Next, physically replace the appliance and complete the initial configuration for a Standby server. Once the server is up, system data will be synchronized from the Active HA appliance.

Procedure

1. **Step 1** (Optional) Back up the Active or Standby server.
   - The backup is not required, but we recommend performing a backup before any major operation.
   - a. Log in to the Active or Standby appliance.
   - b. Backup the system data, as described in Backing up the Cisco PAM Database, page A-1.
   - c. Copy the backup file to a local disk.

2. **Step 2** Stop the appliance to be replaced.
   - a. Log on to the appliance, as described in Logging on to the Cisco PAM Server Administration Utility, page 3-2.
   - b. Select Monitoring and then select Status (Figure B-13).
   - c. In the Admin State Entry, click Stop.
   - d. Verify that the Admin State is Down and the Server Mode is N/A, as shown in Figure B-13.

3. **Step 3** Power down and physically remove the old appliance.

4. **Step 4** Install the replacement appliance, as described in the Cisco Physical Security Multi Services Platform User Guide.
Replacing an Appliance

Step 5  Boot the new appliance and complete the initial configuration for a Standby server.

- Enter a Shared IP Address, as described in Initial Setup Instructions, page 3-7.
- Obtain and reinstall the HA license on the Standby appliance. See Obtaining and Installing Optional Feature Licenses, page 3-44 for more information.

Step 6  Wait for the initial setup process to complete.

Step 7  Verify that the redundant servers are in sync.

a. Log in to the appliance.

b. Open the Monitoring > Status window.

c. Verify that there are entries for Peer Address, Hostname, and Sync Status (Figure B-14).

If the HA servers are not in sync, see the “Monitoring” section on page 3-20 for a description of the HA messages that may appear.

Figure B-14  HA Status: Peer Address, Hostname and Sync Status

![HA Status: Peer Address, Hostname and Sync Status](image-url)
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.

**Usage Notes**
- To boot from the recovery CD/DVD, you must change the boot device order using the BIOS utility, as described in the following procedure.
- Before you begin, back up your system data. The recovery CD deletes all existing data and configurations. See the “Back up the Cisco PAM Database” section on page A-1.
- You can perform this procedure on a standalone appliance, or on either the active or standby appliance in a redundant HA configuration.
- If using the recovery CD on an appliance in a HA configuration, perform the initial setup for a Standby appliance, and enter a Shared IP address.
- After the recovery process, complete the instructions in the “Initial Setup Instructions” section on page 3-7 and then the “Restoring a Server Backup File” section on page A-8.

**Procedure**

**Step 1**
Backup the data on your appliance. See Appendix A, “Back up and Restore Data” for more information.

---

**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 data. See Appendix A, “Back up and Restore Data” for more information.

**Step 2**
Insert the Cisco PAM recovery CD into the server DVD-ROM drive.

**Step 3**
Reboot the Cisco PAM appliance:
- Log on to the Cisco PAM appliance, as described in Logging on to the Cisco PAM Server Administration Utility, page 3-2.
- 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-15.
Reinstalling the Cisco PAM Server Software from a Recovery CD

Appendix B      Upgrading the Server Software

Reinstalling the Cisco PAM Server Software from a Recovery CD

Figure B-15    BIOS Setup Utility

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-16.

Figure B-16    BIOS Boot Settings

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-17**.

**Figure B-17  Boot Device Priority Options**

![Boot Device Priority Options](image)

---

- **Options**
  - 1st FLOPPY DRIVE
  - USB-TEAC DU-203-U
  - SCSI: (Bus 05 Dev 00) LSI SW RAID
  - Disabled

---

A list of available devices appears.

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-18**.

**Figure B-18  1st Boot Device = CD/DVD**

![1st Boot Device = CD/DVD](image)

---

- **Options**
  - 1st FLOPPY DRIVE
  - USB-TEAC DU-203-U
  - SCSI: (Bus 05 Dev 00) LSI SW RAID
  - Disabled

---

f. Press the **F10** function key to save the changes and exit the BIOS utility.
Reinstalling the Cisco PAM Server Software from a Recovery CD

Step 6 Wait for the CD to install the Cisco PAM server software. When finished, the server will reboot again.

Step 7 After the server reboots, remove the Cisco PAM recovery CD from the server DVD-ROM drive.

Step 8 Configure the server as described in Initial Setup Instructions, page 3-7.

Step 9 Restore the system, as described in Restoring a Server Backup File, page A-8.
AppENDIX C

Upgrading and Configuring Gateway Modules

Use the Hardware and Locations & Doors modules to upgrade the firmware on one or more Gateway modules, or change the network settings on the modules. You can also change the NTP settings on multiple Gateway modules to ensure the time is synchronized on all devices.

Note
- We strongly recommend using NTP to synchronize the Cisco PAM appliance and Gateway module clocks to ensure correct event and messaging. See the “Change the NTP Setting for Multiple Gateways” section on page C-8 for instructions to set NTP on Gateway modules.
- The Gateway must be available on the network and in the Up state to use these configuration tools. For initial Gateway installation and configuration, see the Cisco Physical Access Gateway User Guide.

Contents

This appendix includes the following information:
- Displaying the Gateway Network and Firmware Configuration, page C-2
- Changing the Gateway Module Network Settings, page C-4
- Changing the NTP Setting for Multiple Gateway Modules, page C-7
  - (Optional) Set a Default NTP Server, page C-7
  - Change the NTP Setting for Multiple Gateways, page C-8
- Using Locations & Doors to Change Gateway Network Settings, page C-11
- Upgrading Gateway Firmware Images Using Cisco PAM, page C-12
  - Uploading Firmware Images to a TFTP Server, page C-12
  - Updating the Firmware on All Gateway Modules, page C-17
  - Updating the Firmware on Individual Gateway Modules, page C-22
Displaying the Gateway Network and Firmware Configuration

The Extended Status area of the Hardware module displays the network configuration and firmware version for a Gateway module.

**Procedure**

**Step 1** Select the **Hardware** module from the Doors menu.

**Tip** You can also view the Gateway settings from the Locations & Doors module. Filter the display to view the Gateway modules and then select a Gateway. See the “Using Locations & Doors to Change Gateway Network Settings” section on page C-11 for more information.

**Step 2** Expand the **Access GW Driver** and click a Gateway module icon to highlight it (Figure C-1).

The Gateway tab in the Extended Status area displays the Gateway software (firmware) version number, as well as the IP address used for network communication.

*Figure C-1  Gateway Software Version and IP Address Settings*
Tip

The IP address is the address configured on the Gateway Eth0 port, which provides IP network connectivity with the Cisco PAM appliance.

Step 3

Select the Gateway Network Address tab to display the module’s network configuration.
Changing the Gateway Module Network Settings

To change network configuration settings for a Gateway module using Cisco PAM, right-click a Gateway module and select Set Gateway Address.

Procedure

Step 1 Select the Hardware module from the Doors menu.
Step 2 Expand the Access GW Driver.
Step 3 Right-click a Gateway module and select Set Gateway Address (Figure C-2).

Tip You can also change the Gateway settings from the Locations & Doors module. Filter the display to view the Gateway modules and then right-click a Gateway name. See the “Using Locations & Doors to Change Gateway Network Settings” section on page C-11 for more information.

Step 4 Modify the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Address</td>
<td>If a Dynamic Host Configuration Protocol (DHCP) server is configured on your IP network, select the DHCP check box for ETH0 to automatically configure the required IP network settings, including IP address, Subnet Mask, and Gateway.</td>
</tr>
</tbody>
</table>

Figure C-2  Set Gateway Address
## Changing the Gateway Module Network Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address for the module Ethernet interfaces.</td>
</tr>
<tr>
<td></td>
<td>- The ETH0 interface provides IP network connectivity with the Cisco PAM appliance.</td>
</tr>
<tr>
<td></td>
<td>- The ETH1 interface is used for management connections, such as connecting a PC directly to the Gateway module.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The IP address of the default network gateway.</td>
</tr>
<tr>
<td>NTP Address</td>
<td></td>
</tr>
<tr>
<td>NTP Host</td>
<td>The IP Address of a network time protocol (NTP) server used to set the Gateway time. This setting is left blank if a DHCP server provides this setting.</td>
</tr>
<tr>
<td>DNS Server</td>
<td></td>
</tr>
<tr>
<td>Primary DNS Address</td>
<td>Enter the Primary DNS Address configuration if names (not IP addresses) are used for the NTP or CPAM addresses.</td>
</tr>
<tr>
<td>Secondary DNS Address</td>
<td>Enter the Secondary DNS Address configuration if names (not IP addresses) are used for the NTP or CPAM addresses</td>
</tr>
<tr>
<td>Primary Cisco PAM Server Address</td>
<td></td>
</tr>
<tr>
<td>Primary Cisco PAM Server</td>
<td>Enter the Cisco PAM IP Address (IP address or name) to enable Gateway communication with the appliance.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the Port number for the Cisco PAM appliance. The port number must be greater than 1024 and less 65535. The default is 8020.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>The secure socket layer (SSL) is enabled for secure communication between the Gateway and Cisco PAM appliance by default. If necessary SSL can be disabled by deselecting the Enable SSL check box.</td>
</tr>
</tbody>
</table>

**Note**: SSL is enabled by default on all Gateways and Cisco PAM appliances. If SSL is disabled for a Gateway but enabled for Cisco PAM, the Gateway will not be able to connect to the appliance. If the SSL settings are changed, reset all Gateways and the Cisco PAM appliance. We recommend enabling SSL to ensure secure communications.
Step 5  Click OK to save the changes.

Step 6  Right-click the Gateway 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 6-14.

Step 7  Verify that the new network settings appear in the Extended Status area, under the Gateway Network Address tab. See the “Displaying the Gateway Network and Firmware Configuration” section on page C-2.
Appendix C      Upgrading and Configuring Gateway Modules

Changing the NTP Setting for Multiple Gateway Modules

You can set the network time protocol (NTP) server for all Gateway modules, or for selected Gateway modules, to automatically synchronize the device time on the devices.

Usage Notes

- We strongly recommend using the same NTP setting for the Gateways and for the Cisco PAM appliance to ensure synchronized events and messaging. To set the server NTP address, see Chapter 3, “Configuring and Monitoring the Cisco PAM Server”. Other systems that are integrated with Cisco PAM, such as the Video Surveillance Manager (Cisco VSM), should use the same NTP server setting.
- If the Gateway is configured to receive an NTP server setting from DHCP, then the Set NTP Server command will not change the NTP server setting on that Gateway.
- You can also enter a default NTP server address to pre-populate the server field in the Set NTP Server window. This setting is not applied to the Gateways automatically. You must complete the instructions in the “Change the NTP Setting for Multiple Gateways” section on page C-8.

Refer to the following topics:

- (Optional) Set a Default NTP Server, page C-7
- Change the NTP Setting for Multiple Gateways, page C-8

(Optional) Set a Default NTP Server

The default NTP server address pre-populates the NTP Server setting when updating multiple Gateways. This default setting is optional, and is not applied to the Gateways until you complete the instructions in the “Change the NTP Setting for Multiple Gateways” section on page C-8.

Procedure

Step 1  Select System Configuration from the Admin menu.
Step 2  Select the Cisco Settings tab.
Step 3  Enter the IP address in the NTP Server field (Figure C-3).

Note  Enter an IP Address only. For example: 192.169.100.1. Hostnames are not supported.
Changing the NTP Setting for Multiple Gateway Modules

**Change the NTP Setting for Multiple Gateways**

Use the **Set NTP Server** command on the Access Gateway Driver to configure the same NTP server IP Address on multiple Gateways.

**Procedure**

**Step 1** (Optional) Enter a default NTP server setting to auto-populate the NTP Server field. See the “(Optional) Set a Default NTP Server” section on page C-7 for more information.

**Step 2** Select **Hardware** from the **Doors** menu.

**Step 3** Right-click the **Access GW Driver** and select the **Set NTP Server** command (Figure C-4).

---

**Figure C-3 System Configuration: NTP Server IP Address**

**Step 4** Restart Cisco PAM (exit and relaunch the application).

**Note** Changes do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

**Step 5** Continue to the following section: “Change the NTP Setting for Multiple Gateways” section on page C-8.

You must use the **Set NTP Server** command to apply the NTP server setting to one or more Gateways.
Changing the NTP Setting for Multiple Gateway Modules

Figure C-4 Set NTP Server for Multiple Gateways

Step 4 In the Set NTP Server window (Figure C-5), enter the following settings:

a. Enter the NTP server IP address.

Tip If an NTP server address was entered in the System Configuration, that address appears by default. You can edit the address if necessary. See the “(Optional) Set a Default NTP Server” section on page C-7 for more information.

b. Select All Gateways to select all available Gateways. Only Gateways in the UP state are displayed and available for NTP configuration.

c. Select or de-select Gateway modules in the list to include or exclude modules.

Figure C-5 Set NTP Server Configuration Window

Tip Use the Search field to locate and display a specific module.
Step 5  Click OK to save the changes.

Step 6  Select Yes when the confirmation message appears. The approximate time that the command will take to execute appears.

Step 7  Verify that the correct NTP address appears in the Extended Status area, under the Gateway Network Address tab. See the “Displaying the Gateway Network and Firmware Configuration” section on page C-2 for more information.

Note  If the Set NTP Server command is already in progress for one or more Gateways, you must wait for the summary event information to appear before you can use the command again.
Using Locations & Doors to Change Gateway Network Settings

You can use either the Hardware module or the Locations & Doors module to perform Gateway configuration tasks such as changing the network settings or configuring an NTP server for multiple Gateways.

To use the Locations & Doors module, select **Gateway Controllers** from the **View** menu, as shown in Figure C-6. The Gateways are displayed according to their assigned location. Any Gateways not assigned a location are listed under **Unassigned**.

**Figure C-6  Gateway Configuration Options in the Locations & Doors Module**

- Click a Gateway icon to display the network configuration and software (firmware) version in the Extended Status area. See the “Displaying the Gateway Network and Firmware Configuration” section on page C-2 for more information.
- To change the network configuration for a single Gateway, right-click the Gateway icon and select **Set Gateway Address**. See the “Changing the Gateway Module Network Settings” section on page C-4 for additional instructions.
- To change the NTP server address for multiple Gateways, right-click a site icon and select **Set NTP Server**. See the “Changing the NTP Setting for Multiple Gateway Modules” section on page C-7 for additional instructions.
Upgrading Gateway Firmware Images Using Cisco PAM

Gateway modules must have the same firmware version as the Cisco PAM appliance server software. This includes the major version, minor version, maintenance version, and the build number. If any difference in versions exists between the Gateway and the appliance, then only a restricted set of operations (such as image upgrade) can be performed.

For example, if the Cisco PAM appliance is upgraded to release 1.3.0, then all Gateway modules must also be upgraded to firmware release 1.3.0. 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 will be **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 one Gateway at a time.

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 C-12
- Updating the Firmware on All Gateway Modules, page C-17
- Updating the Firmware on Individual Gateway Modules, page C-22

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 C-22 and Updating the Firmware on All Gateway Modules, page C-17.

**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.
• 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 3-2.
b. Select the Monitoring tab and then select Status, as shown in Figure C-7.
c. If the TFTP Service is Down, click Start.
d. Verify that the TFTP service is Up.

Figure C-7  TFTP Service in “Up” State

Step 2  Log in to the Cisco PAM desktop client.
See Logging in to Cisco PAM, page 4-3.
Step 3  Select Image Manager from the Admin menu
Figure C-8 shows the Image Manager window. Table C-1 on page C-14 describes each field.
**Upgrading Gateway Firmware Images Using Cisco PAM**

---

**Table C-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. If using the built-in Cisco PAM TFTP server, this field is read-only. Select the directory path using the Remote Browser. If using a TFTP server other than the build-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. 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 built-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: Create Directory: Creates a directory. 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>
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 C-22.
Tip

To download an image from the TFTP server to a local directory, select the image and local directory, then click the Download button.
Appendix C      Upgrading and Configuring Gateway Modules

Upgrading Gateway Firmware Images Using Cisco PAM

Updating the Firmware on All Gateway Modules

This section describes how to upgrade or downgrade all the Gateways configured in a Cisco PAM server.

To upgrade the firmware for a single Gateway module, see Updating the Firmware on Individual Gateway Modules, page C-22.

Before You Begin

Review the following before upgrading the 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.
- Gateway modules must have the same firmware version as the Cisco PAM appliance server software. This includes the major version, minor version, maintenance version, and the build number. If any difference in versions exists between the Gateway and the appliance, then only a restricted set of operations (such as image upgrade) can be performed.
- 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 6-27 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-6.
- 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.

Step 1  Complete the instructions in Uploading Firmware Images to a TFTP Server, page C-12
Step 2  Log in to the Cisco PAM desktop client.
        See Logging in to Cisco PAM, page 4-3.
Step 3  Select Hardware from the Doors menu.
Step 4  Right-click the Access GW Driver and select Bulk Image Upgrade (Figure C-9).
Upgrading Gateway Firmware Images Using Cisco PAM

Appendix C      Upgrading and Configuring Gateway Modules

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 C-10), 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 that 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 C-14).
– **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-6.

---

**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 C-11**.

---

**Figure C-11  Bulk Image Upgrade Status**

---

c. Expand the **Bulk Image Upgrade** entry to view the upgrade status for each Gateway. The possible states include the following:
Upgrading Gateway Firmware Images Using Cisco PAM

Appendix C  Upgrading and Configuring Gateway Modules

- 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 C-12.

Figure C-12  Summary Event for Bulk Upgrade Command

Note  • 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 C-13.

*Figure C-13  File Manager Menu*

b.  Select the **Image** tab to display a list of the firmware images currently loaded on the Gateway module, as shown in Figure C-14.

*Figure C-14  File Manager Window: Image Tab*

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 C-15**.

---

**Figure C-15** *Reset Gateway Command*

---

**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 C-17**.

**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 6-27** 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-6.

Procedure

Step 1 Complete the instructions in Uploading Firmware Images to a TFTP Server, page C-12

Step 2 Log in to the Cisco PAM desktop client. See Logging in to Cisco PAM, page 4-3.

Step 3 Select Hardware from the Doors menu.

Step 4 Right-click a Gateway Controller (blue icon) and select File Manager (Figure C-16).

**Tip**
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 C-17).

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:

a. Select the **Initiate Download** button, as shown in Figure C-17.
   The Initiate Download Input window appears, as shown in Figure C-18.

![Figure C-18 Initiate Download Input Window](image)

b. Enter the **Image Name**:
   - If the image is located on the Cisco PAM TFTP server, click **Browse** (Figure C-18) to select a firmware image name.
   - If the image is located on a different TFTP server, enter the filename manually.

c. Enter the **TFTP Server IP address**.
   The Cisco PAM appliance TFTP server IP address is entered by default.

d. 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.

e. 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-6.

**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 C-19).

**Figure C-19**  **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 C-20.

Figure C-20  Reset Gateway Command
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 C-12.

To disable the TFTP server, complete the following steps.

**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 C-12 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 3-2.

**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*

Once the TFTP Service is Down, the button changes to Start. Click Start to enable the TFTP server.
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 E-1

Licensing: Frequently Asked Questions

This section provides answers to common licensing questions. For more information, see Obtaining and Installing Optional Feature Licenses, page 3-44.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<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</td>
<td>• CIAC-PAME-M64= is needed for up to 64 additional Cisco Modules</td>
</tr>
<tr>
<td>Cisco modules?</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=  
- The Web Services API feature requires CIAC-PAME-WSAPI= |
What is the process to acquire additional licenses?

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. See the “Obtaining and Installing Optional Feature Licenses” section on page 3-44.

What are Controller Conversion licenses for?

These are for supporting non Cisco access panels.

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
Related Documentation

Refer to the following documentation for additional information and instructions for the features and subjects discussed in this guide:

- Cisco Physical Access Control User Documentation, page F-1
- Cisco Video Surveillance Manager (Cisco VSM) User Documentation, page F-1
- Related Security Documentation, page F-2

Cisco Physical Access Control User Documentation

- Cisco Physical Access Control API Reference Guide
- Cisco Physical Access Manager User Guide
- Cisco Physical Access Manager Quick Start Guide
- Cisco Physical Access Gateway Quick Start Guide
- Cisco Physical Access Gateway User Guide
- Release Notes for Cisco Physical Access Control

Cisco Video Surveillance Manager (Cisco VSM) User Documentation

- Installing and Upgrading Cisco Video Surveillance Manager Release 6.3
- Video Surveillance Monitoring Workstation Recommended Baseline Specification
Cisco IP Interoperability and Collaboration System (IPICS) Documentation

- Cisco IPICS Documentation Roadmaps
- Cisco IPICS API Reference Guide
- Cisco IPICS End User Guide
- Cisco IPICS Server Administration Guide
- Cisco IPICS Documentation (links to all available technical documentation)

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
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.
<table>
<thead>
<tr>
<th><strong>C</strong></th>
<th><strong>Calendar</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Camera</strong></td>
<td>Cameras record digital video files to be stored on the DVR. See also: Closed Circuit Television</td>
</tr>
<tr>
<td></td>
<td><strong>CAN (Controller Area Network) bus</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Card</strong></td>
<td>See Badge.</td>
</tr>
<tr>
<td></td>
<td><strong>Card format</strong></td>
<td>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. See also: Wiegand See also: Magnetic Stripe</td>
</tr>
<tr>
<td></td>
<td><strong>Card format type</strong></td>
<td>The type of a card format, which may be Wiegand or magstripe. See also: Wiegand See also: Magnetic Stripe</td>
</tr>
<tr>
<td></td>
<td><strong>Card number</strong></td>
<td>The card number encoded within the badge, often on the magnetic stripe or internally for proximity cards. See also: Badge</td>
</tr>
<tr>
<td></td>
<td><strong>CCTV</strong></td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td></td>
<td><strong>CHUID/CUID</strong></td>
<td>Card Holder Unique Identity Model.</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco PAM client</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco PAM server</strong></td>
<td>An appliance used to manager 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.</td>
</tr>
<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>
<td></td>
</tr>
</tbody>
</table>
| **Credential** | A general category that includes login, badge, and biometric; something that is used to gain access to a physical or logical resource.  
See also: Login  
See also: Badge  
See also: Biometric |
| **Dashboard** | A module with real-time graphs, charts, and diagrams that is used for monitoring details and statistics for the system. |
| **Debounce** | 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.  
See also: Input point |
| **Dedicated Micros Driver** | A dedicated micros driver is a software device that manages the sending and receiving of data between the CCTV cameras and the DVR.  
See also: Driver |
| **Default Gateway** | In a network using subnets, the router that forwards traffic to a destination outside of the subnet of the transmitting device.  
See also: Subnet |
| **Department** | A sub-division of an organization, and used to organize personnel.  
See also: Organization |
| **Device** | 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. |
| **Device Status** | 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.  
See also: Top Alarm State |
| **Device status module** | 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. |
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 time-out 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 back up 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. This 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 can not 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).
**G**

**Gateway module**  
A device that can accept one 10 wire Wiegand reader, or two 5 wire Wiegand readers, three inputs, three outputs, power fail, and tamper sensor inputs. The gateway communicates with the CPAM server over TCP/IP over Ethernet. It also communicates up to 15 additional Reader, Input, or Output modules over a 3 wire CAN bus. The gateway can be powered via POE or 12V or 24V DC.

The Gateway can download badge access credentials and store them locally permitting access control even without network connectivity to the Cisco PAM server. Events that occur while the connection to the server is down are stored locally and uploaded to the Cisco PAM server once the network connection resumes.

**GND pins**  
Ground for the DC voltage input.

**Graphic maps editor**  
A module which allows graphic maps to be imported and configured. A graphic map can have links to other maps and or links to other devices. The map links can be used to navigate between maps in the graphic maps viewer. The device links show the real-time status of the device in the graphics maps viewer.

**Graphic maps viewer**  
A module allowing facility maps to be viewed. The Graphic maps viewer displays the location and status of devices within the facility. The maps can also contain links used to navigate to other maps.

**H**

**Hardware**  
See Device

**Hardware module**  
A module allowing operators to add, edit, and disable the hardware.

See also: Device

**Hardware tree**  
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.

See also: Device

See also: Hardware tree

See also: Hardware module

**Hexadecimal**  
A numbering system usually written using the symbols 0–9 and A–F or a–f.

**HID**  
A company manufacturing the industry standard proximity access-control cards.

See also: Proximity

**Hold time**  
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.
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.

L
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
M

**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 a 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.

O

**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 can not be powered via POE.

**Organization**
An organization with which a personnel record can be associated.

P

**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 Wiegand reader, or two 5 wire Wiegand 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.
S

Scroll lock  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.

Serial communications  A method of communicating over a dedicated line.

Site  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.

SSN  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.

SSL  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.

Status  See Device Status

Subnet  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.

Supervised input  A supervised input has 4 states. (1) Short (2) Open (3) Non-Alarm or (4) Alarm.

An unsupervised input has 2 states. (1) Normal or (2) Alarm.

Unsupervised inputs have limited functionality. If a wire is cut or shorted between the input module and a normally open device. The server cannot determine the change and the device would remains in inactive state even when the switch is closed.

To make the input device supervised, use two 1K resistors in the circuit.

- In the inactive state, the circuit measures 2000 ohms.
- In the active state, the circuit measures 1000 ohms.
- In the short state the circuit measures 0 ohms
- In the open state the circuit measures infinite ohms.

Once the input device is supervised, CPAM can determine if a wire is cut or shorted.

See also input and Input module. See Device Configuration Properties for more information.
### Glossary

**T**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP communications</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>Telnet</td>
<td>An Internet communications protocol that enables a computer to function as a terminal working from a remote computer.</td>
</tr>
<tr>
<td>Time interval</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>Time received</td>
<td>The time an event or alarm was actually received by the access-control system and stored in the database.</td>
</tr>
<tr>
<td>Time schedule</td>
<td>A defined set of time intervals used to make access-control, triggering, and other decisions. See also: Time interval</td>
</tr>
<tr>
<td>Time zone</td>
<td>24 longitudinal divisions of the globe, nominally 15 degrees wide, in which clocks show the same time.</td>
</tr>
<tr>
<td>TM input</td>
<td>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.</td>
</tr>
<tr>
<td>Top alarm</td>
<td>The most important alarm present at a given device. Based on alarm state, time, and priority. See also: Alarm and Alarm state</td>
</tr>
<tr>
<td>Top alarm state</td>
<td>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</td>
</tr>
<tr>
<td>Trigger</td>
<td>A trigger waits for an operator-defined combination of events, addresses, properties, and time schedules to occur, then executes a procedure. See also: Procedure</td>
</tr>
<tr>
<td>TTR</td>
<td>Triple Technology Reader. A reader which combines three devices in one: a magnetic card reader, HID proximity card reader, and piezoelectric keypad.</td>
</tr>
</tbody>
</table>

**U**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use limit</td>
<td>An option which can restrict a badge to a certain number of uses. The default is 0 (off). See also: Badge</td>
</tr>
<tr>
<td>Username</td>
<td>A sequence of characters used as identification when logging onto the application.</td>
</tr>
</tbody>
</table>

**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.

**Wiegand 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 Wiegand 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 Wiegand 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.
INDEX

A
Access Control Modules 6-5
Access GW Driver 6-4
ADA timespec multiplier 8-15
Alarms 12-8
Alert sounds 12-37
Anti-Passback Areas 11-19
Archived events 3-11
Audit trail records 12-13
Authenticate Credential 9-36
Automatic Backups A-2
Automation Driver 13-19

B
Badge Designer 1-17

C
Camera integration 14-2
Camera Inventory 15-28
Cisco Energywise 14-2
Cisco unified Call Manager (CUCM) 16-1
Cisco Video Surveillance Manager (Cisco VSM) 15-1
Cisco VSM Video Player 1-17
Cloning a Gateway 7-33
comma separated value (CSV) 9-16
Configure 1-5
Gateways
Doors 1-5
Credential Watch 12-18
CSV Import 13-28

D
Device Errors 6-15
Device I/O Rules 13-15
Devices 6-5
Device Status Colors 6-14
Digital media player (DMP) integration 14-2
Discovered configuration 6-2, 7-23
Door configuration templates 6-1
Door enable schedule 6-28
Door Modes 7-46
Door schedules 11-8
Door Sensor 6-24
Door Swing 6-24
Driver Manager 6-4

E
Edge Policies 13-9
EDI module 1-16
Electrostatic Discharge iii-xix
Enterprise Data Integration (EDI) 14-16
Events & Alarms 12-3

F
File Manager 7-42
Filter 4-12
First Unlock 6-31, 8-14
# Index

## G
- Gateway Controller 6-4
- Gateway template 1-10
- Graphic Map 5-4
- Graphic Map Editor 12-44
- Graphic Maps 12-40
- Graphic Maps Viewer 12-41
- Grid Arrangement 15-13
- Group Edit 4-14
- One-Time Manual Backup A-6

## P
- Personnel Fields Settings 17-12
- PIN generator 17-17
- Provisioned configuration 6-2, 7-23
- Pruned events 3-11

## Q
- Quick Launch buttons 13-2

## R
- Reader 6-24
- Really Simple Syndication (RSS) iii-xv
- redundant (HA) server configuration 3-16
- Relock interval time 8-29
- Reset Gateway Password 7-39
- REX 6-24

## S
- Scheduled mode 6-29
- Schedule Manager 11-8
- Server Backup File A-8
- Special Cases 11-16
- spurious events 8-36
- Squelch 7-44
- System Sanity Report 6-18

## T
- Time Entry Collections 11-18
- Time Ranges 11-16
- Two-Door Policies 11-27

## O
- Occupational Information 9-4

## K
- Keypad 8-22

## L
- Least Restrictive 5-2
- Lightweight Directory Access Protocol (LDAP) 5-12

## M
- Module Interface 6-5
- Most Restrictive 5-2

## H
- Holiday 11-14
- HSPD-12 Smart Card 9-34
Index

U
UCS Admin  3-16
Unsquelch  7-44
User Interface Elements  4-8

V
VSM Camera Driver 6X  15-20
VSM Camera Driver 7X  15-17

W
Watch Level  12-11
Wiegand  8-22
Wiegand Keypad  8-22
Work Weeks  11-14