Identiv Connected Physical Access Manager 2.1 User Guide

February 1, 2016

Identiv, Inc.
www.identiv.com

Text Part Number: IC01-01

Identiv
2201 Walnut Ave., Suite 310
Fremont, CA 94538

Phone:(949) 250-8888
Fax:(949) 250-7372
Web:www.identiv.com

Identiv and the Identiv logo are trademarks or registered trademarks of Identiv and/or its affiliates in the U.S. and other countries. To view a list of Identiv trademarks, go to this URL: http://www.identiv.com/legal.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR IDENTIV REPRESENTATIVE FOR A COPY.

The implementation of TCP header compression in this product is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. IDENTIV AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL IDENTIV OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF IDENTIV OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Identiv and the Identiv logo are trademarks or registered trademarks of Identiv and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Identiv and any other company. (1110R)

CONTENTS

Preface

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, e-mail Identiv technical support at:

support_icpam@identiv.com

or consult the Identiv website at:

http://www.identiv.com/support-icpam

For information on credential templates, refer to:

http://www.identiv.com/icpam-credential-templates

Safety Warnings

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

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

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

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

Warning **This unit might have more than one power cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit.** Statement 106

Warning **This is a Class A Information Product, when used in residential environment, it may cause radio frequency interference, under such circumstances, the user may be requested to take appropriate countermeasures.** Statement 257

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

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

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

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

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

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

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

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

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

Warning **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Warning **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

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

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

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

Warning **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

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

Warning **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

Warning **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 Identiv or 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- and Identiv-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.

CHAPTER 1

Overview

This user guide describes how to install and configure the Identiv Connected Physical Access Manager (ICPAM) and the ICPAM appliance using the ICPAM desktop software.

This chapter provides an overview of the main hardware and software components of the ICPAM appliance, and a summary of the chapters and topics included in this ICPAM User Guide.

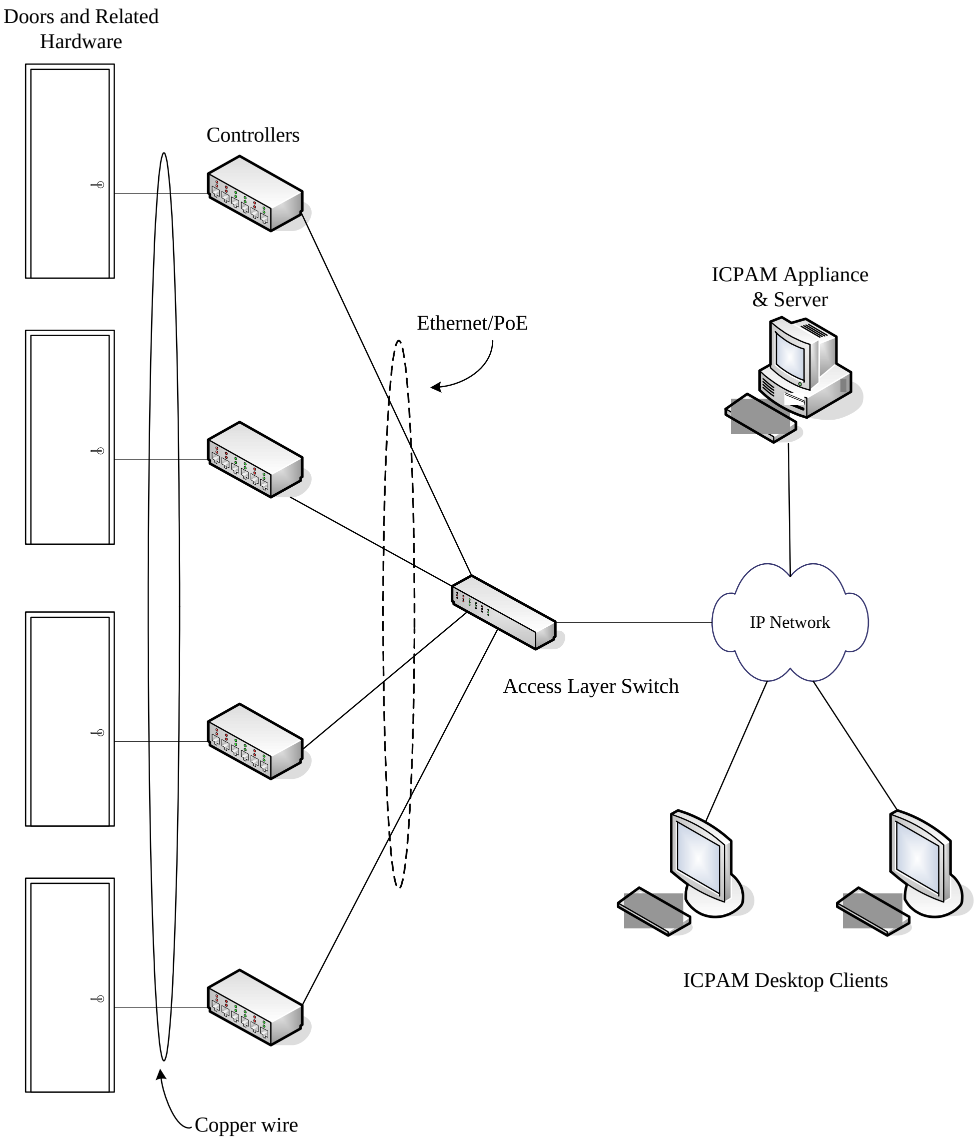
Note Throughout this guide, the generic terms ‘controller’ or ‘controller or gateway’ are generally used to describe both the Identiv EM-100 Edge controller and the Cisco gateway. In those places where the ICPAM applies only to the Cisco gateway, the term ‘Cisco gateway’ or ‘gateway’ is used. Similarly, in those places where the ICPAM applies only to the EM-100 Edge controller, the term ‘EM-100 controller’ is used.

Contents

Overview: ICPAM Physical Device Connections

The ICPAM appliance is a hardware and software solution that provides advanced configuration and management of the ICPAM system, as shown in Figure 1-1.

Figure 1-1 Identiv Connected Physical Access Control System



The ICPAM desktop client is used to define access control rules enroll users, manage badges, and configure the controller 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 *ICPAM Installation Guide* for instructions on how to install and configure controllers and door-related hardware.

Installation and Configuration Summary

Complete the following tasks to install and configure your ICPAM system.

- Install the Cisco Gateway Hardware and Software Components
- Install the EM-100 Edge Controller Hardware and Software Components
- Configure Doors and Users in ICPAM

Install the Cisco Gateway Hardware and Software Components

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

Step 2 Install and configure the server software. See Chapter 2, "Configuring and Monitoring the ICPAM Server"

Step 3 Install the desktop client. See Chapter 3, "Getting Started With the ICPAM Desktop Software"

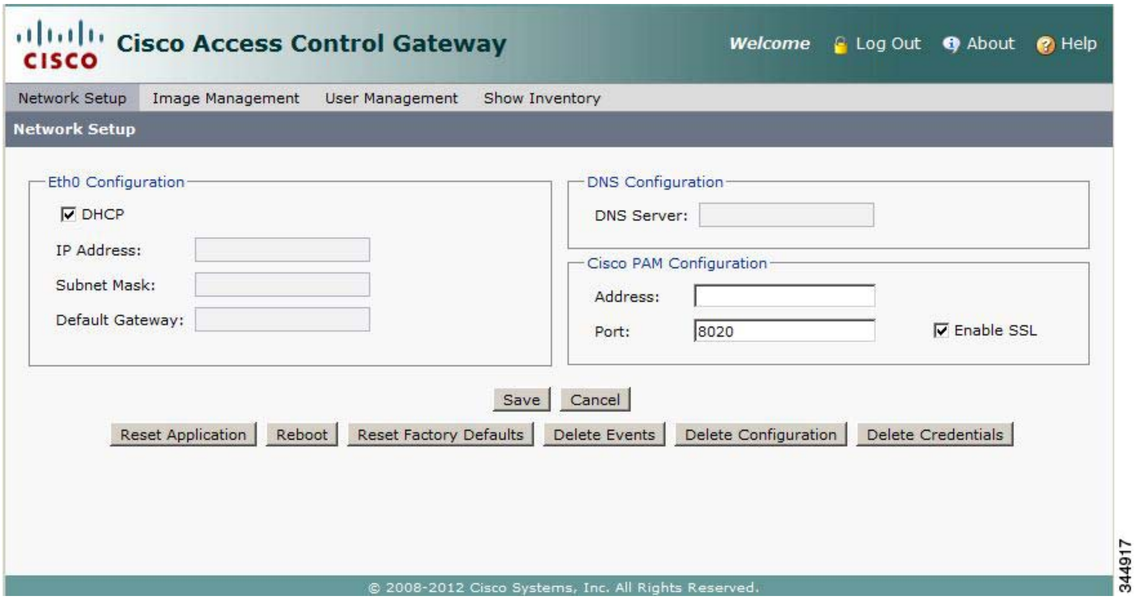
Step 4 Install the door devices, including locks, readers and other input and output devices.

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.*

Figure 1-2 Cisco Access Control Gateway



Network Setup

Eth0 Configuration

☑ DHCP

IP Address:

Subnet Mask:

Default Gateway:

DNS Configuration

DNS Server:

Cisco PAM Configuration

Address:

Port: 8020 ☑ Enable SSL

© 2008-2012 Cisco Systems, Inc. All Rights Reserved.

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 ICPAM, as described in Configure Doors and Users in ICPAM, page 1-5. For more information, see Provisioned (Pre-Populated) vs. Discovered Controller Configurations, page 5-1.

Step 8 Wait for the gateway to connect to the ICPAM appliance. Verify that the gateway status is *Up* in the Hardware Tree view (select **Hardware Tree** from the **Doors** menu in ICPAM).

Install the EM-100 Edge Controller Hardware and Software Components

Step 1 Install and configure the server software. See Chapter 2, "Configuring and Monitoring the ICPAM Server".

Step 2 Install the desktop client. See Chapter 3, "Getting Started With the ICPAM Desktop Software".

Step 3 Install the door devices, including locks, readers and other input and output devices.

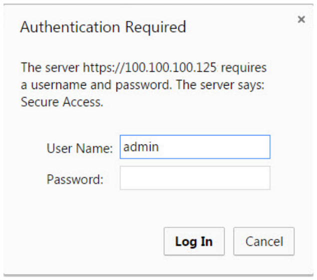
Step 4 Install the EM-100 Edge controller modules as described in *ICPAM Installation Guide*.

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

Step 5 Connect an Ethernet cable from a PC directly to the RJ-45 connector on the EM-100 controller.

Step 6 Open a browser on the connected PC and enter this default URL: **https://169.254.242.121.**

Step 7 From the Login window User Name field, enter **admin**.


Authentication Required

The server https://100.100.100.125 requires a username and password. The server says: Secure Access.

User Name: admin

Password:

Step 8 At the Password field enter **identiv123** then click **Login**.

Step 9 Follow the instructions on the web browser screen to configure the EM-100.

Most importantly, specify a fixed address or host name for this controller so that ICPAM can locate and configure this controller for use within the system.

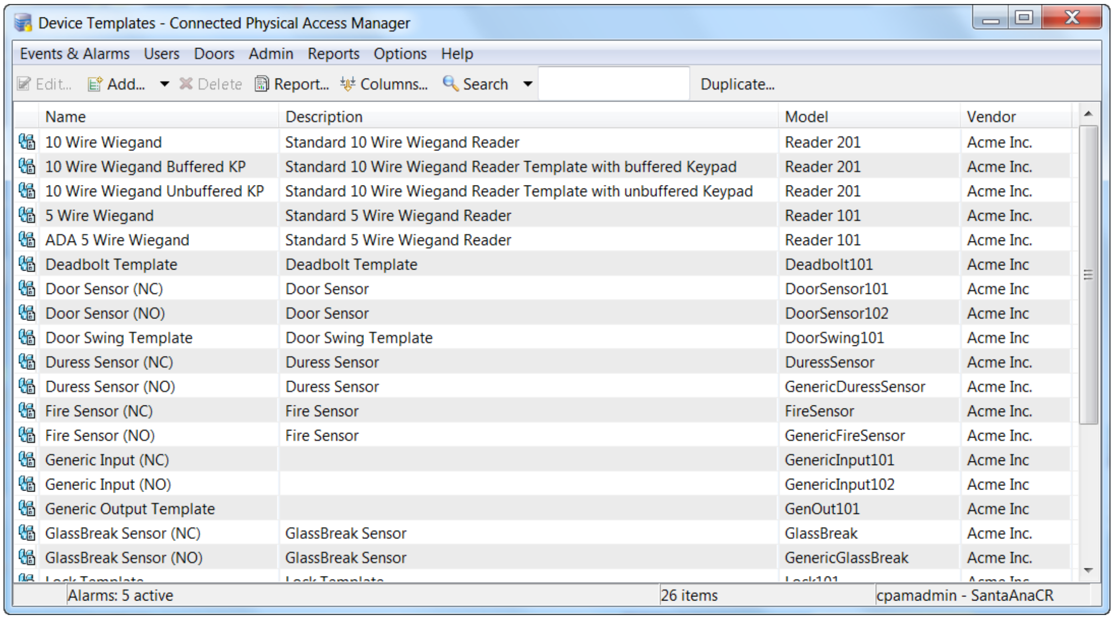
Step 10 Once configuration is completed, disconnect the Ethernet cable between the configuring computer and the EM-100, then connect the network cable (routed through the EM-100 faceplate) to the EM-100's RJ-45 socket.

Step 11 Wait for the controller to connect to the ICPAM appliance. Verify that the controller status is *Up* in the Hardware Tree view (select **Hardware Tree** from the **Doors** menu in ICPAM).

Configure Doors and Users in ICPAM

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

Step 1 Assign the appropriate device templates to the reader templates.



Name	Description	Model	Vendor
10 Wire Wiegand	Standard 10 Wire Wiegand Reader	Reader 201	Acme Inc.
10 Wire Wiegand Buffered KP	Standard 10 Wire Wiegand Reader Template with buffered Keypad	Reader 201	Acme Inc.
10 Wire Wiegand Unbuffered KP	Standard 10 Wire Wiegand Reader Template with unbuffered Keypad	Reader 201	Acme Inc.
5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
ADA 5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
Deadbolt Template	Deadbolt Template	Deadbolt101	Acme Inc
Door Sensor (NC)	Door Sensor	DoorSensor101	Acme Inc
Door Sensor (NO)	Door Sensor	DoorSensor102	Acme Inc
Door Swing Template	Door Swing Template	DoorSwing101	Acme Inc
Duress Sensor (NC)	Duress Sensor	DuressSensor	Acme Inc.
Duress Sensor (NO)	Duress Sensor	GenericDuressSensor	Acme Inc.
Fire Sensor (NC)	Fire Sensor	FireSensor	Acme Inc.
Fire Sensor (NO)	Fire Sensor	GenericFireSensor	Acme Inc.
Generic Input (NC)		GenericInput101	Acme Inc
Generic Input (NO)		GenericInput102	Acme Inc
Generic Output Template		GenOut101	Acme Inc
GlassBreak Sensor (NC)	GlassBreak Sensor	GlassBreak	Acme Inc.
GlassBreak Sensor (NO)	GlassBreak Sensor	GenericGlassBreak	Acme Inc.
Lock Template	Lock Template	Lock101	Acme Inc

Alarms: 5 active
26 items
cpamadmin - SantaAnaCR

Menu:

Doors > Templates > Device Templates

Instructions:

- Understanding Device Templates, page 5-24
- Understanding Virtual Credential Templates, page 5-24
- Understanding Gateway Credential Templates, page 5-25
- Configuring Device Templates, page 8-10
- To create additional credential templates, see Configuring Credential Templates, page 8-13.

Step 2 Configure controllers and doors:

a. Use gateway templates to add new controllers on the Hardware Tree menu.

b. Create the hierarchical location map (select **Door/Location-based Hardware** in the **Doors** menu).

c. To add doors to the locations, right click the controller driver then select **Add Doors...**

Note Cisco gateways and EM-100 controllers can be configured before connecting them to the network. You can also connect the modules to the network first, then complete the ICPAM configuration. See the "Provisioned (Pre-Populated) vs. Discovered Controller Configurations" section on page 5-1 for more information.

Menu:

Doors > Door/Location-based Hardware

Doors > Hardware Tree

Overview Information:

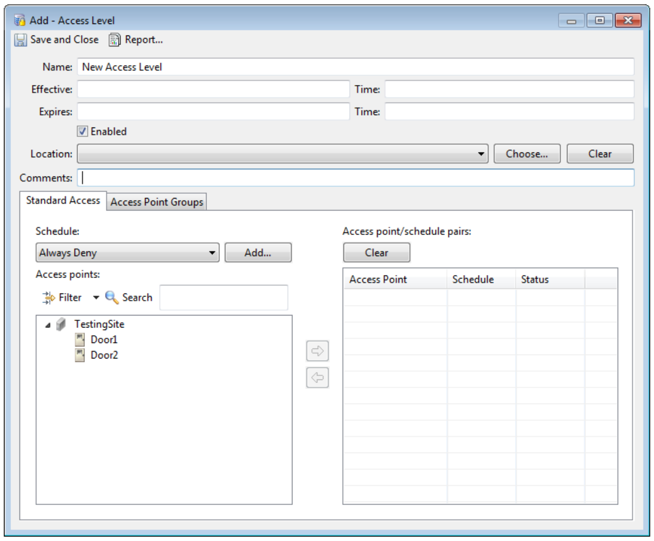
- Viewing Doors and Devices by Location, page 5-7
- Gateway Templates, page 5-23

Instructions:

- Creating the Location Map, page 5-8
- Configuring New Controllers, page 6-1
- Adding Doors Using Door Templates, page 7-2

Tip To create additional controller 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.



Add - Access Level

Name: New Access Level

☑ Enabled

Schedule: Always Deny

Access Point	Schedule	Status

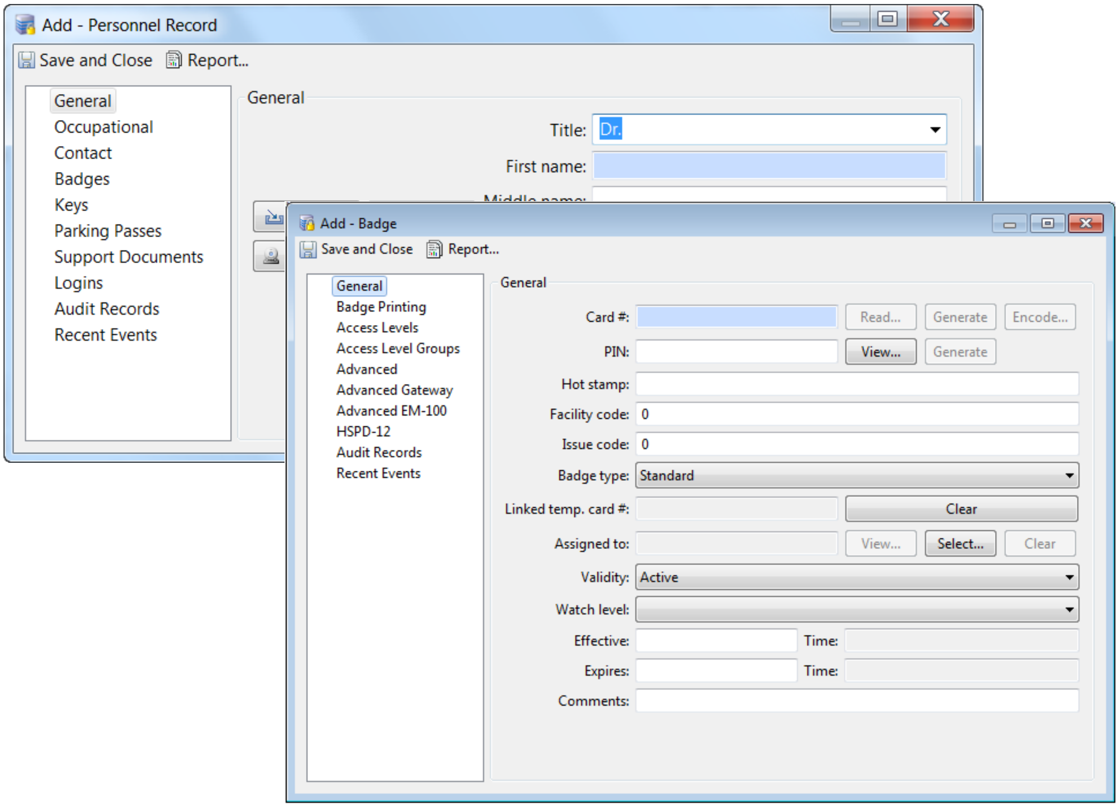
Menu:

Doors > Access Policies

Configuration Instructions:

- Chapter 11, "Configuring Access Policies"

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



Title: Dr.

Facility code: 0

Issue code: 0

Badge type: Standard

Validity: Active

Menu:

- **Users > Personnel**

Configuration Instructions:

- Chapter 9, "Configuring Personnel and Badges"

Step 5 Add the controller modules to the network:

a. Connect an Ethernet cable from a PC to the ETH1 interface on the gateway or the Ethernet interface on the controller.

b. Enter the controller's network settings.

c. Connect an Ethernet cable from the ETH0 interface on the Cisco gateway or the Ethernet connector on the Identiv EM-100 controller to the network.

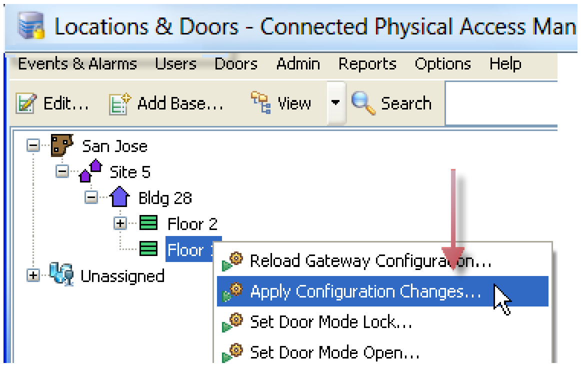
d. Wait for the controller or gateway to connect to the ICPAM appliance. Verify that the controller status is *Up* in the Hardware Tree view (select **Hardware Tree** from the Doors menu in ICPAM).

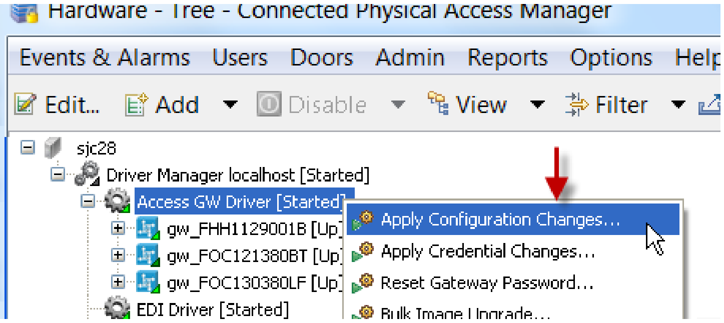
Tip Controllers are added to the ICPAM configuration in Step 2. You can also add the controllers to the network before configuring doors and users in ICPAM. See Provisioned (Pre-Populated) vs. Discovered Controller Configurations, page 5-1 for more information.

Instructions:

- *ICPAM Installation Guide*

Step 6 Right-click and select **Apply Configuration Changes** to apply configuration changes to the controller modules. Changes are not active until applied.




Hardware - Tree - Connected Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Edit...
Add
Disable
View
Filter
sjc28
Driver Manager localhost [Started]
Access GW Driver [Started]
gw_FHH1129001B [Up]
gw_FOC121380BT [Up]
gw_FOC130380LF [Up]
EDI Driver [Started]
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...

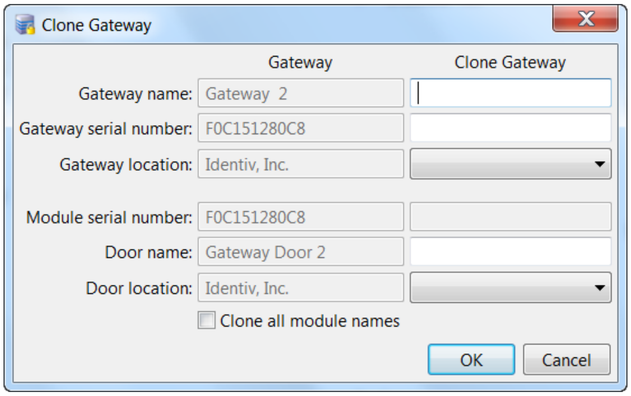
Menu:

- **Doors > Door/Location-based Hardware**
- **Doors > Hardware - Tree**

Configuration Instructions:

- Applying Configuration Changes, page 7-12

Step 7 (Optional) If this is a gateway, clone the new gateway and door configuration and apply it to another controller. This quickly adds an additional door to the ICPAM configuration. Enter the serial number and door name for the new controller or gateway module. Repeat this process as many times as necessary.


Clone Gateway

	Gateway	Clone Gateway
Gateway name:	Gateway 2	
Gateway serial number:	F0C151280C8	
Gateway location:	Identiv, Inc.	
Module serial number:	F0C151280C8	
Door name:	Gateway Door 2	
Door location:	Identiv, Inc.	

☐ Clone all module names

Menu:

Doors > Hardware Tree

Configuration Instructions:

- Creating Custom Gateway Configurations without Templates, page 6-2
- Cloning a Gateway Configuration, page 6-33

Tip You can also create a gateway template from the configuration.

If this is an EM-100 controller, save an existing controller as a ‘wizard template’ using this method:

a. **Doors** > **Hardware - Tree**

b. Expand the EM-100 driver.

c. Right click the EM-100 controller you wish to clone.

d. Select **Save as Wizard Template...**

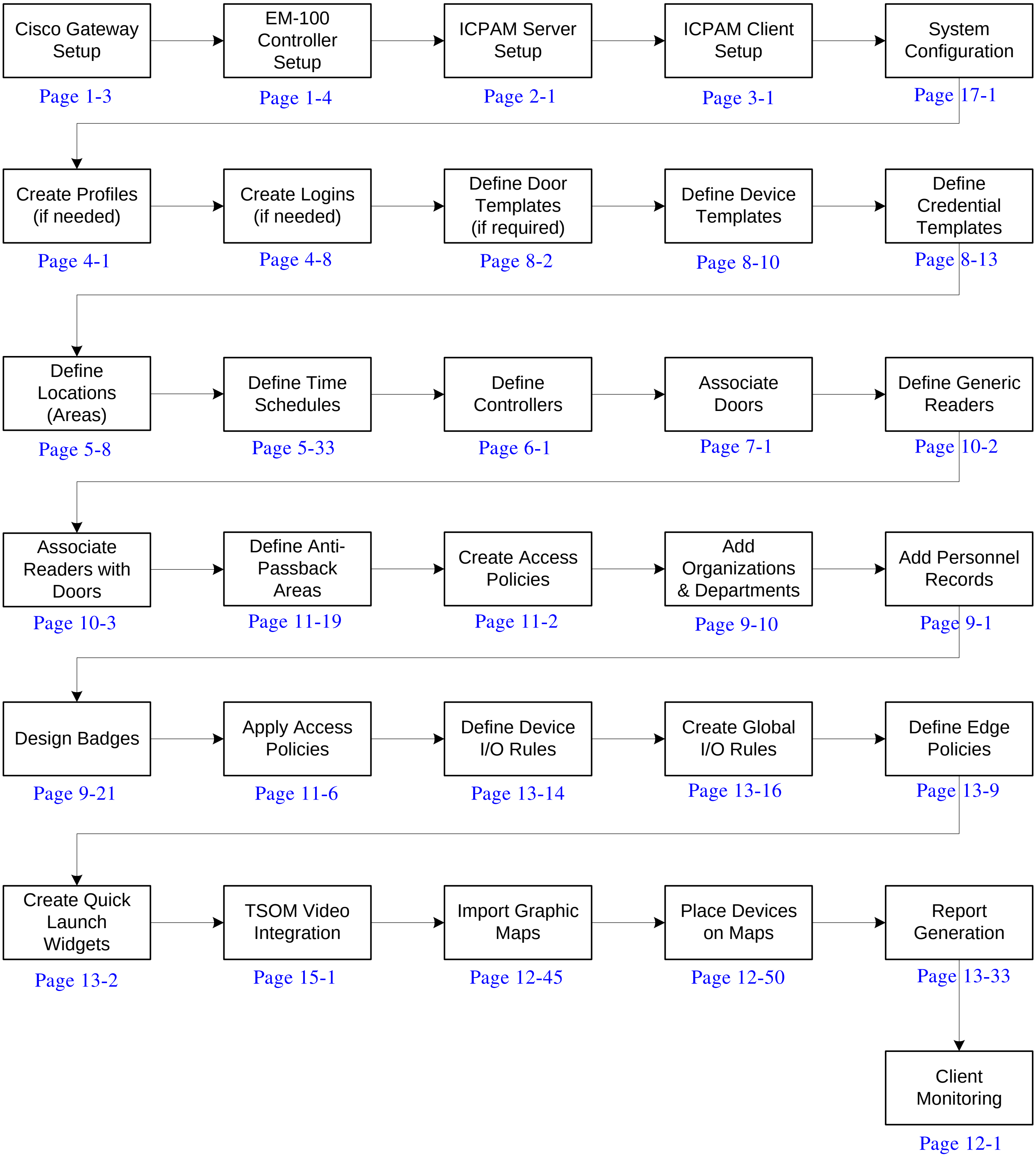
For more on this, refer to Creating Custom EM-100 Controller Configurations without Templates, page 6-15.

ICPAM Installation and Configuration Flowchart

Figure 1-3 on page 1-10 provides a guide to the installation and configuration of each procedure and feature required to run ICPAM, presented in the order in which they should be performed.

Note The starting page number of the section in this guide where each process is detailed appears below the step.

Figure 1-3 ICPAM Installation and Configuration Flowchart



System Recovery

In case of system crash, the Recovery ISO image can be used to bring back the system to normal state.

The ISO prompts for two input options. They are:

- **Factory**
- **Recovery**

If the user selects the input as **Factory**, the existing system is uninstalled completely and a new image is installed with zero license. The user can retrieve the original licenses by restoring the DB.

If the user selects the input as **Recovery**, the following happens:

- The database, ICPAM software are retained.
- A fresh OS is installed and the existing password is replaced as **cpamadmin**. This is provided as the password for the webadmin, ICPAM client and the SSH. The user is allowed to change the password later.
- The ETH0 IP address is retained but the rest of the NIC configurations is required to be manually configured. After configuring, the network and the immortal services are required to be restarted.
- The DNS server requires reconfiguration in webadmin.
- In case of HA, the server which is recovered will be standby server.
- RPM is not uninstalled in the recovered server. Hence, for a fresh ICPAM image to be installed the user should select Factory as input by using the recovery ISO image.

User Guide Contents

This User Guide describes how to install and configure the ICPAM appliance, and how to use the ICPAM desktop client to configure, manage, and monitor the Identiv Connected Physical Access Control system.

Table 1-1 describes the chapters and subjects included in this guide.

Table 1-1 Chapters and Features in the ICPAM

Chapter	Description
Chapter 1, "Overview"	Introduces the main ICPAM hardware and software components.
Chapter 2, "New and Changed Information"	New and Changed Information of the current release.
Chapter 2, "Configuring and Monitoring the ICPAM Server"	Describes how to configure the ICPAM server software, including optional feature licenses and high availability. This chapter also describes the additional server monitoring and configuration features of the ICPAM Server Administration utility.
Chapter 3, "Getting Started With the ICPAM Desktop Software"	Describes how to install the ICPAM desktop client software, log on to ICPAM, and begin configuring access control features and doors. This chapter also includes an overview of the ICPAM user interface.
Chapter 4, "Configuring User Access for the ICPAM Desktop Client"	Describes how to configure ICPAM operators.
Chapter 5, "Understanding Controller and Door Configurations"	Describes the terms and concepts used to configure doors and templates.

Table 1-1 Chapters and Features in the ICPAM

Chapter	Description
Chapter 6, "Configuring Controllers"	Describes how to configure the controllers and gateways for use with the ICPAM system.
Chapter 7, "Configuring Doors"	Describes how to configure doors, including how to clone controller or gateway configurations to quickly create another door.
Chapter 8, "Configuring Door and Device Templates"	Describes how to create and modify ICPAM door and device templates.
Chapter 9, "Configuring Personnel and Badges"	Describes how to create the personnel records and badges used to access doors in the Identiv Connected Physical Access Control system.
Chapter 10, "Multifactor Authentication"	Describes how to configure additional access control devices to ensure security. These devices are called as generic readers. These generic readers are biometric devices.
Chapter 11, "Configuring ICPAM Access Policies"	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.
Chapter 12, "Events & Alarms"	Describes how to view the event and alarm records in ICPAM, and how to use the Event Policy Manager to configure the log codes and other properties that define how events are captured and managed.
Chapter 13, "Configuring Automated Tasks"	Describes how to used to create and manage automated tasks to perform actions such as Trigger a relay when an alarm is generated, play alarm video, or generate a report and e-mail it to a user.
Chapter 14, "System Integration"	Describes how to use EDI to automatically synchronize ICPAM 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.
Chapter 15, "Video Monitoring"	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.
Chapter 16, "VoIP Integration"	Describes how to configure a VoIP phone to ICPAM as an additional feature to allow access to personnel without badges.
Chapter 17, "System Configuration Settings"	Describes the system-wide site settings available in the System Configuration module.
Appendix A, "Backing Up and Restoring Data"	Describes how to backup and restore the ICPAM database.
Appendix B, "Upgrading the Server Software"	Describes how to upgrade or reinstall the ICPAM server software, desktop client software, and controller module firmware.
Appendix C, "Upgrading and Configuring Gateways"	Describes how to configure network addresses, including IP addresses and an NTP server on the controller or gateway module using the ICPAM software. Also describes how to upgrade the module firmware.
Appendix D, "Security"	Provides security information related to the configuration and operation of the ICPAM software.
Appendix E, "Troubleshooting"	Describes troubleshooting techniques for the ICPAM software.
Appendix F, "Related Documentation"	Provides links to related ICPAM documentation, and documentation for related products.

Table 1-1 Chapters and Features in the ICPAM

Chapter	Description
Glossary	Provides definitions to terms used in the ICPAM system.
Index	Provides an index to subjects within the manual.

ICPAM Software Overview

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

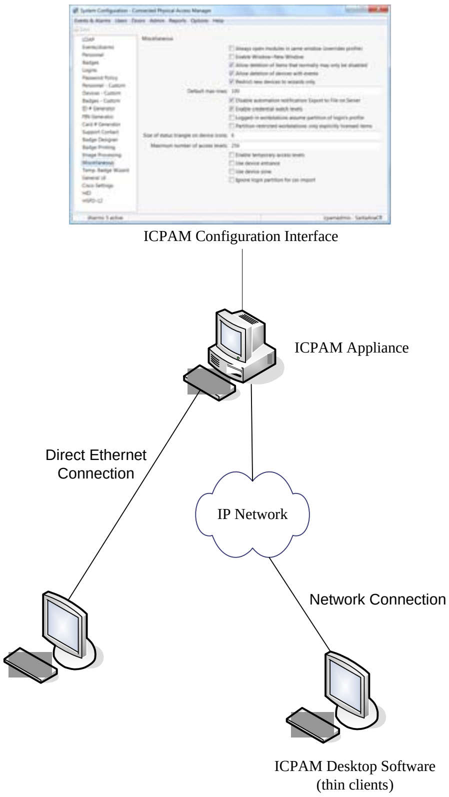
- ICPAM Desktop Client Software, page 1-14
- ICPAM Server Administration Utility, page 1-15
- Controller or Gateway Administration Utility, page 1-16
- The Enterprise Data Integration (EDI) Desktop Studio, page 1-17
- Cisco Video Surveillance, page 1-18
- Badge Designer, page 1-18

ICPAM Desktop Client Software

The ICPAM Manager (Figure 1-4) is a Java-based desktop client used to configure the ICPAM appliance and access control features.

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

Figure 1-4 ICPAM Context Diagram

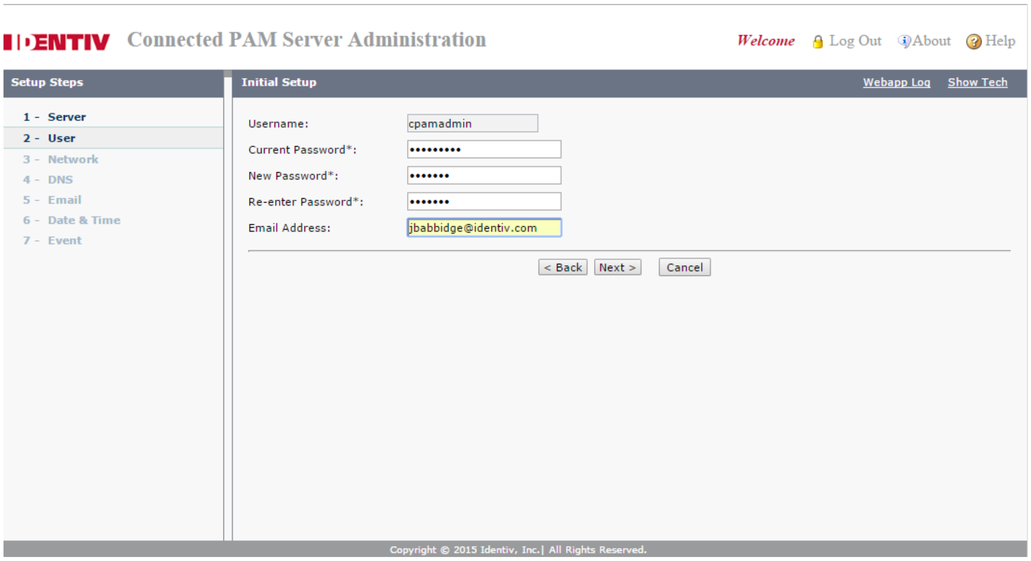

ICPAM Configuration Interface
ICPAM Appliance
Direct Ethernet Connection
IP Network
Network Connection
ICPAM Desktop Software (thin clients)

ICPAM Server Administration Utility

The ICPAM Server Administration utility (Figure 1-5) is a web-based tool used to configure and monitor the ICPAM appliance server software. Use this utility to set up a new server, install the desktop client software, back up data, install licenses, and perform a variety of other server maintenance and monitoring tasks.

See Chapter 2, "Configuring and Monitoring the ICPAM Server" for more information.

Figure 1-5 ICPAM Server Administration Utility



Setup Steps

1 - Server
2 - User
3 - Network
4 - DNS
5 - Email
6 - Date & Time
7 - Event

Initial Setup

Username: cpamadmin
Current Password*: •••••••••
New Password*: •••••••
Re-enter Password*: •••••••
Email Address: jbabbidge@identiv.com

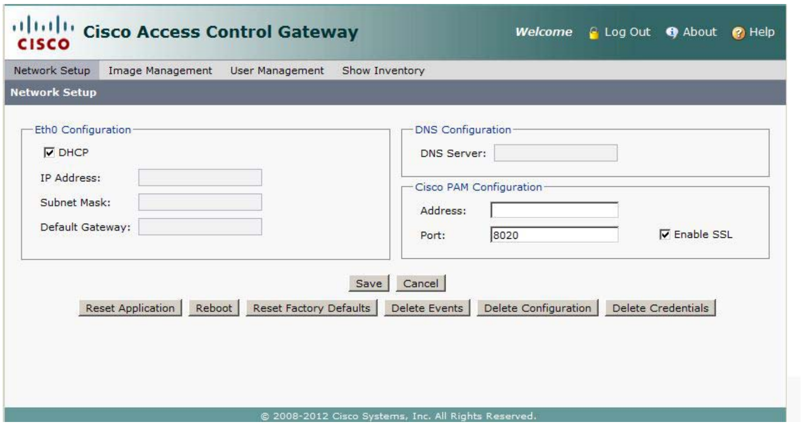
Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Controller or Gateway Administration Utility

The Cisco Gateway Administration utility (Figure 1-6) 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 1-6 Cisco Administration Utility



Eth0 Configuration

☑ DHCP

IP Address:

Subnet Mask:

Default Gateway:

DNS Configuration

DNS Server:

Cisco PAM Configuration

Address:

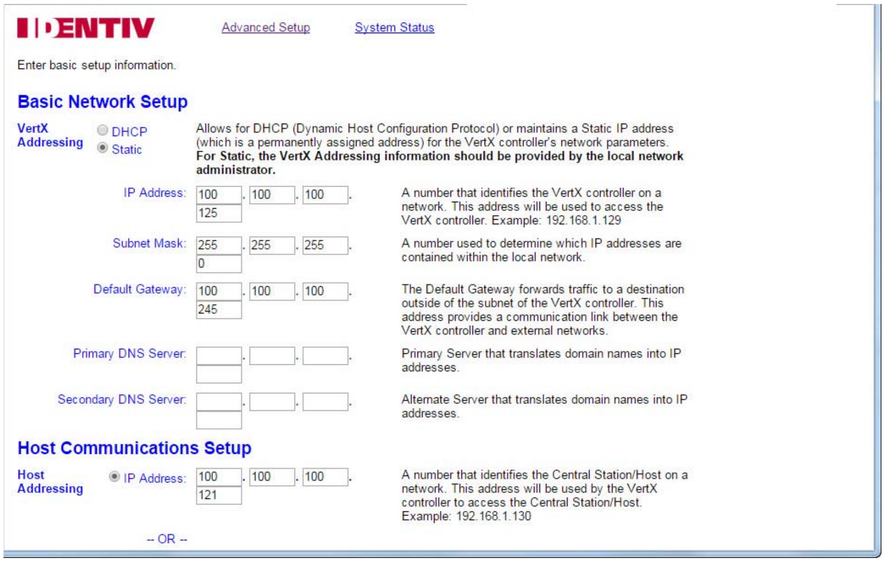
Port: 8020

☑ Enable SSL

The Identiv EM-100 Edge controller utility (Figure 1-7) uses a direct PC connection to enter the initial network settings for the controller. You can also use the utility to upgrade the controller's firmware and for other monitoring and maintenance tasks.

See the *ICPAM Installation Guide* for instructions on using this tool.

Figure 1-7 EM-100 Controller Setup Utility



Enter basic setup information.

Basic Network Setup

VertX Addressing ○ DHCP ● Static — Allows for DHCP (Dynamic Host Configuration Protocol) or maintains a Static IP address (which is a permanently assigned address) for the VertX controller's network parameters. **For Static, the VertX Addressing information should be provided by the local network administrator.**

IP Address: 100 . 100 . 100 . 125 — A number that identifies the VertX controller on a network. This address will be used to access the VertX controller. Example: 192.168.1.129

Subnet Mask: 255 . 255 . 255 . 0 — A number used to determine which IP addresses are contained within the local network.

Default Gateway: 100 . 100 . 100 . 245 — The Default Gateway forwards traffic to a destination outside of the subnet of the VertX controller. This address provides a communication link between the VertX controller and external networks.

Primary DNS Server: . . . — Primary Server that translates domain names into IP addresses.

Secondary DNS Server: . . . — Alternate Server that translates domain names into IP addresses.

Host Communications Setup

Host Addressing ● IP Address: 100 . 100 . 100 . 121 — A number that identifies the Central Station/Host on a network. This address will be used by the VertX controller to access the Central Station/Host. Example: 192.168.1.130

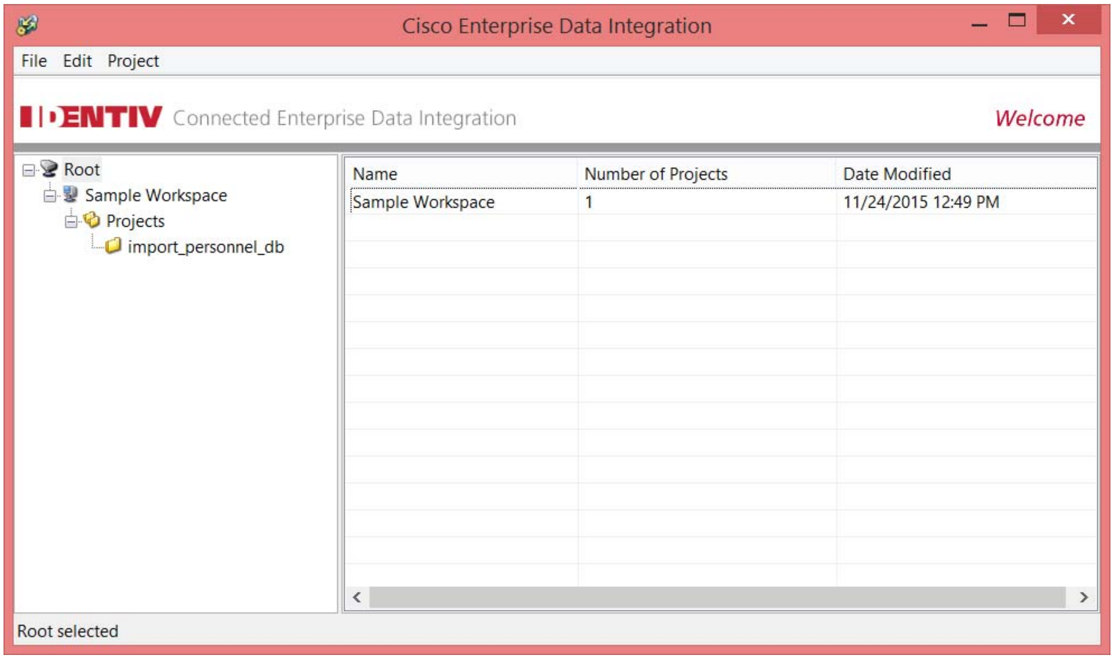
-- OR --

The Enterprise Data Integration (EDI) Desktop Studio

The EDI Studio (Figure 1-8) is a desktop application used to create data integration projects for automatically synchronizing ICPAM 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 ICPAM.

See Chapter 14, "System Integration" for more information.

Figure 1-8 EDI Studio Desktop Software



Name	Number of Projects	Date Modified
Sample Workspace	1	11/24/2015 12:49 PM

Note This feature requires an optional ICPAM license. The **EDI** menu appears only after the license is installed on the ICPAM server. See the "Obtaining and Installing Optional Feature Licenses" section on page 2-44 for more information.

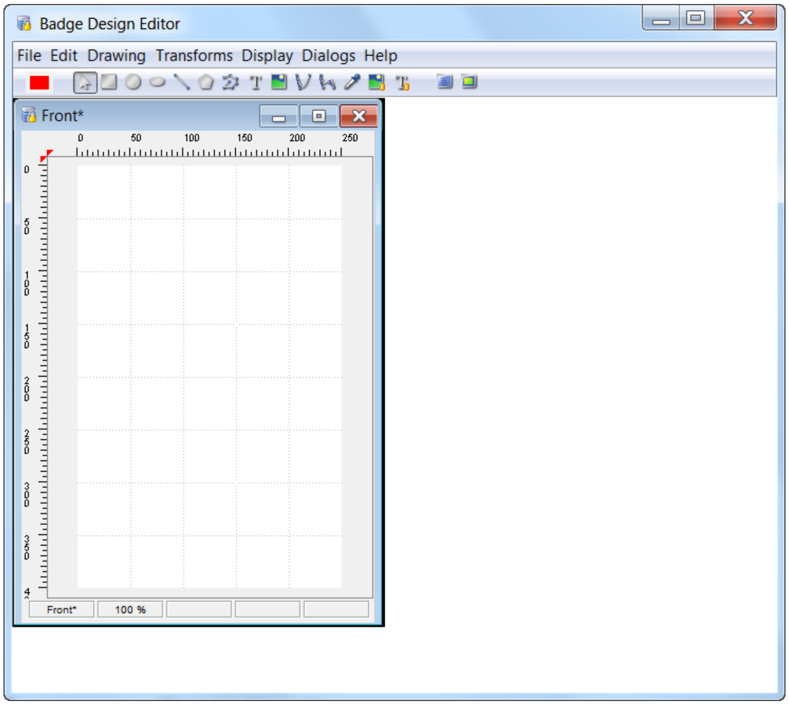
Cisco Video Surveillance

The Cisco VSM Video Player is a desktop application used to archived video from the Video Surveillance Manager. See Chapter 15, "Video Monitoring" for more information.

Badge Designer

The Badge Format (Figure 1-9) feature is included with the optional Badge Designer module to create and modify badge designs. See Chapter 9, "Configuring Personnel and Badges"for more information on designing and modifying badges.

Figure 1-9 Badge Format



CHAPTER 2

Configuring and Monitoring the ICPAM Server

This chapter describes how to configure the ICPAM server software, including optional feature licenses and high availability. This chapter also describes the additional server monitoring and configuration features of the ICPAM 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 ICPAM desktop client software and additional feature licenses. A variety of other configuration and monitoring tasks can also be performed.

Contents

Overview

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

Refer to the following topics:

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

About the ICPAM Server Administration Utility

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

- When you access the utility for the first time, the initial setup screens appear. See Entering the Initial Server Configuration, page 2-5.
- After the initial server configuration is complete, see Using the Web Admin Menus, Commands and Options, page 2-18.

Note The ICPAM 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 ICPAM Desktop Software, page 3-2.

Logging on to the ICPAM Server Administration Utility

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

- Connect a PC directly to the server Eth0 port, as described in Entering the Initial Server Configuration, page 2-5.
- Log in to the ICPAM 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 ICPAM 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 ICPAM appliances in a redundant configuration. One appliance acts as the active server, and the second appliance 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 2-44.

Understanding IP Addresses on the ICPAM Server

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

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

- ICPAM Appliance IP Addresses, page 2-3
  - Eth0 Port IP Address, page 2-3
  - Shared IP Address, page 2-3
  - Eth1 Port IP address, page 2-4
- Upgrading a Single Standalone Server to an HA Configuration, page 2-4
- Controller and Gateway Module IP Addresses, page 2-4

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

ICPAM 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 ICPAM appliance and the controller or controllers. The *Eth0* IP address is also used to log on to the ICPAM 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 controller or controllers 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 ICPAM Server Administration utility, and is configured on each controller.
- 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 ICPAM 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 controllers.

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 ICPAM 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.

Controller and Gateway Module IP Addresses

The Identiv EM-100 Edge controller and Cisco gateway module are configured with the following field values:

- **ICPAM Configuration**—defines the IP address and port of the ICPAM appliance used to manage the controller. This can be either the Eth0 address in a standalone configuration, or the Shared IP address in an HA configuration. See the "ICPAM Appliance IP Addresses" section on page 2-3.
- **Eth0**—defines the network settings for the Eth0 port on the Cisco gateway. Eth0 is used for network connectivity with the ICPAM appliance.
- **IP Address**—defines the network setting for the Ethernet port on the Identiv EM-100 Edge controller. This address is used for communication between the ICPAM appliance and the network.
- **ICPAM Configuration Address**—defines the IP address for the ICPAM appliance to which the Identiv EM-100 Edge controller is connected. There is also a port address that must be designated for the EM-100 controller.
- **DNS**—defines the domain name server (DNS) if names, not IP addresses, are used for the NTP or ICPAM addresses.

For instructions to install and configure Cisco gateway modules, see the Cisco Physical Access Gateway User Guide. For instructions for installing and configuring the EM-100 Edge controller, see the ICPAM Installation Guide.

To use ICPAM to configure gateway network settings, see the "Changing the Gateway Network Settings" section on page C-3.

Entering the Initial Server Configuration

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

- Before You Begin, page 2-5
- Connecting a PC to the Appliance, page 2-5
- Initial Setup Instructions, page 2-7

Before You Begin

Before you power on the ICPAM 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 ICPAM appliance. Cross-over and straight-through cables are supported.

In addition, gather the following information:

- IP, subnet, and gateway addresses for the ICPAM 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 ICPAM Server, page 2-3.
- (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 ICPAM configuration, connect an Ethernet cable from a PC to the ICPAM 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 ICPAM 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 Power on the appliance. See *Cisco Physical Security Multi Services Platform User Guide* or *Cisco Physical Access 1125 Appliance User Guide* for the location of the power button.

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

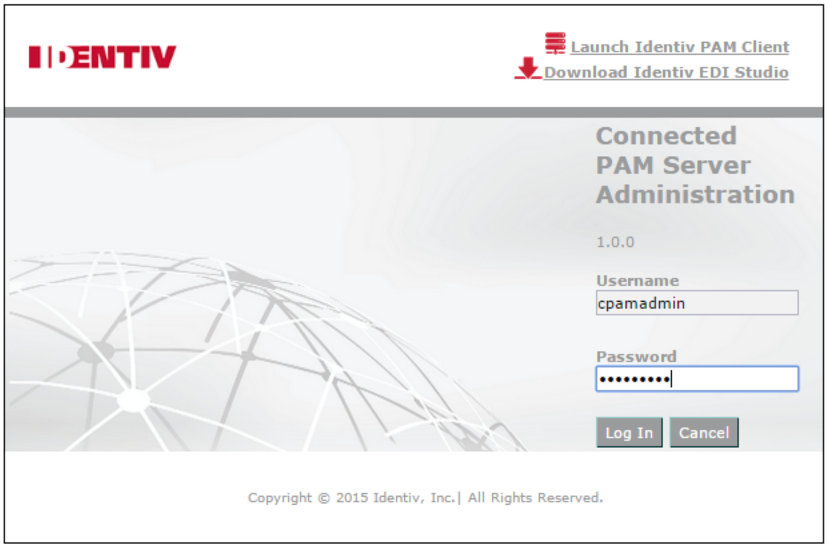
Note Be sure to include the *s* in *https://*. This connects your browser to the secure URL.

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

default username: **`cpamadmin`**

default password: **`cpamadmin`**

Figure 2-1 ICPAM Server Administration Utility: Login



IDENTIV
Launch Identiv PAM Client
Download Identiv EDI Studio
Connected
PAM Server
Administration
1.0.0
Log In
Cancel
Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Username: cpamadmin

Password: •••••••••

Tip The default **`cpamadmin`** password is used the first time you log into the active or standby appliance. You are required to configure a new password during the initial setup process, as described in Initial Setup Instructions, page 2-7. The **`cpamadmin`** username cannot be changed.

Note See Changing or Recovering the Server Password, page 2-40 for more information.

Initial Setup Instructions

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

Step 1 Log on to the appliance, as described in Connecting a PC to the Appliance, page 2-5.

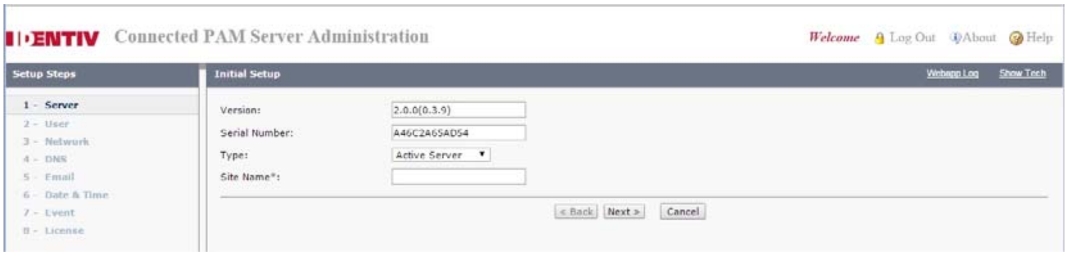
Step 2 Enter the server configuration, as shown in Figure 2-2:

Note The version and serial number are not configurable.

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

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

Figure 2-2 Initial Setup: Server Configuration



Version: 2.0.0(0.3.9)
Serial Number: A46C2A65AD54
Type: Active Server
Site Name*:

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

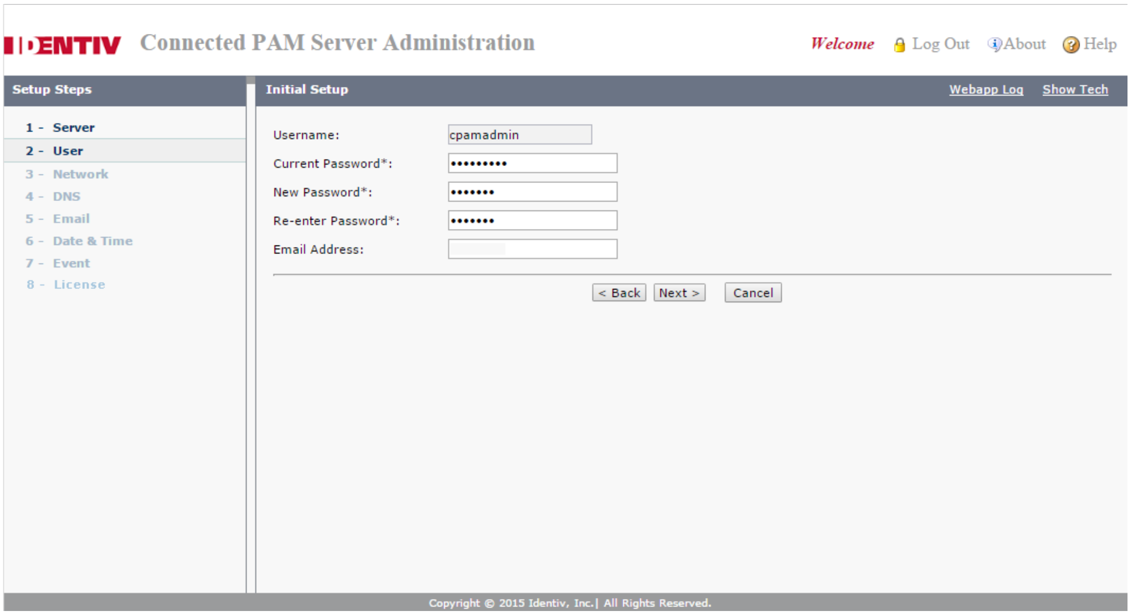
Enter any combination of letters and numbers up to 32 characters. Spaces are not allowed. Dashes and underscore characters are allowed.

Example: `SJCSite1`.

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

Step 3 Enter the initial User settings to define the administrator password and email address, as shown in Figure 2-3. Enter the same settings on the active and standby appliance.

Figure 2-3 Initial Setup: User Configuration



Username: cpamadmin
Current Password*: •••••••••
New Password*: •••••••
Re-enter Password*: •••••••
Email Address:

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

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

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

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

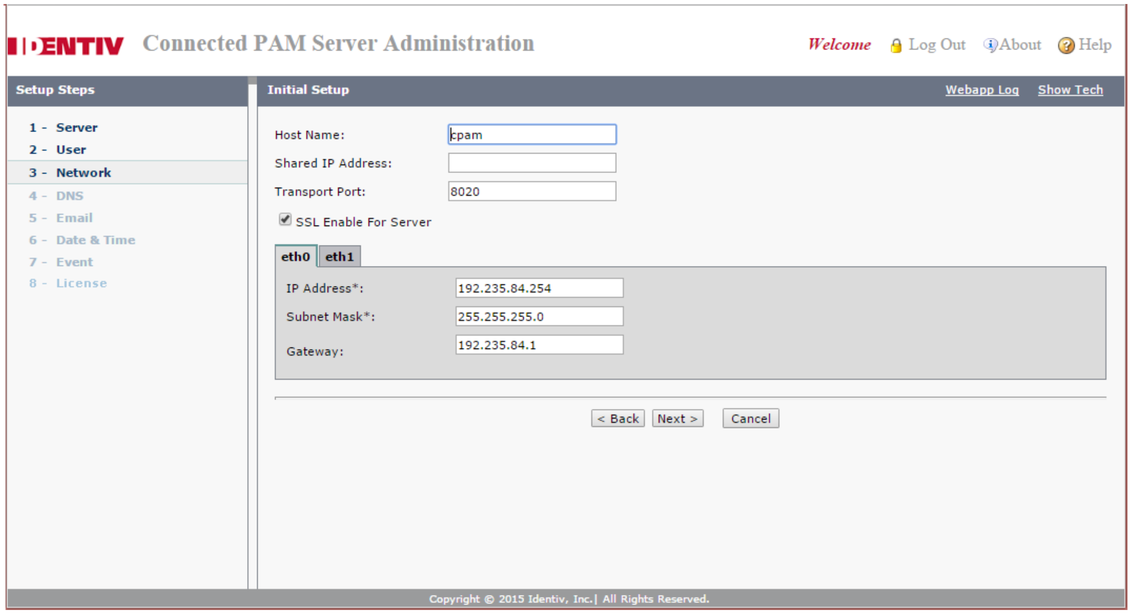
e. **Email Address**: (Optional) Enter the email address that will receive system messages. This email address also receives Forgot Password emails (see Resetting a Forgotten Password, page 2-41).

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

Step 4 Enter the Network configuration for the ICPAM appliance, as shown in Figure 2-4.

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

Figure 2-4 Initial Setup: Network Configuration



Host Name: cpam

Shared IP Address:

Transport Port: 8020

☑ SSL Enable For Server

IP Address*: 192.235.84.254

Subnet Mask*: 255.255.255.0

Gateway: 192.235.84.1

Complete the following Network settings:

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

b. **Shared IP Address**: 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 ICPAM Server, page 2-3 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** check box to enable or disable secure IP communication between the ICPAM appliance and attached controllers. The settings must be the same on the active and standby appliances.

Note SSL is enabled by default on all controllers and ICPAM appliances. If SSL is disabled for a controller but enabled for ICPAM, the controller will not be able to connect to the appliance. If the SSL settings are changed, reset all controllers and the ICPAM appliance. Identiv recommends enabling SSL to ensure secure communications.

e. **Eth0**: (Required) Enter a static IP address for the Eth0 port. If the appliance is a standalone server, this port is the ICPAM 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 ICPAM Server, page 2-3 for more information.

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

f. **Eth1**: This port is disabled by default. You can enable and configure the Eth1 port for remote Internet connections to the ICPAM 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 ICPAM 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 ICPAM appliance. Enter the same settings on the active and standby appliance.

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

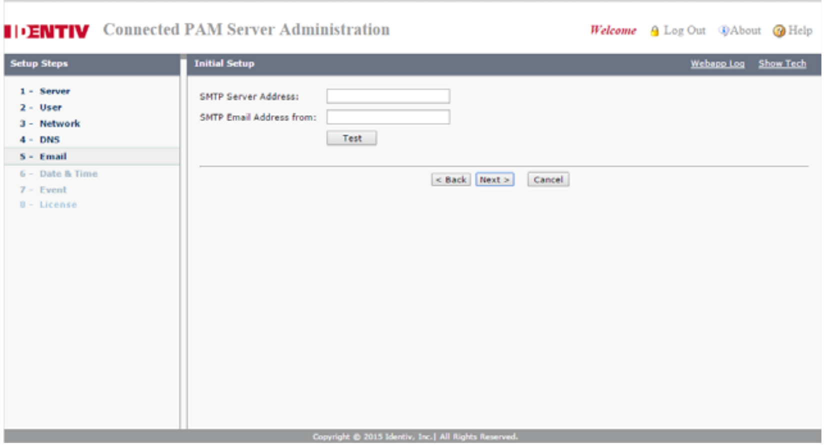
b. **Secondary DNS**: (Optional) Enter the secondary DNS.

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

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

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

Figure 2-5 Initial Setup: Email Configuration



SMTP Server Address:

SMTP Email Address from:

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

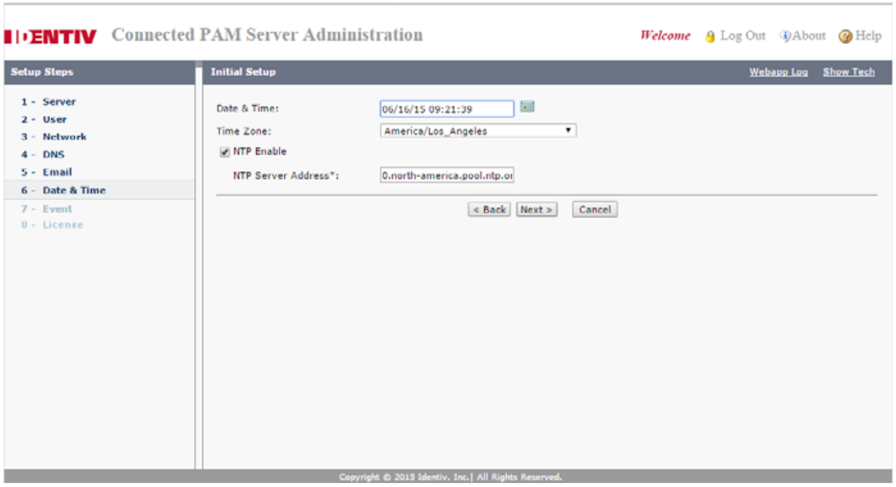
b. **SMTP Email Address from**: Enter the email address that will appear in the From field for messages sent by the ICPAM appliance. This email address is also the Reply To address.

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 Gateways. Enter the same settings on the active and standby appliance.

Figure 2-6 Initial Setup: Date & Time Configuration



Date & Time: 06/16/15 09:21:39

Time Zone: America/Los_Angeles

☑ NTP Enable

NTP Server Address*: 0.north-america.pool.ntp.or

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 check box to enable use of an optional Network Time Protocol server, used to automatically adjust the date and time for the ICPAM appliance.

Note We strongly recommend using NTP to synchronize the ICPAM appliance and controller clocks to ensure correct event and messaging. See the "Changing the NTP Setting for Multiple Gateways" section on page C-6 for more information.

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

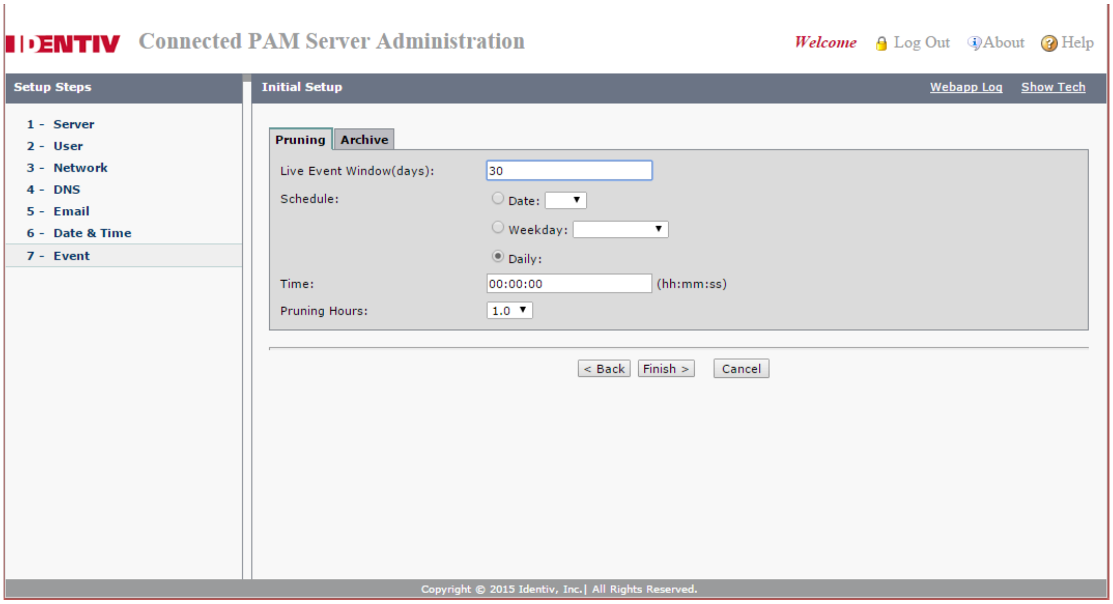
i. Select **Next** to apply the settings and continue.

Step 8 Enter the Event pruning and archiving settings, as shown in Figure 2-7.

- 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 ICPAM 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 ICPAM 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 2-25 for more information.

a. Select the **Pruning** tab (Figure 2-7), and enter the following settings:

Figure 2-7 Initial Setup: Event Pruning and Archiving



IDENTIV Connected PAM Server Administration

Welcome Log Out About Help

Setup Steps

1 - Server
2 - User
3 - Network
4 - DNS
5 - Email
6 - Date & Time
7 - Event

Initial Setup Webapp Log Show Tech

Pruning | Archive

Live Event Window(days): 30

Schedule: ○ Date: ▼
○ Weekday: ▼
● Daily:

Time: 00:00:00 (hh:mm:ss)

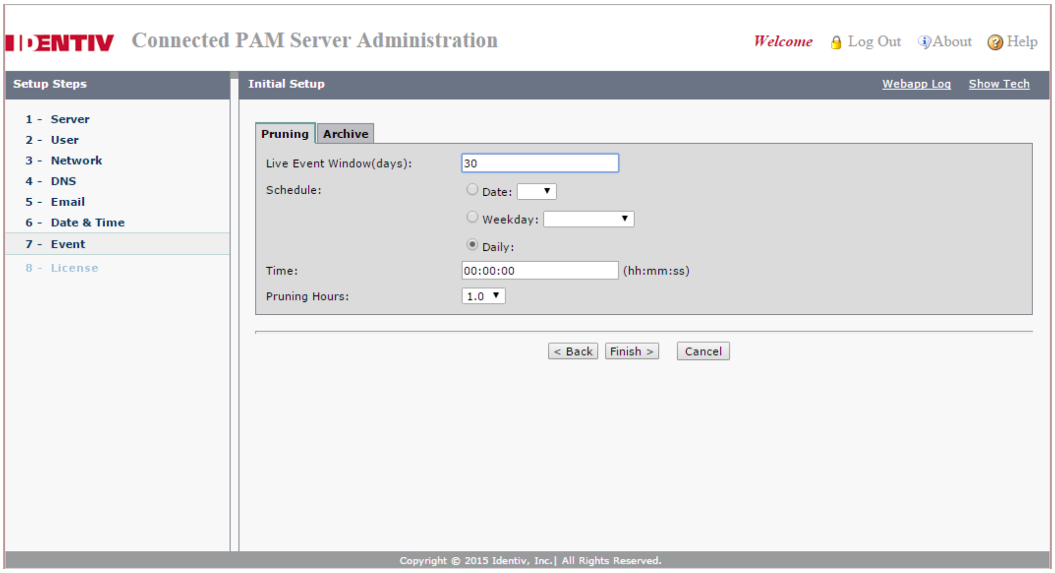
Pruning Hours: 1.0 ▼

< Back | Finish > | Cancel

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

- **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.

Figure 2-8 Pruning Hours



Live Event Window(days): 30

Schedule: ○ Date: ▼ ○ Weekday: ▼ ● Daily:

Time: 00:00:00 (hh:mm:ss)

Pruning Hours: 1.0 ▼

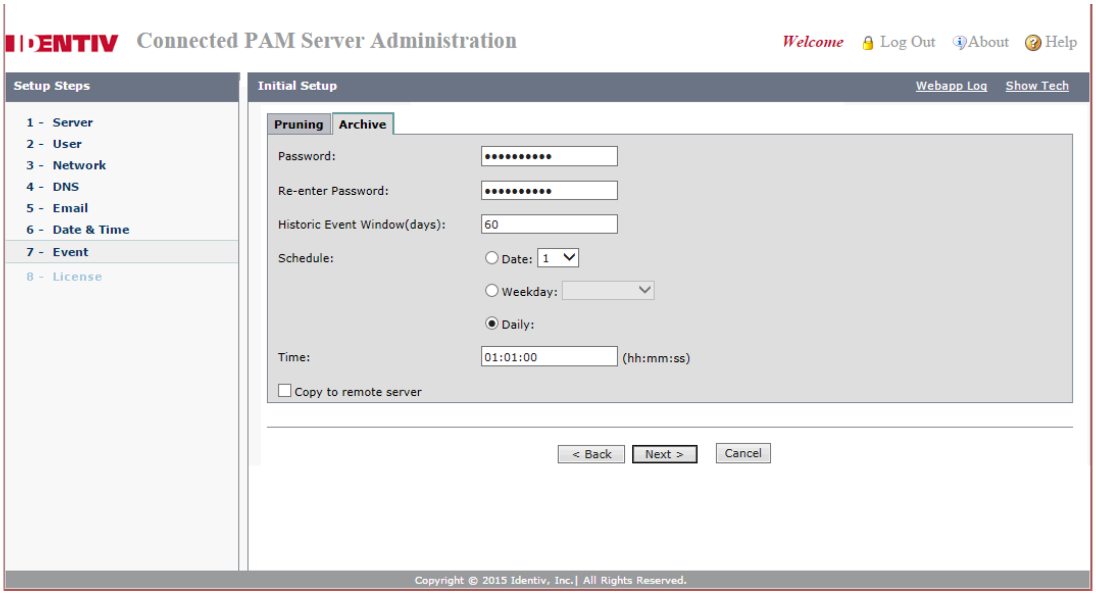
- For other options in Schedule, the Pruning Hours field is read-only.See Figure 2-7.

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 2-9) and enter the following settings:

Figure 2-9 Archiving Events



Password: ••••••••••

Re-enter Password: ••••••••••

Historic Event Window(days): 60

Schedule: ○ Date: 1 ○ Weekday: ● Daily:

Time: 01:01:00 (hh:mm:ss)

□ Copy to remote server

Tip The archive settings are required during the initial setup. After a the server is up, you can disable auto-archiving if necessary. See the "Archiving Historical Events" section on page 2-25.

- 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.

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.

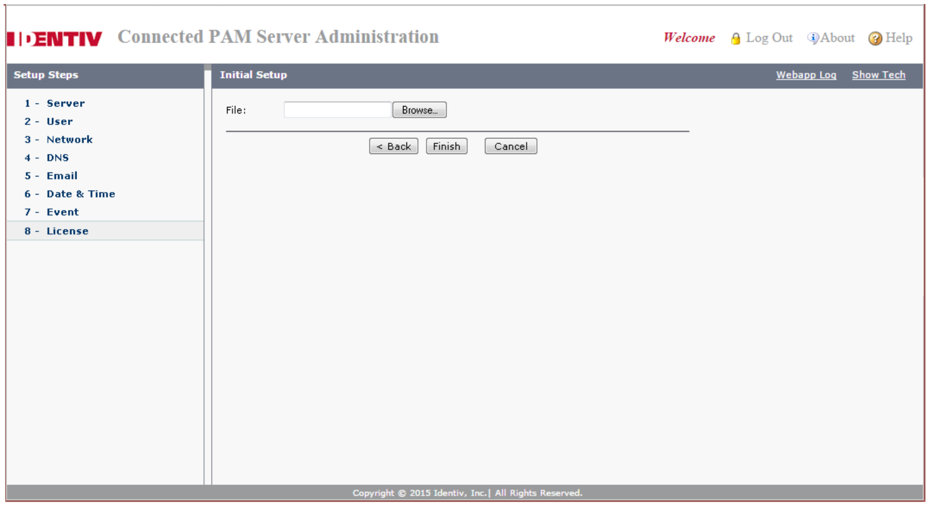
c. Select **Next** to apply the settings and continue.

Tip Pruning and Archiving schedules must not overlap each other.

Step 9 Install the software license.

Note The License option only appears before this copy of ICPAM is registered. Once the license for this software is authenticated, the option no longer appears.

Figure 2-10 Initial Setup: License Installation



Note Enter all licenses except high availability (HA) on the active appliance. Enter only the HA license on the standby appliance. See Licenses in a Redundant Configuration, page 2-44 for more information. See also Licensing: Frequently Asked Questions, page E-1.

a. Locate the Product Authorization Key included with the ICPAM appliance or purchased separately. See Obtaining and Installing Optional Feature Licenses, page 2-44.

b. In a Web browser, open the Identiv Product License Registration Web page.

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

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

d. Transfer the file to the drive of the PC used for the configuration.

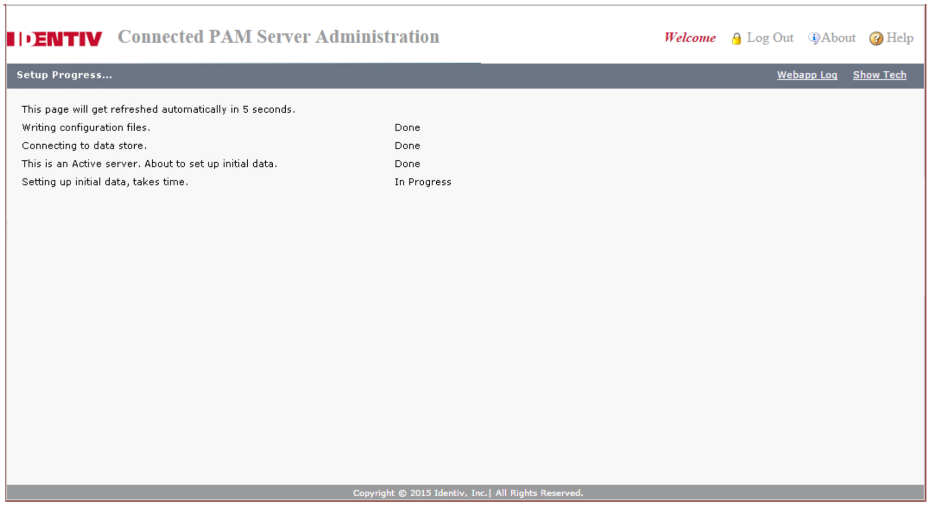
e. In the License screen (Figure 2-10), click Browse to select the license file located on your local drive. when you select the file, the file name appears in the File field.

f. Select **Finish** to install the license file on the ICPAM appliance and activate the features.

Step 10 When you click **Finish**, the initial installation is applied, as shown in Figure 2-11. 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 Identiv support representative for assistance.

Figure 2-11 Initial Setup: Setup Progress


IDENTIV
Connected PAM Server Administration
Welcome
Log Out
About
Help
Setup Progress...
Webapp Log
Show Tech
Copyright © 2015 Identiv, Inc.| All Rights Reserved.

```
This page will get refreshed automatically in 5 seconds.
Writing configuration files.                          Done
Connecting to data store.                             Done
This is an Active server. About to set up initial data.  Done
Setting up initial data, takes time.                  In Progress
```

Step 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 ICPAM on Virtual Machine (VM)

The ICPAM is configured virtually on VMware. The VMware is installed in the UCS server by the UCS admin. Once connected to the VMware the initial setup screens appear automatically when you boot the ICPAM appliance for the first time, (or after a complete system restore). The instructions in this section are for a standalone server, or for the two servers in a redundant (high availability) configuration.

- Before You Begin, page 2-5

Before You Begin

Before you power on the ICPAM 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 ICPAM in VMware.

Note Ensure that the VMware is already created through Vsphere client and the IP address is received.

- IP, subnet, and gateway addresses for the ICPAM 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://<<icpam 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 2-1:

default username: **`cpamadmin`**

default password: **`cpamadmin`**

Step 3 Follow the remaining steps in the setup process, for more information, see Initial Setup Instructions, page 2-7.

Using the Web Admin Menus, Commands and Options

After the initial setup is complete, you can log into the ICPAM 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 ICPAM Server Administration Utility, page 2-18
- Menus and Options in the ICPAM Server Administration Utility, page 2-20
- Archiving Historical Events, page 2-25
- Installing and Revising Language Packs, page 2-30
- Changing or Recovering the Server Password, page 2-40
- Obtaining and Installing Optional Feature Licenses, page 2-44
- Displaying the ICPAM Appliance Serial Number, page 2-46
- Performing a Graceful Failover with Redundant Appliances, page 2-47

Accessing the ICPAM Server Administration Utility

To use the ICPAM Server Administration utility, do the following:

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

- For a direct connection, see Connecting a PC to the Appliance, page 2-5.
- For an Internet connection, open a web browser and enter the IP address used for the ICPAM Server Administration utility. See Logging on to the ICPAM Server Administration Utility, page 2-2, or ask your system administrator for assistance.

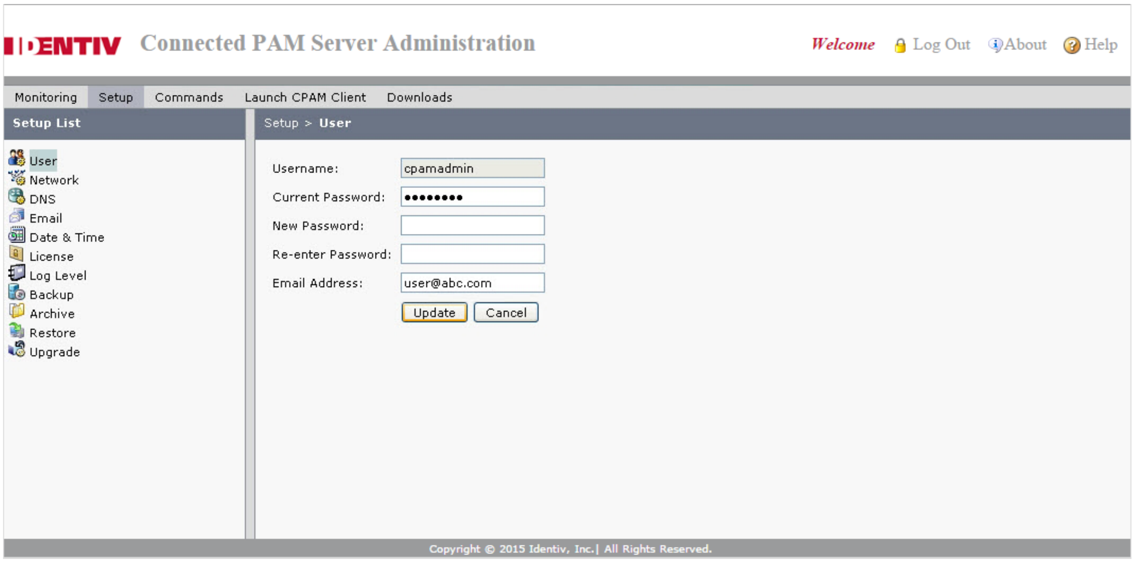
Note The administration screens also appear immediately following the initial setup.

Step 2 Select a menu from the tabs along the top of the window, as shown in Figure 2-12. 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 ICPAM Server Administration Utility" section on page 2-20.

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

Figure 2-12 ICPAM Server Administration Utility: Setup Menus



Username: cpamadmin
Current Password: ••••••••
New Password:
Re-enter Password:
Email Address: user@abc.com

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Menus and Options in the ICPAM Server Administration Utility

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

- Monitoring, page 2-21
- Setup, page 2-22
- Commands, page 2-23
- Launch Client, page 2-24
- Downloads, page 2-24

Monitoring

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

Table 2-1 Monitoring Menu

Menu	Description
Status	Displays real-time information about the current state of the ICPAM 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 2-2. • **Version**: The release number of the current ICPAM appliance server software. • **Serial Number**: the serial number of the ICPAM 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 ICPAM" section on page C-11 and the "Disabling the ICPAM TFTP Server" section on page D-2. • **Web Service API**: Determines if ICPAM web services are available. 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.

Table 2-1 Monitoring Menu (continued)

Menu	Description
High Availability Audit Log	Displays real-time events related to a redundant server configuration.
URL Log	Displays the output (HTTP response) from URL actions.

Setup

This menu option enables you to view and edit the server configuration using the following submenus.

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

Table 2-2 Setup Menu

Menu	Description
User	The username, password and email of the administrator login.
Network	The IP address configuration for the appliance and for the Eth0 and Eth1 network ports. See Entering the Initial Server Configuration, page 2-5 for more information.
DNS	The DNS settings for the appliance, if DNS is used.
Email	The email settings for the appliance, including **SMTP Server Address** and **SMTP Email Address from**. These settings are used to send notifications and other information from the server. • Click **Test** to send a test message and verify the settings. The test message is sent to the administrator email address entered in User settings. • Select **Update** to apply the settings.
Date & Time	The server date and time settings. If a network time protocol server is used, click **NTP enable** and enter the **NTP Server Address** settings. **Note** We strongly recommend using NTP to synchronize the ICPAM appliance and controller clocks to ensure correct event and messaging. See the "Changing the NTP Setting for Multiple Gateways" section on page C-6 for instructions to set NTP on controllers.
License	Displays the Identiv licenses installed on the appliance and allows you to install additional licenses. • **Install**: Install additional Identiv Connected Physical Access Control feature licenses. See Obtaining and Installing Optional Feature Licenses, page 2-44. • **Features**: Displays the licensed modules currently installed in the appliance. • **Files**: Lists the license files installed on the appliance.
Log Level	Defines the log level for capturing log messages. Select a level for each log subject (such as Security). The log levels are Debug, Info, Warn, Error, and Fatal.
Backup	Creates a compressed backup file of all system and configuration data that can be used to restore a server. See Backing up the ICPAM Database, page A-1.
Event	Prunes and archives historical events from the ICPAM 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 2-25 for more information.

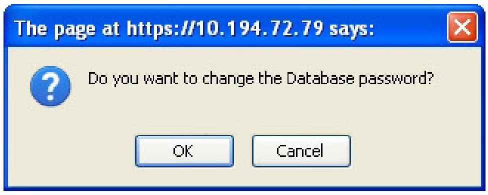
Table 2-2 Setup Menu (continued)

Menu	Description
Restore	Restores data from a backup or archive file. The server must be stopped using **Stop Server** in the Commands menu. See the “Restoring a Server Backup File” section on page A-8.
Upgrade	Upgrades the server software. To upgrade the server, select **Stop Server** from the Commands menu, click **Browse** to select an upgrade file, and then click **Upgrade**. Select **Start Server** from the Commands menu when the upgrade is complete. See the “Upgrading the ICPAM Server Software” section on page B-10.
Localization	Allows you to create and add language packs that display ICPAM 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 2-47. **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 2-3 Commands Menu

Command	Description
Start Server	Enables the ICPAM access control server functions and user logins.
Stop Server	Disables the ICPAM access control server functions. All user logins are denied. The appliance remains in operation and you can still log in to the ICPAM Server Administration utility using a direct connection. To restart the access control server, select **Start Server**. **Note** When the server restarts, a message appears asking if you want to change the database password. Click **Cancel** or **OK**. This password is a security measure used for troubleshooting and technical support. It does not impact user operation,  The page at https://10.194.72.79 says: Do you want to change the Database password? **Note** All EDI projects run when the ICPAM 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 ICPAM, page 14-37.
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 Identiv technical support.This command is processor intensive and can result in decreased system performance. Use the command only under the supervision of a Identiv support representative.
Processes	Displays the processes running on the system for use in troubleshooting.

Launch Client

Launches the ICPAM 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 2-2) and in the Downloads menu.

Downloads

Provides links to download additional software, including the following:

Table 2-4 Downloads Menu

Download	Description
JRE 1.7 (Windows)	Installs only the required version of the JRE (Java Runtime Environment) on a Windows PC. JRE 1.7 is now supported for the client.
ICPAM Client (JRE required)	Installs Java, and then installs the ICPAM desktop client. This link is the same as the client installation link on the log in page (Figure 2-2).
Cisco EDI Studio (JRE required)	Installs the EDI studio required to configure data integration. See Chapter 14, "System Integration" for more information. This link is the same as the client installation link on the log in page (Figure 2-2).
SnapShell Driver **Snap Shell SDK**	Installs the drivers and other software required by the SnapShell scanner. See the Using a SnapShell License Scanner to Create Personnel Records, page 9-16.

Archiving Historical Events

If access control events are allowed to accumulate in the ICPAM 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 ICPAM 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 2-5. Use the instructions in this section to can change the pruning and archiving settings.

This section includes the following topics:

- Understanding Live, Pruned and Archived Events, page 2-25
- Pruning and Archiving Historical Events, page 2-26

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 ICPAM 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 ICPAM 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 12-58

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 ICPAM 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 ICPAM version number, and other information. For example, cpam-2.1_0.3.10.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 ICPAM, 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 12-58 for more information. Archived event files can also be used by other applications to view old events or run reports.

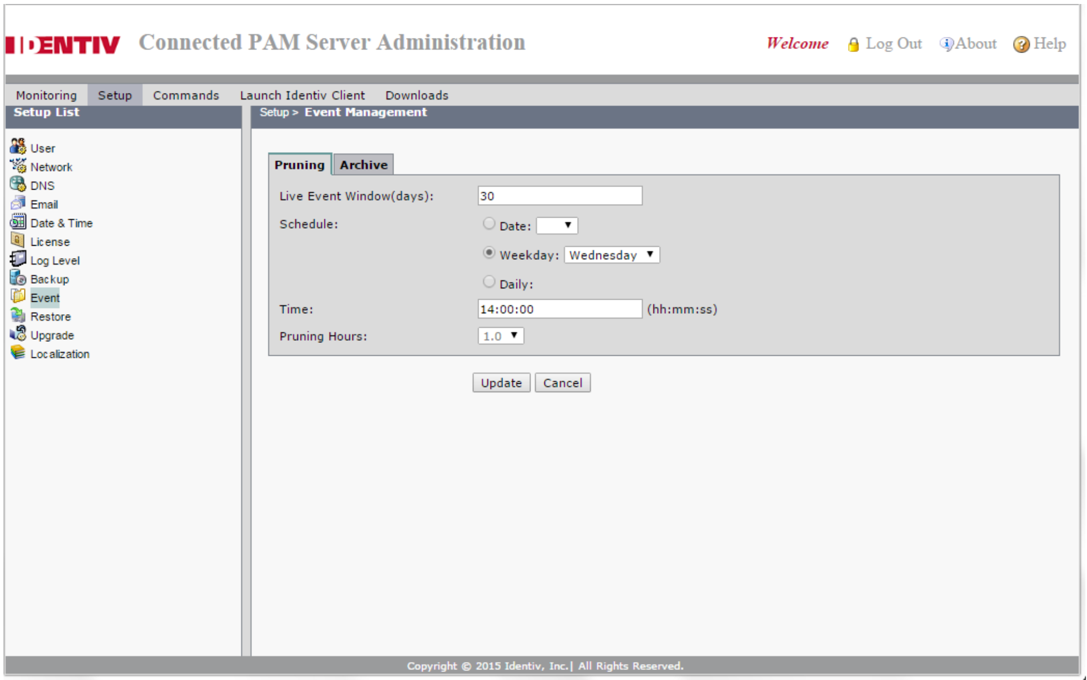
Pruning and Archiving Historical Events

Event management settings are entered during the initial server setup, as described in the "Entering the Initial Server Configuration" section on page 2-5. Use the following procedure to revise the pruning and archiving settings.

Step 1 Log on the ICPAM Server Administration utility, as described in the "Logging on to the ICPAM Server Administration Utility" section on page 2-2.

Step 2 Choose **Setup** and then **Event** (Figure 2-13).

Figure 2-13 Pruning Events



Live Event Window(days): 30

Schedule:
○ Date:
● Weekday: Wednesday
○ Daily:

Time: 14:00:00 (hh:mm:ss)

Pruning Hours: 1.0

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`.

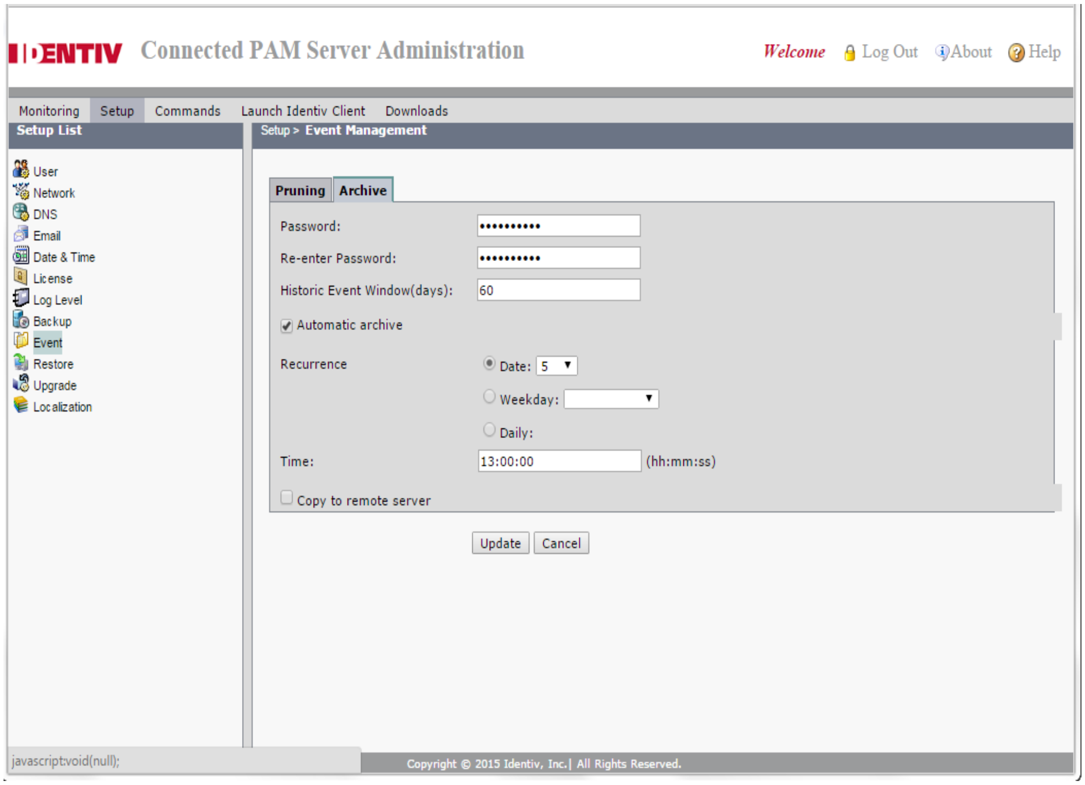
c. **Pruning Hours**— This field is enabled only when Daily is selected in Schedule.The default value is one.

Note The Pruning Hours field is available from ICPAM 1.5.1 release onward.

d. Select **Update** to save the changes.

Step 4 Select the **Archive** tab (Figure 2-14) and enter the following archive settings:

Figure 2-14 Archiving Events



Password: ••••••••••

Re-enter Password: ••••••••••

Historic Event Window(days): 60

☑ Automatic archive

Recurrence ● Date: 5 ○ Weekday: ○ Daily:

Time: 13:00:00 (hh:mm:ss)

□ Copy to remote server

Note

- 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 ICPAM version number, and other information. For example: cpam-2.1_0.3.10.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 2-25.

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.

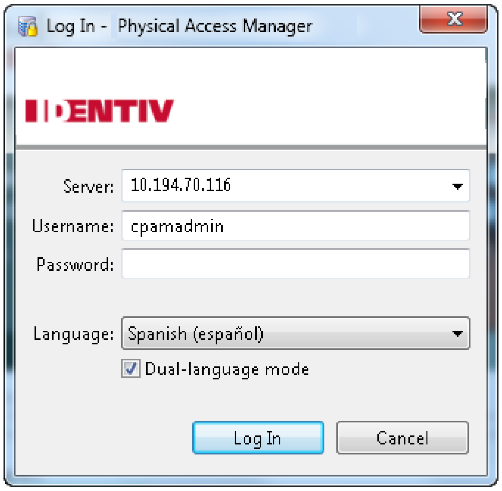
Note If the IP address, username, password, or path is incorrect, or if the server is not available, then the backup is not copied to the remote server. The backup is still created on the ICPAM server.

f. Click **Update** to save the changes.

Installing and Revising Language Packs

Optional language packs are installed on the ICPAM appliance to display ICPAM 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 ICPAM application (Figure 2-15). Users can also select *Dual-language mode* to display text and menus in both English and the selected language.

Figure 2-15 Login Screen



Server: 10.194.70.116
Username: cpamadmin
Password:
Language: Spanish (español)
☑ Dual-language mode

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 ICPAM 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, page 2-31.
- Log files and the ICPAM 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 ICPAM 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 ICPAM appliance using the ICPAM Server Administration utility. Finally, reinstall the ICPAM 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 2-5.
- For an Internet connection, open a web browser and enter the IP address used for the ICPAM Server Administration utility. See Accessing the ICPAM Server Administration Utility, page 2-18, or ask your system administrator for assistance.

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

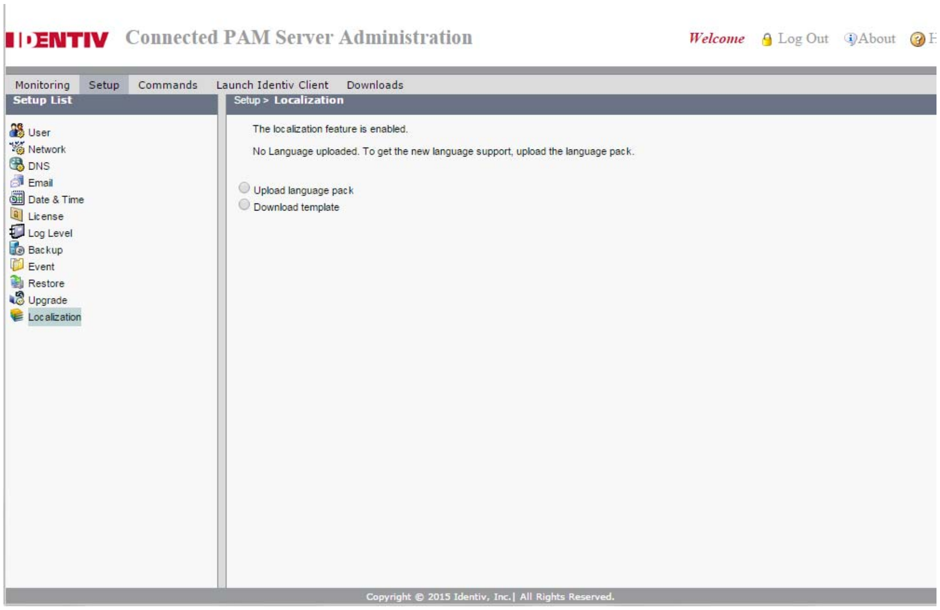
Tip Back up system data before performing any major operation to ensure the integrity of your existing data.

Step 3 Select **Setup**, and then select **Localization** (Figure 2-16).

Step 4 Enable localization, if necessary (Figure 2-16):

- 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.

Figure 2-16 Enable Localization



The localization feature is enabled.

No Language uploaded. To get the new language support, upload the language pack.

○ Upload language pack
○ Download template

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 2-16).

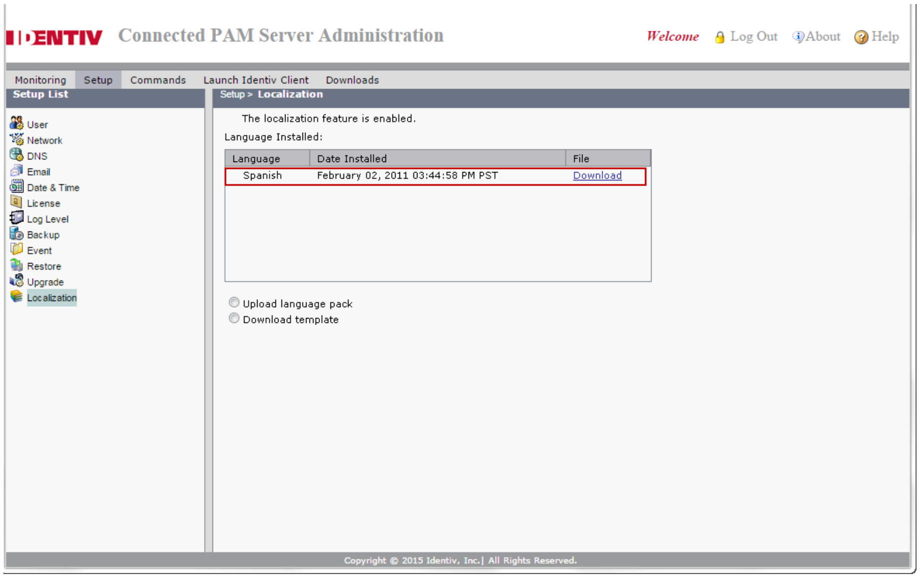
c. Click **OK** when the confirmation message appears.

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 2-17), and skip to Step 7.

Figure 2-17 Localization Menu in the ICPAM Server Administration Utility



The localization feature is enabled.

Language Installed:

Language	Date Installed	File
Spanish	February 02, 2011 03:44:58 PM PST	Download

Step 6 To create a new language pack, download a language template:

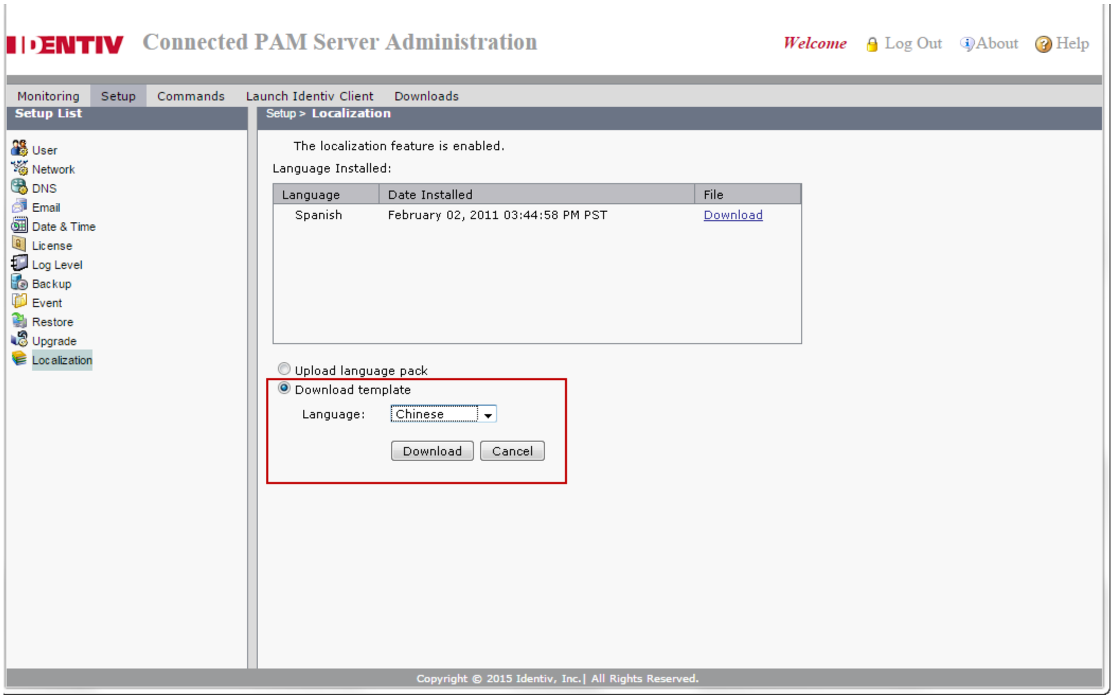
a. Select the **Download templates** radio button (Figure 2-18).

b. Choose a language from the Language menu.

c. Select **Download**.

d. Continue to Step 7.

Figure 2-18 Download Language Templates



The localization feature is enabled.

Language Installed:

Language	Date Installed	File
Spanish	February 02, 2011 03:44:58 PM PST	Download

Language: Chinese

Step 7 Select a location on your hard drive to save the compressed `.zip` file.

The filename includes the release number, and language code. For example: `languagepack_zh_2.1_0.3.10`

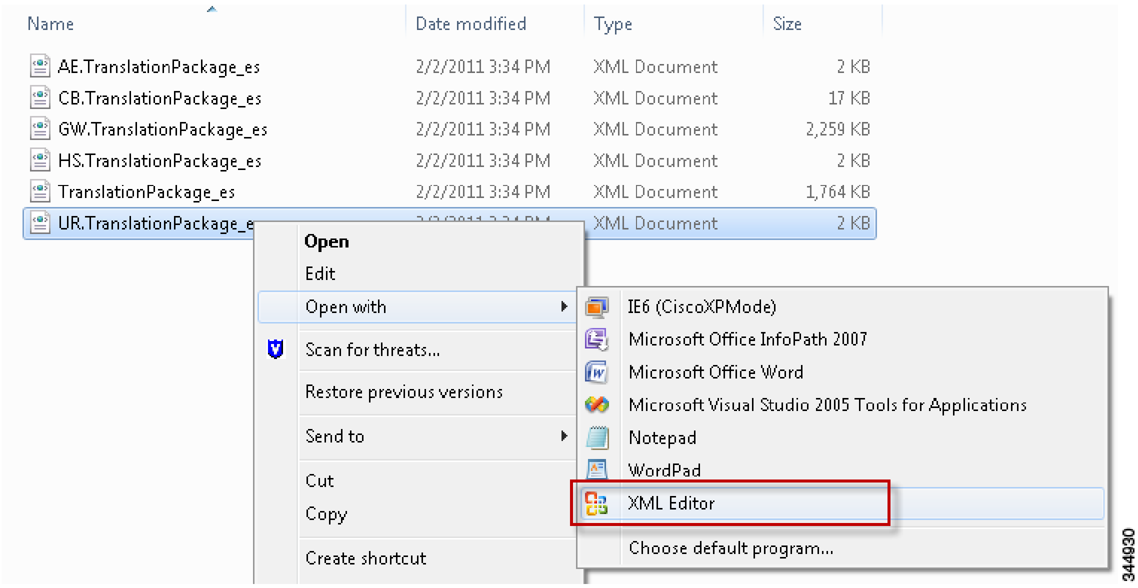
Step 8 Edit the XML files to include the translated text:

a. Unzip the compressed language pack directory.

b. Open each file in a Unicode-supported.

For example: in Windows, right-click the file name and select **Open with** and then **XML** (Figure 2-19).

Figure 2-19 Download Language Templates

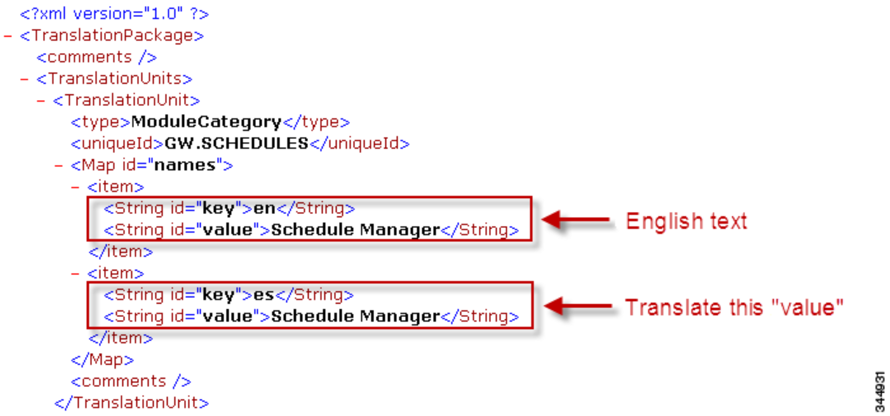


Name	Date modified	Type	Size
AE.TranslationPackage_es	2/2/2011 3:34 PM	XML Document	2 KB
CB.TranslationPackage_es	2/2/2011 3:34 PM	XML Document	17 KB
GW.TranslationPackage_es	2/2/2011 3:34 PM	XML Document	2,259 KB
HS.TranslationPackage_es	2/2/2011 3:34 PM	XML Document	2 KB
TranslationPackage_es	2/2/2011 3:34 PM	XML Document	1,764 KB
UR.TranslationPackage_e		XML Document	2 KB

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 2-20).

Figure 2-20 XML Language File



```
  <?xml version="1.0" ?>
- <TranslationPackage>
    <comments />
  - <TranslationUnits>
    - <TranslationUnit>
        <type>ModuleCategory</type>
        <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>
        <comments />
      </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 ICPAM 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 ICPAM 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 ICPAM 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.

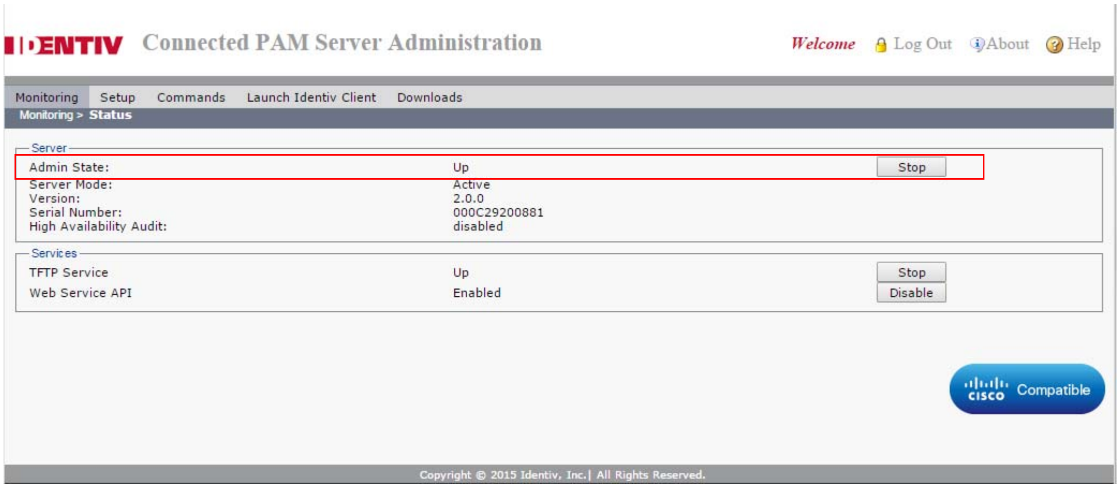
Caution Placing the server in Admin State *Down* stops all ICPAM services. If a redundant Standby server is configured, you must also place the Standby server in the Admin State *Down* state.

a. Log on to the *standby* ICPAM appliance (if configured).

b. Select **Monitoring** and then **Status** (Figure 2-21).

c. Select **Stop** (next to Admin State).

Figure 2-21 Stop the ICPAM Server



Server

Admin State: Up

Server Mode: Active

Version: 2.0.0

Serial Number: 000C29200881

High Availability Audit: disabled

Services

TFTP Service Up

Web Service API Enabled

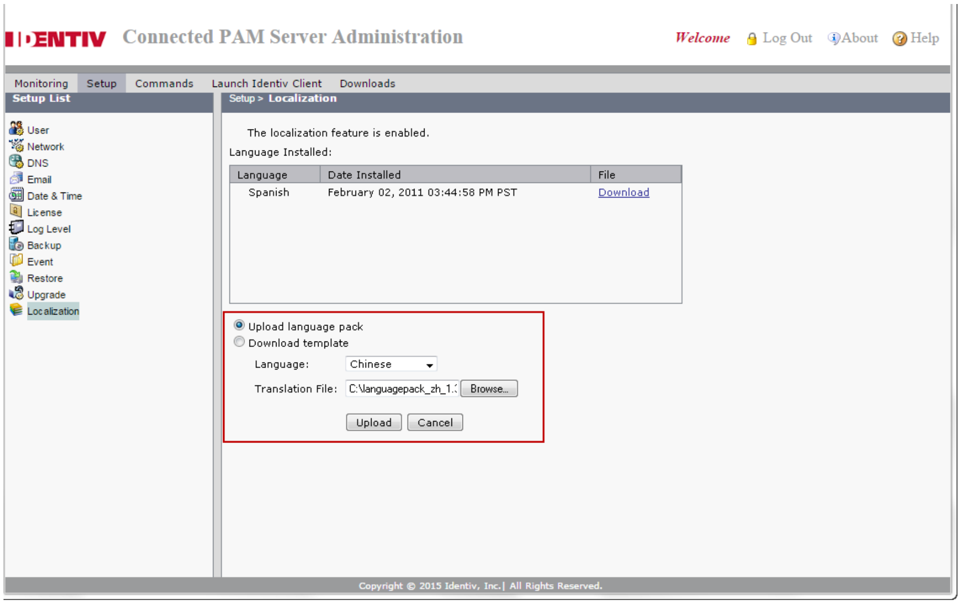
- **a.** Log on to the *active* ICPAM appliance.
- **b.** Select **Monitoring** and then **Status** (Figure 2-21).
- **c.** Select **Stop** (next to Admin State).

Step 11 Upload the revised language pack.

- **a.** Select **Setup** and then select **Localization**.
- **b.** Select the **Upload language pack** radio button (Figure 2-22).
- **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_2.1_0.3.10`
- **e.** Click **Upload**.

Figure 2-22 Apply the Language Pack



The localization feature is enabled.

Language Installed:

Language	Date Installed	File
Spanish	February 02, 2011 03:44:58 PM PST	Download

● Upload language pack
○ Download template

Language: Chinese

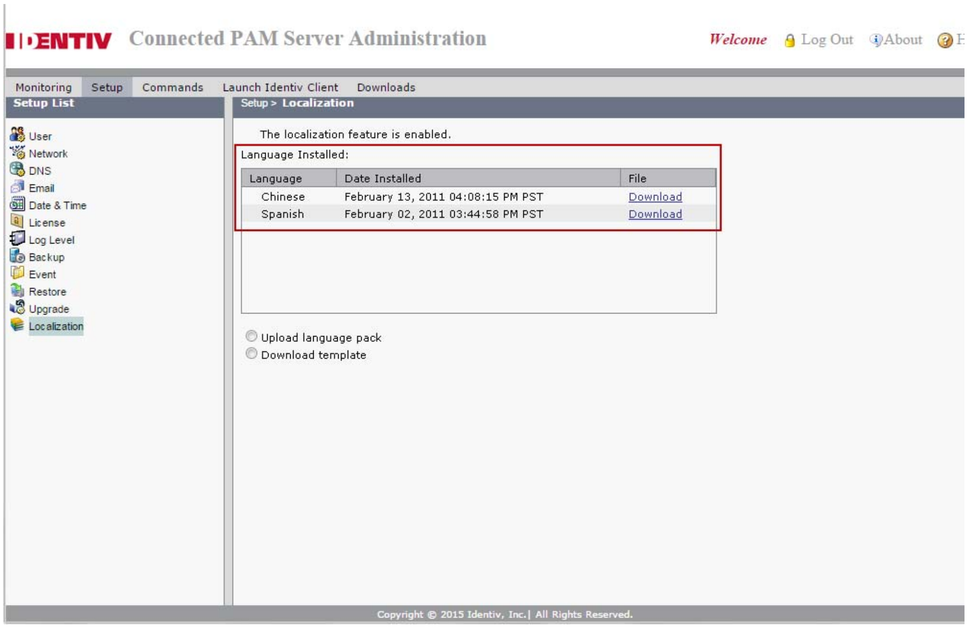
Translation File: C:\languagepack_zh_1.: Browse...

Upload Cancel

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 2-23).

Figure 2-23 Languages Installed on the ICPAM Server



The localization feature is enabled.

Language Installed:

Language	Date Installed	File
Chinese	February 13, 2011 04:08:15 PM PST	Download
Spanish	February 02, 2011 03:44:58 PM PST	Download

○ Upload language pack
○ Download template

Step 14 Restart the ICPAM server.

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 ICPAM client application.

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

a. If the ICPAM client is already installed on your Windows PC, uninstall it.

- Go to **Start** > **Programs** > **Identiv Connected Physical Access Manager** > **Uninstaller** and follow the onscreen instructions.
- Or go to **Start** > **Control Panel** > **Uninstall a Program** > **Identiv Connected Physical Access Manager** and choose **Uninstall**.

b. Use one of the following methods to reinstall the desktop client:

- In the ICPAM Server Administration utility, click **Launch ICPAM Client**.
- Select **Downloads** and then **ICPAM Client (JRE required)**.
- Click **Launch ICPAM Client** on the web utility login page.

Tip See the "Installing or Updating the ICPAM Desktop Software" section on page 3-2 for more information.

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

Step 16 Select the new language when logging in to the ICPAM desktop client (Figure 2-24).

a. Launch the ICPAM application.

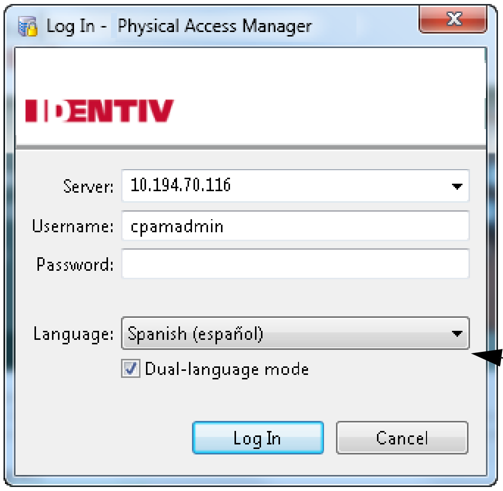
b. In the Log In window, choose the language you want to use (Figure 2-24).

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**.

Figure 2-24 Selecting a Language at the ICPAM Login



Server: 10.194.70.116

Username: cpamadmin

Password:

Language: Spanish (español)

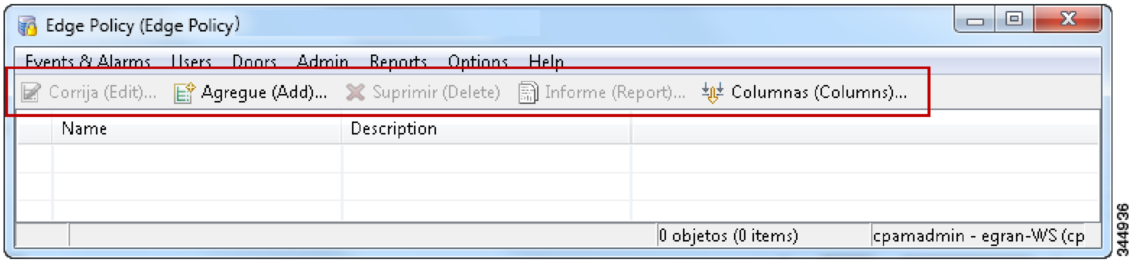
☑ Dual-language mode

Language option field

Step 17 Verify that the translated text appears correctly in the ICPAM application (Figure 2-25).

If you chose *Dual-language mode*, english appears after the translated text (in parentheses).

Figure 2-25 Translated Menus in ICPAM


Edge Policy (Edge Policy)
Events & Alarms Users Doors Admin Reports Options Help
Corrija (Edit)... Agregue (Add)... Suprimir (Delete) Informe (Report)... Columnas (Columns)...
Name
Description
0 objetos (0 items)
cpamadmin - egran-WS (cp
344936

Tip The Login screen (Figure 2-24) also displays the selected language the next time you log in.

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 ICPAM client application each time you upload a language pack for the changes to appear.

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 ICPAM 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 ICPAM 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 4, "Configuring User Access for the ICPAM Desktop Client" for more information.

This section includes the following information:

- Changing the ICPAM Server Administration Utility Password, page 2-40
- Resetting a Forgotten Password, page 2-41
- Recovering a Lost Server Password, page 2-43

Changing the ICPAM Server Administration Utility Password

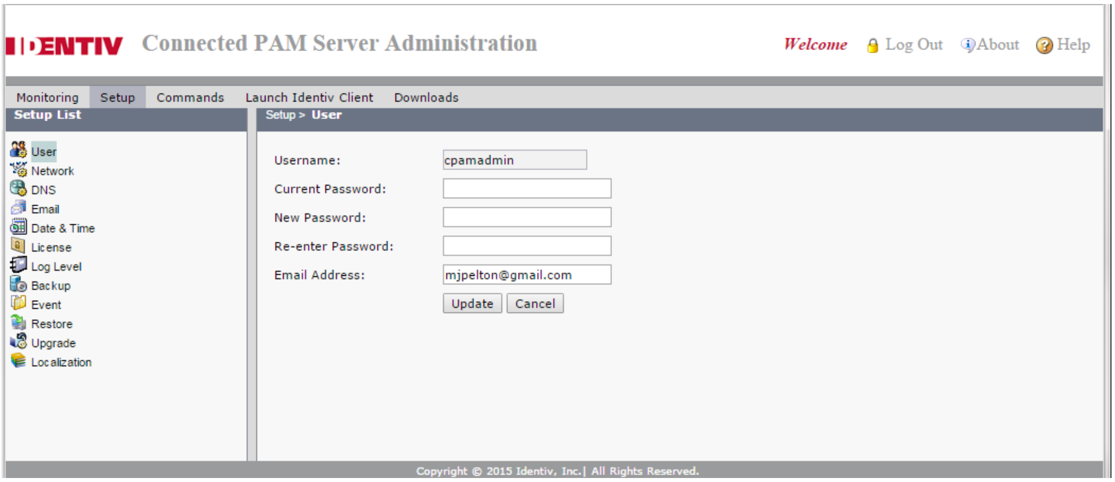
To change the password for the `cpamadmin` username on the ICPAM Server Administration utility, do the following:

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

- For a direct connection, see Connecting a PC to the Appliance, page 2-5.
- For an Internet connection, open a web browser and enter the IP address used for the ICPAM Server Administration utility. See Logging on to the ICPAM Server Administration Utility, page 2-2, or ask your system administrator for assistance.

Step 2 Select the Setup tab and then select the User menu, as shown in Figure 2-26.

Figure 2-26 ICPAM Server Administration Utility: Setup Menus



Username: cpamadmin
Current Password:
New Password:
Re-enter Password:
Email Address: mjpelton@gmail.com

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 ICPAM desktop client. See Chapter 4, "Configuring User Access for the ICPAM Desktop Client" for information on managing desktop client usernames and passwords.

Resetting a Forgotten Password

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

Note

- The **Forgot Password?** link appears only if the feature is enabled (as described in Enabling the Forgot Password Feature, page 2-42). 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 2-43.
- The server password is different from the ICPAM desktop client password. See Chapter 4, "Configuring User Access for the ICPAM 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 ICPAM Server Administration utility login page.

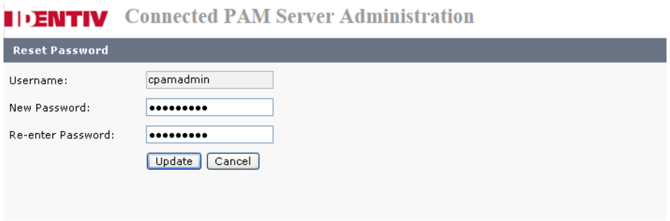
Step 2 Click the **Forgot Password?** link that appears below the Password field.

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

Step 3 Access the email in your email application, and click the included URL to open an online reset password form, as shown in Figure 2-27.

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

Figure 2-27 Reset Password Page



Username: cpamadmin
New Password: •••••••••
Re-enter Password: •••••••••

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

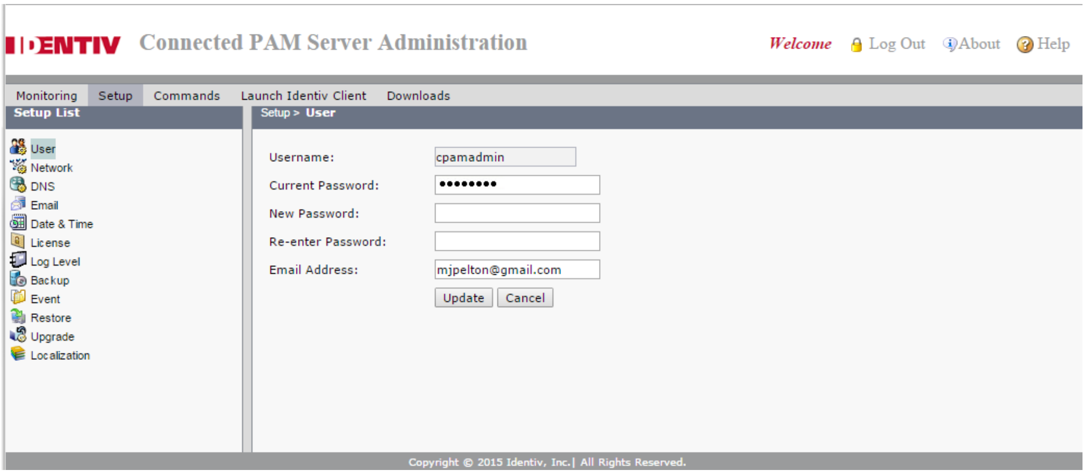
The **Forgot Password?** link appears on the login page only if the server email settings are configured, as described in the following steps:

Step 1 Log in to the ICPAM Server Administration utility.

Step 2 Enter the email address that will receive **Forgot Password?** emails.

a. Select the Setup tab and then select the User menu, as shown in Figure 2-28.

Figure 2-28 Email Recipient for Forgotten Password



Username: cpamadmin
Current Password: ••••••••
New Password:
Re-enter Password:
Email Address: mjpelton@gmail.com

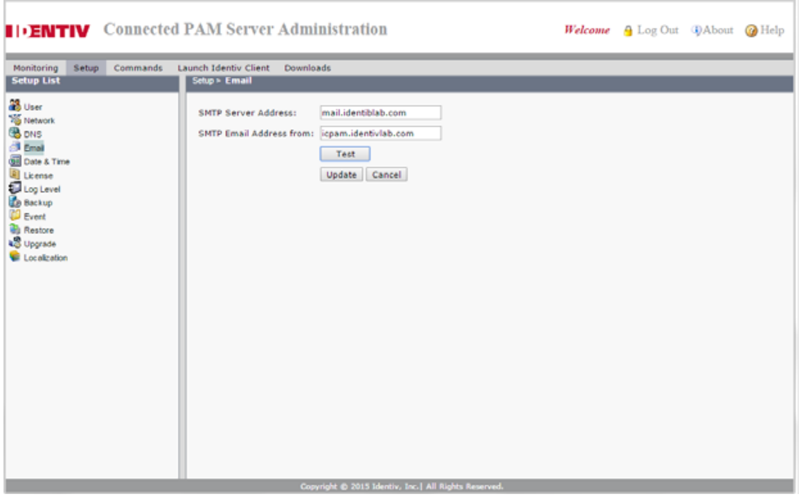
b. Enter an Email Address that will receive Forgot Password emails.

c. Click **Update**.

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

a. In the Setup tab, click the **Email** menu, as shown in Figure 2-29.

Figure 2-29 Send Email Settings for Forgot Password



SMTP Server Address: mail.identiblab.com

SMTP Email Address from: icpam.identivlab.com

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 ICPAM appliance. This email address is also the `Reply To` address.

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

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

Recovering a Lost Server Password

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

Step 1 Reinstall the server software and enter a new `cpamadmin` password, as described in Reinstalling the ICPAM Server Software from a Recovery CD, page B-21. Reinstalling the ICPAM server software deletes all server information and settings.

Step 2 Restore the ICPAM 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

ICPAM client and server software, the badge designer, and the web services API are all included as part of the ICPAM hardware purchase; there is no need to purchase these as separate feature licenses.

The HA and EDI licenses are the only optional feature licenses.

Customers who purchase the HA or EDI licenses will electronically receive information on how to obtain the license files. Refer to Table 2-5 on page 2-45 for optional feature licenses and part numbers available for purchase.

To enable the HA- or EDI-licensed features:

Step 1 Start the ICPAM application.

Step 2 On the License screen, click **Browse**.

Step 3 Find and select the license file located on your local drive.

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

Step 5 Select the **Features** tab to verify that the new license has been added.

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

Note

- The menus for licensed software features do not appear unless the license is installed on the ICPAM appliance.
- If you are installing a new server, or reconfiguring a server after a system restore from a CD/DVD, see Entering the Initial Server Configuration, page 2-5 to install licenses during the initial setup.
- Licenses installed on a ICPAM appliance cannot be transferred to another appliance.
- Licenses installed in an HA configuration are automatically transferred from the active appliance to the standby server during a failover.

This section includes the following topics:

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 2-5.

Table 2-5 on page 2-45 lists the part numbers for the optional feature licenses.

Part Numbers for the Optional Feature Licenses

Table 2-5 lists the part numbers for the optional feature licenses.

Table 2-5 Optional Feature Licenses and Part Numbers

Part	Optional Feature Licence
CIAC-PAME-HA=	ICPAM HA License
CIAC-PAME-EAI=	ICPAM EDI License

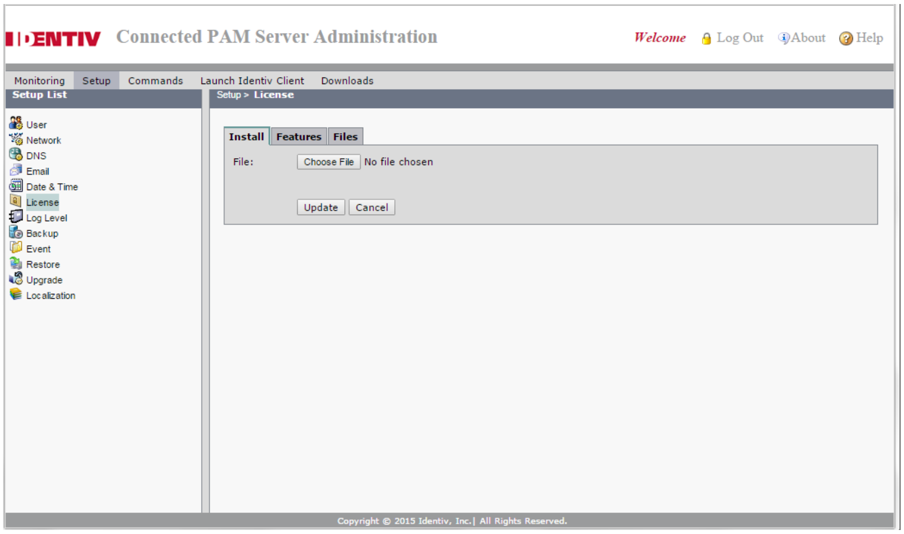
For information on how to purchase these optional licenses, contact sales@identiv.com.

To contact ICPAM support for technical support information, go to the following link and submit your request via web or contact us: http://www.identiv.com/support-icpam.

Installing Additional Licenses

This section contains instructions on how to download and install additional license files after the ICPAM appliance is set up. If you are installing a new appliance, see Entering the Initial Server Configuration, page 2-5.

Figure 2-30 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 Identiv Product License Registration Web page:

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

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

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

Step 5 In the License screen (Figure 2-30), 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 ICPAM appliance and activate the features.

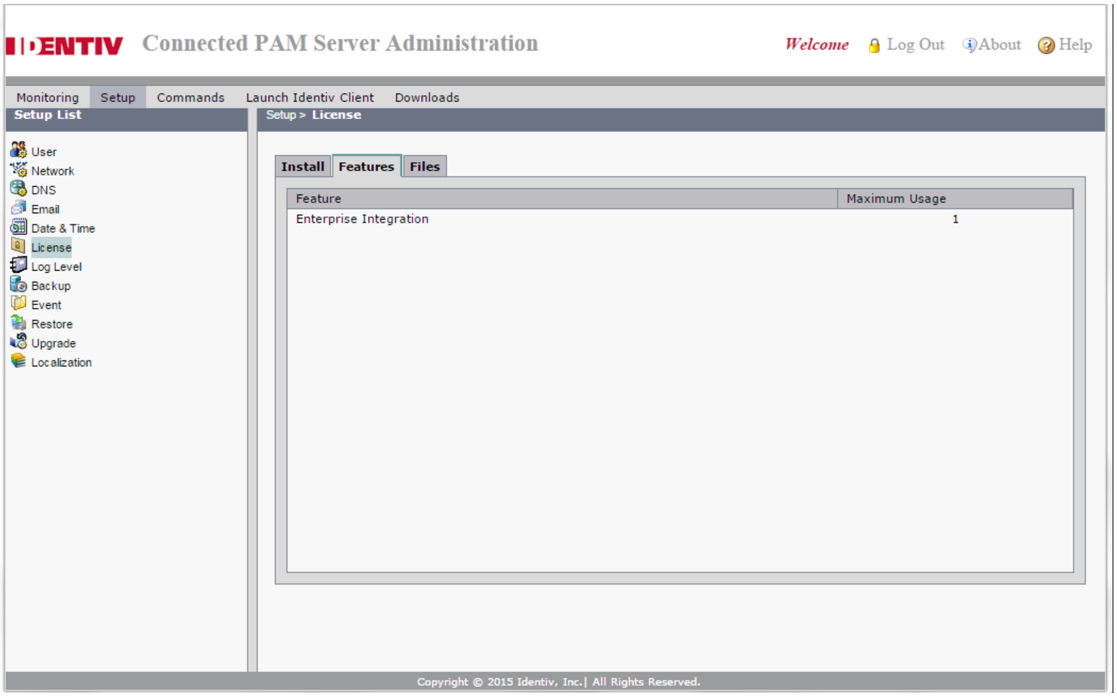
Step 7 Select the **Features** tab to verify that the new license was added. See Displaying a Summary of Installed Licenses, page 2-46 for more information.

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

Displaying a Summary of Installed Licenses

From the ICPAM Server Administration utility, select the Features tab in the Setup menu to view a list of installed feature licenses, as shown in Figure 2-31.

Figure 2-31 License Features List



Feature	Maximum Usage
Enterprise Integration	1

Displaying the ICPAM Appliance Serial Number

To view the appliance serial number, do the following:

Step 1 Log on to the ICPAM Server Administration utility:

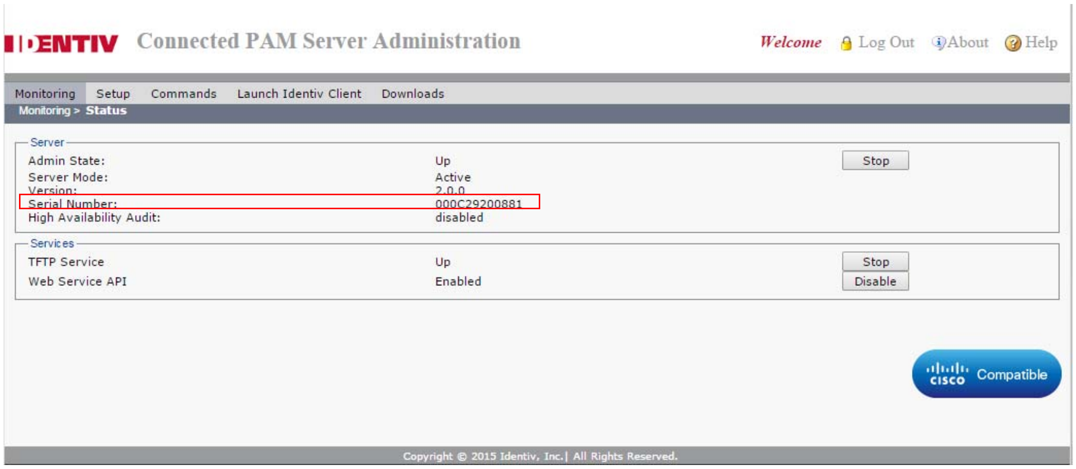
- For a direct connection, see Connecting a PC to the Appliance, page 2-5.
- For an Internet connection, open a web browser and enter the IP address used for the ICPAM Server Administration utility. See Logging on to the ICPAM Server Administration Utility, page 2-2, or ask your system administrator for assistance.

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

Step 2 Select the Monitoring tab, and then select Status, as shown in Figure 2-32.

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

Figure 2-32 ICPAM Appliance Serial Number



Server

Admin State: Up
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

Services

TFTP Service Up
Web Service API Enabled

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

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 ICPAM 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 2-18 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. Identiv recommends performing a manual failover only when system usage is low.

Troubleshooting and Monitoring

See Using the Web Admin Menus, Commands and Options, page 2-18 for information on the monitoring and troubleshooting features available in the ICPAM Server Administration utility. Most of the functions are used to gather information for Identiv technical support. For more information, contact your Identiv 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 Identiv 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 ICPAM appliance is ready to configure the access control features of your system, including doors, users, badges, and other features. See Chapter 3, "Getting Started With the ICPAM Desktop Software" for instructions to log in and get started. For information on installing and configuring the access gateway and other physical modules, see the *Cisco Physical Access Gateway User Guide*.

CHAPTER 3

Getting Started With the ICPAM Desktop Software

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

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

Contents

Before You Begin

Before you can use the ICPAM desktop software to configure the Identiv Connected Physical Access Manager, do the following:

- Verify that your computer is connected to the Internet, including access to the ICPAM appliance through the IP network.
- Verify that your PC meets the following requirements:
  - Windows XP or Vista, and Internet Explorer 6.0 or higher, or Windows 7 (32-bit or 64-bit) and Internet Explorer 8.0 (32-bit only). To install and use ICPAM client on 64-bit windows, a 32-bit JRE needs to be installed.
  - Java Runtime Environment (JRE) 1.7 32-bit. To download Java, go to http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html
  - 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 logging.
- Obtain your username and password from your system administrator.

Installing or Updating the ICPAM Desktop Software

To install the desktop software, you must connect to the ICPAM Server Administration utility.

Always upgrade the ICPAM desktop client when the server software is upgraded. If the versions are not the same, an error occurs when launching the desktop client.

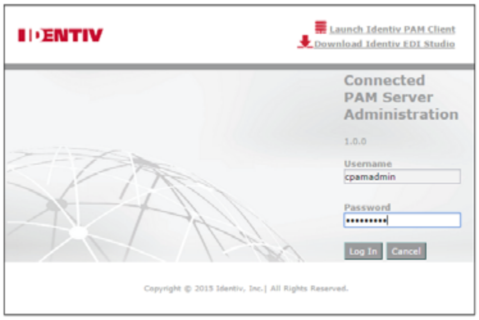
Step 1 Log on to the ICPAM Server Administration utility:

- To use a direct connection, see Connecting a PC to the Appliance, page 2-5.
- To use an Internet connection, open a web browser and enter the IP address used for the ICPAM Server Administration utility. See Understanding IP Addresses on the ICPAM Server, page 2-3, or ask your system administrator for assistance.

Step 2 Select **Launch ICPAM Client** from the Login window, as shown in Figure 3-1 on page 3-3.

- If the correct version of the ICPAM 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 ICPAM client launches using Java Web Start.

Figure 3-1 ICPAM Server Administration Utility: Login



Connected
PAM Server
Administration

1.0.0

Username: cpamadmin

Password: •••••••••

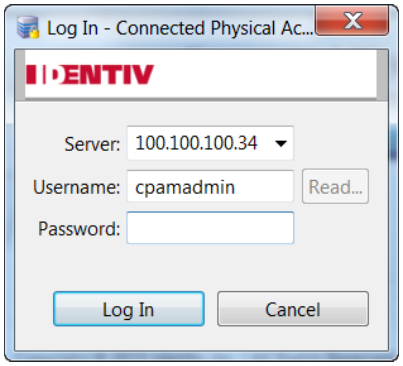
Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Tip For additional methods to install or upgrade the ICPAM desktop software using the ICPAM Server Administration utility, See Using the Web Admin Menus, Commands and Options, page 2-18.

Logging into ICPAM Client

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

Figure 3-2 Login Screen



Server: 100.100.100.34

Username: cpamadmin

Password:

Step 1 Enter the server IP address of the ICPAM 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**.

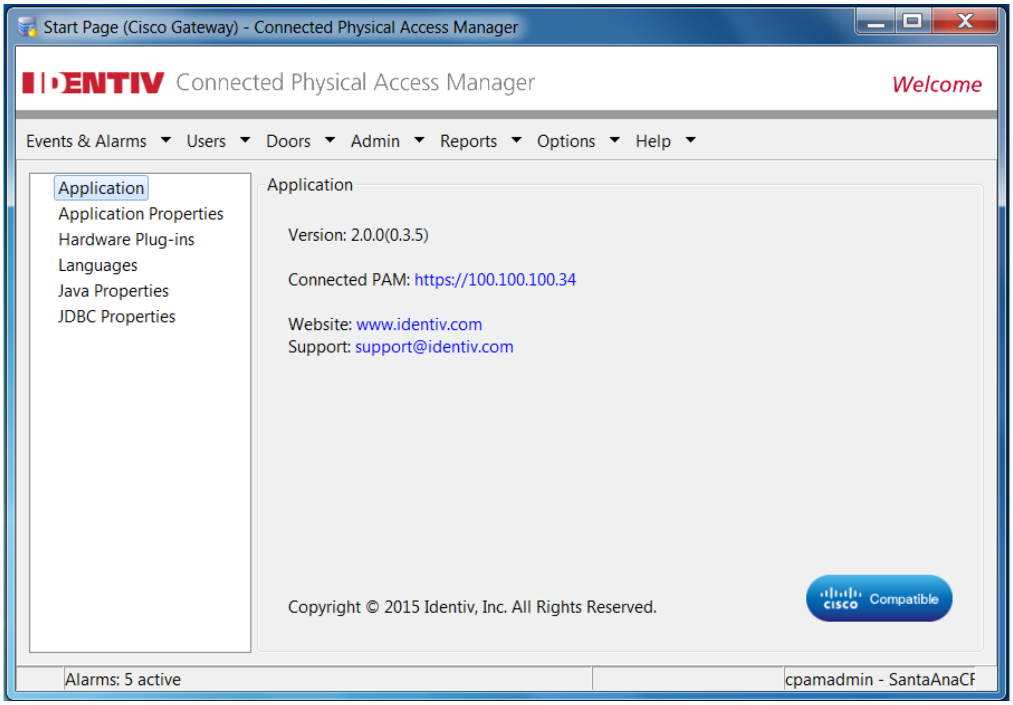
If the username and password are valid, ICPAM displays the **Start Page**, or the modules that were open during the operator's previous session.

Tip To change your password, log on to the ICPAM 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 ICPAM desktop client for the first time, as shown in Figure 3-3. The main menus provide access to ICPAM features, and are also displayed in the main window for each feature.

Figure 3-3 ICPAM Start Page



Application

Version: 2.0.0(0.3.5)

Connected PAM: https://100.100.100.34

Website: www.identiv.com
Support: support@identiv.com

Copyright © 2015 Identiv, Inc. All Rights Reserved.

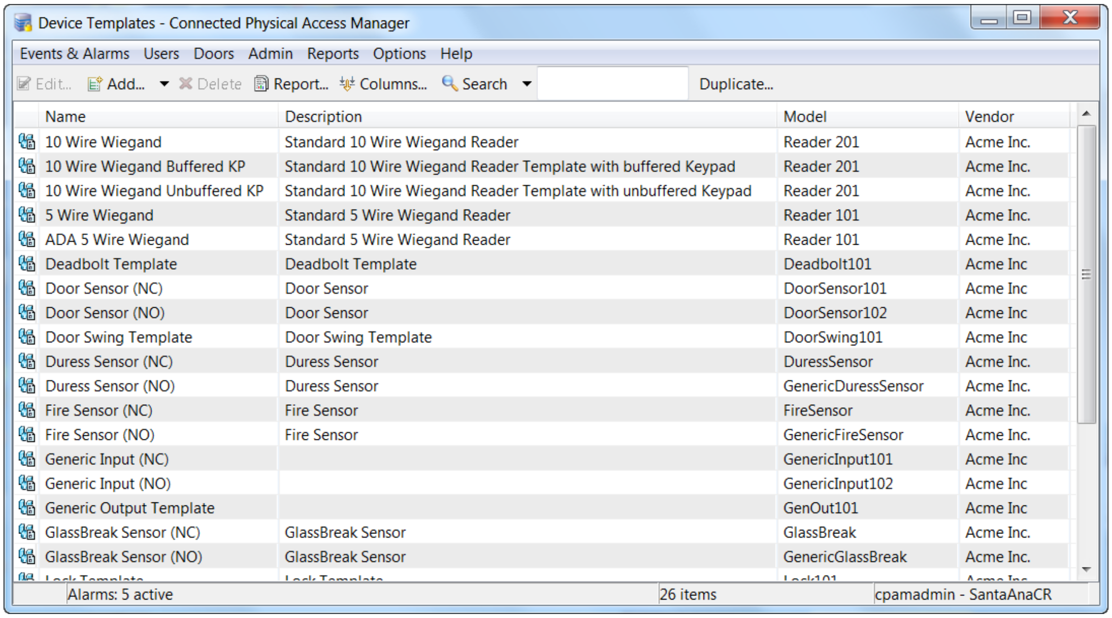
Alarms: 5 active

cpamadmin - SantaAnaCF

Note The available modules vary depending on the software license purchased and the operator's access privileges. Some menus are activated only after the feature license is installed. See Obtaining and Installing Optional Feature Licenses, page 2-44 and Chapter 4, “Configuring User Access for the ICPAM Desktop Client”.

Select a menu item to open the main window for that feature in a new window, as shown in Figure 3-4. You can open multiple module windows simultaneously and drag the windows across multiple monitors. The size and position of the open windows is restored when you log out and log back in.

Figure 3-4 Device Templates Main Window



Name	Description	Model	Vendor
10 Wire Wiegand	Standard 10 Wire Wiegand Reader	Reader 201	Acme Inc.
10 Wire Wiegand Buffered KP	Standard 10 Wire Wiegand Reader Template with buffered Keypad	Reader 201	Acme Inc.
10 Wire Wiegand Unbuffered KP	Standard 10 Wire Wiegand Reader Template with unbuffered Keypad	Reader 201	Acme Inc.
5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
ADA 5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
Deadbolt Template	Deadbolt Template	Deadbolt101	Acme Inc
Door Sensor (NC)	Door Sensor	DoorSensor101	Acme Inc
Door Sensor (NO)	Door Sensor	DoorSensor102	Acme Inc
Door Swing Template	Door Swing Template	DoorSwing101	Acme Inc
Duress Sensor (NC)	Duress Sensor	DuressSensor	Acme Inc.
Duress Sensor (NO)	Duress Sensor	GenericDuressSensor	Acme Inc.
Fire Sensor (NC)	Fire Sensor	FireSensor	Acme Inc.
Fire Sensor (NO)	Fire Sensor	GenericFireSensor	Acme Inc.
Generic Input (NC)		GenericInput101	Acme Inc
Generic Input (NO)		GenericInput102	Acme Inc
Generic Output Template		GenOut101	Acme Inc
GlassBreak Sensor (NC)	GlassBreak Sensor	GlassBreak	Acme Inc.
GlassBreak Sensor (NO)	GlassBreak Sensor	GenericGlassBreak	Acme Inc.
Lock Template	Lock Template	Lock101	Acme Inc

Keeping a Module On Top

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

To configure a window to always be on top:

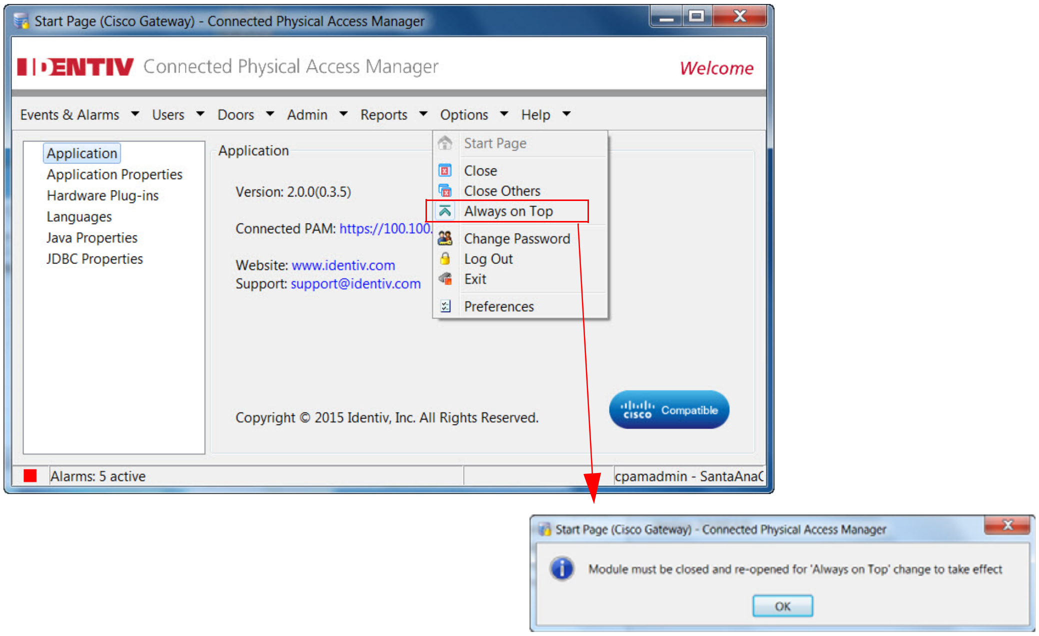
Step 1 Select **Always on Top** from the Options menu, as shown in Figure 3-5.

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

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

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

Figure 3-5 Always on Top



Version: 2.0.0(0.3.5)

Connected PAM: https://100.100

Website: www.identiv.com
Support: support@identiv.com

Copyright © 2015 Identiv, Inc. All Rights Reserved.

Module must be closed and re-opened for 'Always on Top' change to take effect

Note When selected, **Always on Top** is displayed with a check. The setting remains in effect even if you close and then reopen the window.

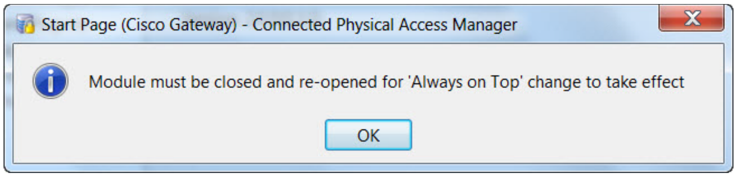
Choosing Multiple *Always on Top* Windows

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

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

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

Figure 3-6 Always on Top Confirmation Message



Start Page (Cisco Gateway) - Connected Physical Access Manager

Module must be closed and re-opened for 'Always on Top' change to take effect

Deselecting *Always on Top*

To deselect Always on Top, do the following:

Step 1 Deselect **Always on Top** to remove the check.

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

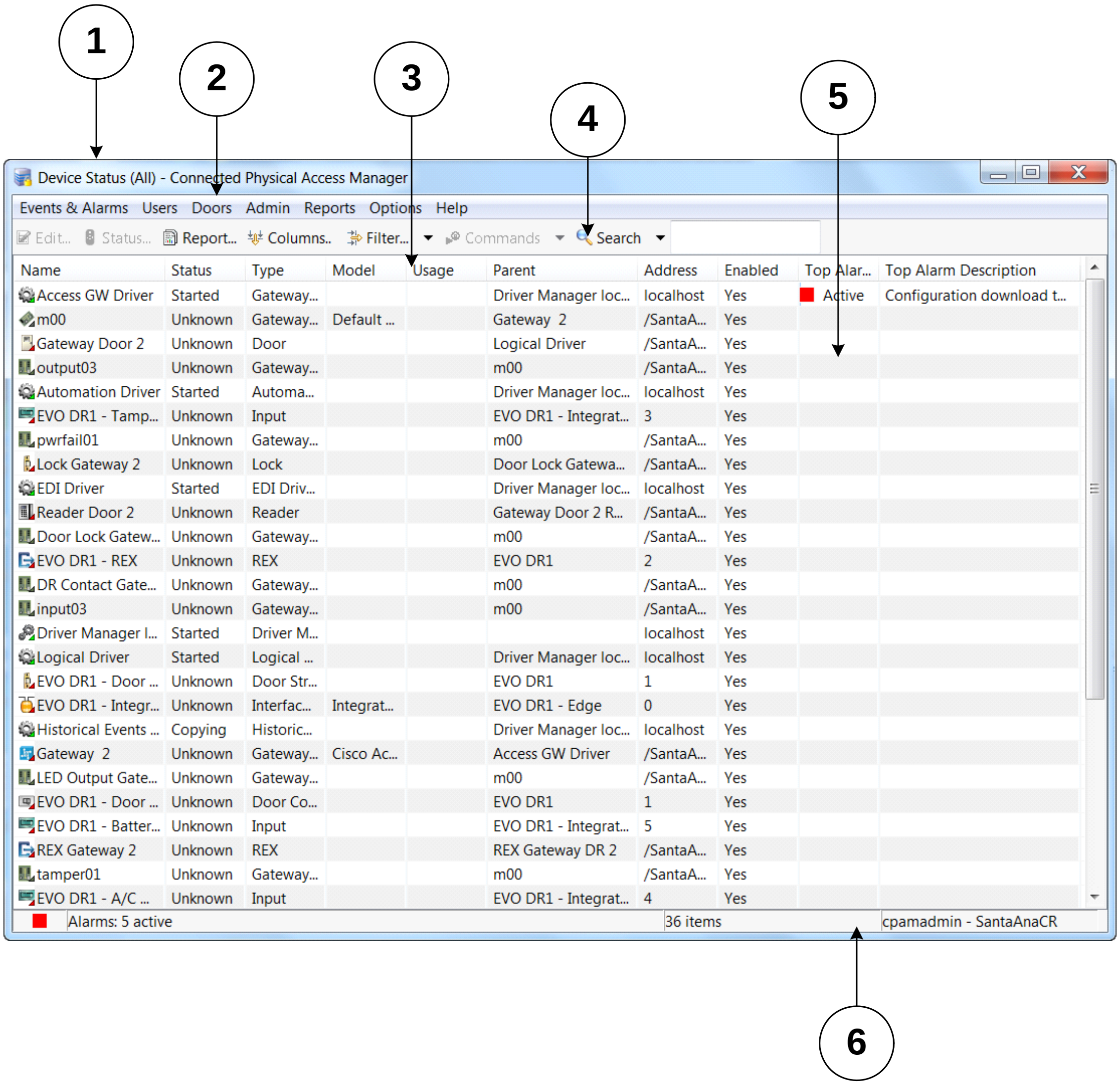
Step 3 Close the ICPAM window and reopen it for changes to take effect.

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

User Interface Elements

The user interface for most features includes the following elements:

Figure 3-7 User Interface Elements



Name	Status	Type	Model	Usage	Parent	Address	Enabled	Top Alar…	Top Alarm Description
Access GW Driver	Started	Gateway…			Driver Manager loc…	localhost	Yes	🟥 Active	Configuration download t…
m00	Unknown	Gateway…	Default …		Gateway 2	/SantaA…	Yes		
Gateway Door 2	Unknown	Door			Logical Driver	/SantaA…	Yes		
output03	Unknown	Gateway…			m00	/SantaA…	Yes		
Automation Driver	Started	Automa…			Driver Manager loc…	localhost	Yes		
EVO DR1 - Tamp…	Unknown	Input			EVO DR1 - Integrat…	3	Yes		
pwrfail01	Unknown	Gateway…			m00	/SantaA…	Yes		
Lock Gateway 2	Unknown	Lock			Door Lock Gatewa…	/SantaA…	Yes		
EDI Driver	Started	EDI Driv…			Driver Manager loc…	localhost	Yes		
Reader Door 2	Unknown	Reader			Gateway Door 2 R…	/SantaA…	Yes		
Door Lock Gatew…	Unknown	Gateway…			m00	/SantaA…	Yes		
EVO DR1 - REX	Unknown	REX			EVO DR1	2	Yes		
DR Contact Gate…	Unknown	Gateway…			m00	/SantaA…	Yes		
input03	Unknown	Gateway…			m00	/SantaA…	Yes		
Driver Manager l…	Started	Driver M…				localhost	Yes		
Logical Driver	Started	Logical …			Driver Manager loc…	localhost	Yes		
EVO DR1 - Door …	Unknown	Door Str…			EVO DR1	1	Yes		
EVO DR1 - Integr…	Unknown	Interfac…	Integrat…		EVO DR1 - Edge	0	Yes		
Historical Events …	Copying	Historic…			Driver Manager loc…	localhost	Yes		
Gateway 2	Unknown	Gateway…	Cisco Ac…		Access GW Driver	/SantaA…	Yes		
LED Output Gate…	Unknown	Gateway…			m00	/SantaA…	Yes		
EVO DR1 - Door …	Unknown	Door Co…			EVO DR1	1	Yes		
EVO DR1 - Batter…	Unknown	Input			EVO DR1 - Integrat…	5	Yes		
REX Gateway 2	Unknown	REX			REX Gateway DR 2	/SantaA…	Yes		
tamper01	Unknown	Gateway…			m00	/SantaA…	Yes		
EVO DR1 - A/C …	Unknown	Input			EVO DR1 - Integrat…	4	Yes		

🟥 Alarms: 5 active 36 items cpamadmin - SantaAnaCR

The following items are shown in Figure 3-7:

Table 3-1 User Interface Elements

	UI Element	Description
1	Window Title Bar	Shows the module and application name (for example: Device Status (All)).
2	Menu Bar	Allows the operator to perform a number of functions, including open a new module, close a module or the application, and get help. The menu bar is the same for all modules.

Table 3-1 User Interface Elements (continued)

	UI Element	Description
3	Table Columns	Column visibility and order may be edited using the **Columns...** button. Column width may be adjusted by dragging the edge of the column header. Clicking the column header allows the list to be sorted by a particular column. A directional arrow shows the current sort column, as well as the direction. Clicking the column header a second time reverses the sort order. See Revising the Column Display, page 3-14.
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 3-10. • **Filter:** Select or edit a filter. This determines which items are visible in the table. See Using Filters, page 3-12. • **Columns...:** Configure which columns are visible, and the order in which they appear. See Revising the Column Display, page 3-14. • **Group Edit:** Make changes to all items displayed in a module table. See Using Group Edit, page 3-14. • **Quick Search:** Quickly search results in the main module window. See Search, page 3-15.
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 3-10
- Using Filters, page 3-12
- Revising the Column Display, page 3-14
- Using Group Edit, page 3-14
- Search, page 3-15

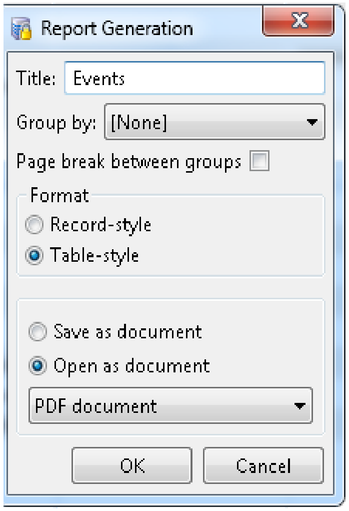
Creating Reports

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

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

Step 2 Click the **Report...** button in the toolbar. This opens the **Report Generation** window (Figure 3-8).

Figure 3-8 Report Generation Window



Report Generation

Title: Events

Group by: [None]

Page break between groups □

Format

○ Record-style

● Table-style

○ Save as document

● Open as document

PDF document

The following items are shown in Figure 3-8.

Table 3-2 Report Generation

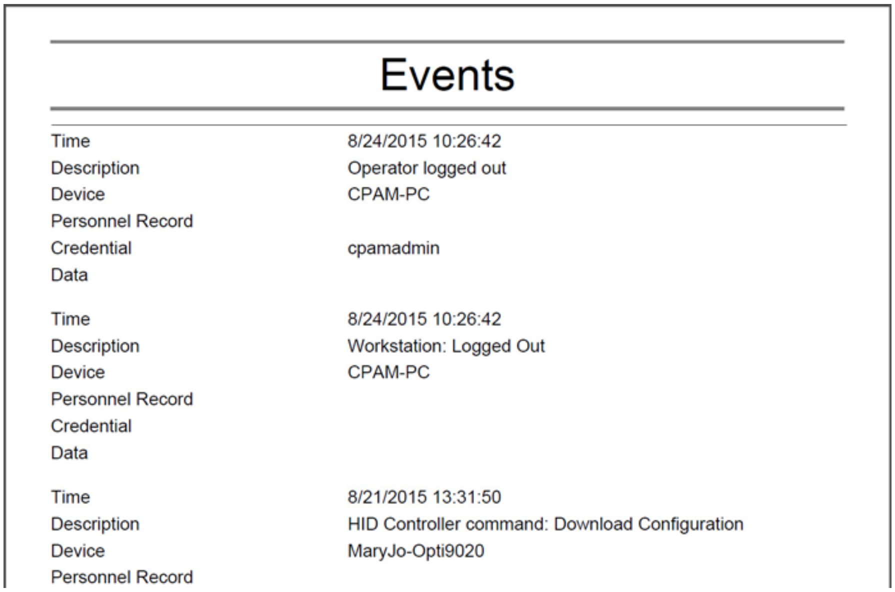
Type	Description
Title	The title of the report.
Include	Depending on the type of objects in the report (event, badge, personnel record, and so on.), there may be additional details that are to be included in the report. If so, these will be available as check boxes. For example, in a report of personnel records, checking the **Badges** option will include a list of badges assigned to each person.

Table 3-2 Report Generation (continued)

Type	Description
Group by	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.
Format	• **Record-style:** displays the data similarly to the layout of an address book, and in a portrait (vertical) view. • **Table-style:** displays the data in a grid layout, similar to a spreadsheet, and in a landscape (horizontal) view.
Viewing Options	• **Open in report:** Opens the report with an integrated report . • **Save as document:** Saves the report as PDF document, Excel spreadsheet, OpenDocument Text, Text (tab-delimited), HTML, and OpenDocument Spreadsheet. • **Open as document:** Allows you to open the report in a number of formats, including PDF document, Excel spreadsheet, OpenDocument Text, Text (tab-delimited), HTML, and OpenDocument Spreadsheet.

Step 3 Choose the desired options, and then click **OK** to save or open the report. This may take a moment, depending on the size and complexity of the report. Figure 3-9 shows a report in PDF format from the **Events** module.

Figure 3-9 Events Report in Report



Events

Time	8/24/2015 10:26:42
Description	Operator logged out
Device	CPAM-PC
Personnel Record	
Credential	cpamadmin
Data	
Time	8/24/2015 10:26:42
Description	Workstation: Logged Out
Device	CPAM-PC
Personnel Record	
Credential	
Data	
Time	8/21/2015 13:31:50
Description	HID Controller command: Download Configuration
Device	MaryJo-Opti9020
Personnel Record	

Using Filters

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

- **No Filter**: Show all items, without filtering.
- **Default Filter**: The default view of the table. Shows all enabled items.
- **Presets**: Select from preset filters. A check mark next to the filters displays which filter is currently in use, as shown in Figure 3-11.
- **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.

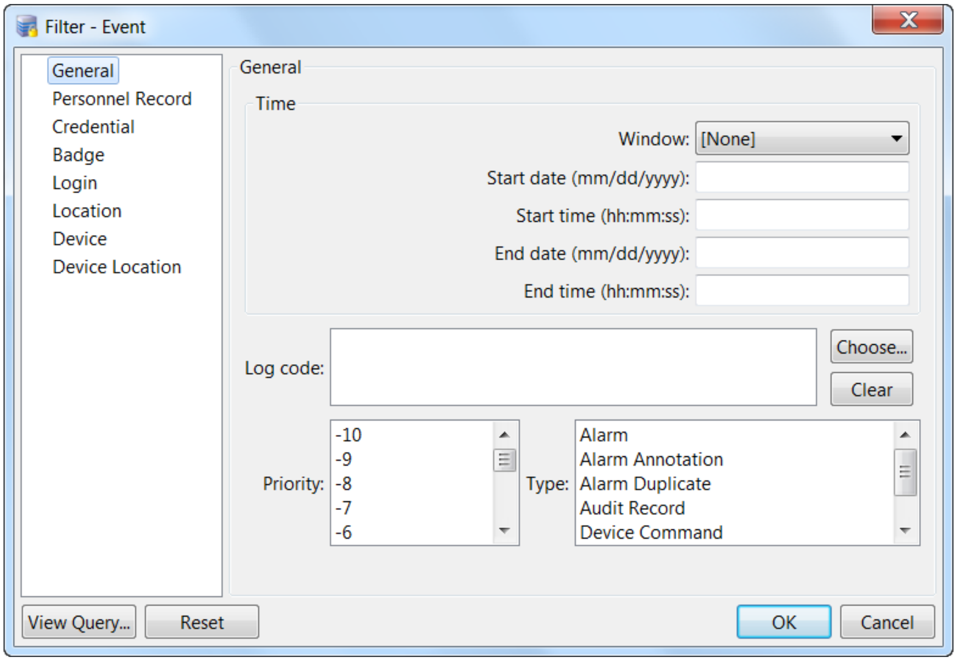
Filter Example

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

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

Step 2 Click **Filter** in the toolbar to open the filter window, as shown in Figure 3-10.

Figure 3-10 Filter - Event Window

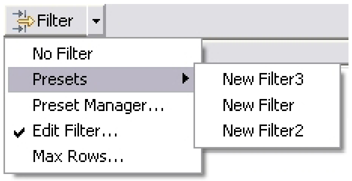


Window: [None]

Step 3 Specify the object filtering criteria:.

- The **General**, **Personnel Record**, **Credential**, **Badge**, **Login**, and **Device** tabs on the left specify the event criteria, such as the event's properties or associated objects.
- The **View Query...** button opens a window detailing the actual filter definition as an SQL-like expression string.
- The **Save as Preset...** button saves the filter criteria as a named preset for later use. Once a filter is saved as a preset, it can be selected from the **Filter** button drop-down menu, as shown in Figure 3-11.
- The **Reset** button clears the filter so that all enabled items will be displayed.

Figure 3-11 Filter Presets



Step 4 Choose the criteria to filter by, then click the **OK** button. This closes the window, and the table view is updated to reflect the filter criteria. Incoming events will also be filtered according to these criteria.

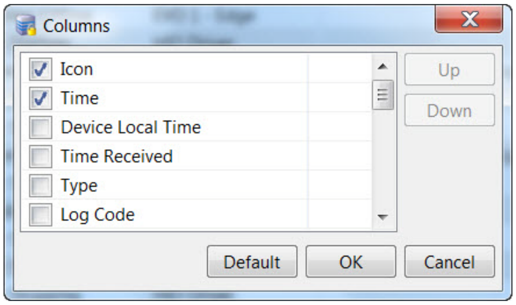
Revising the Column Display

The **Columns...** button in the toolbar allows you to change the order and visibility of columns.

Click the **Columns...** button to open the window shown in Figure 3-12.

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

Figure 3-12 Columns Window for the Event Manager



☑ Icon
☑ Time
□ Device Local Time
□ Time Received
□ Type
□ Log Code

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

Using Group Edit

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

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

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

Group Edit Example

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

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

Step 2 Filter the list so it contains only the records to be changed.

a. Click the **Filter** button in the toolbar.

b. Select the **Assigned to** tab.

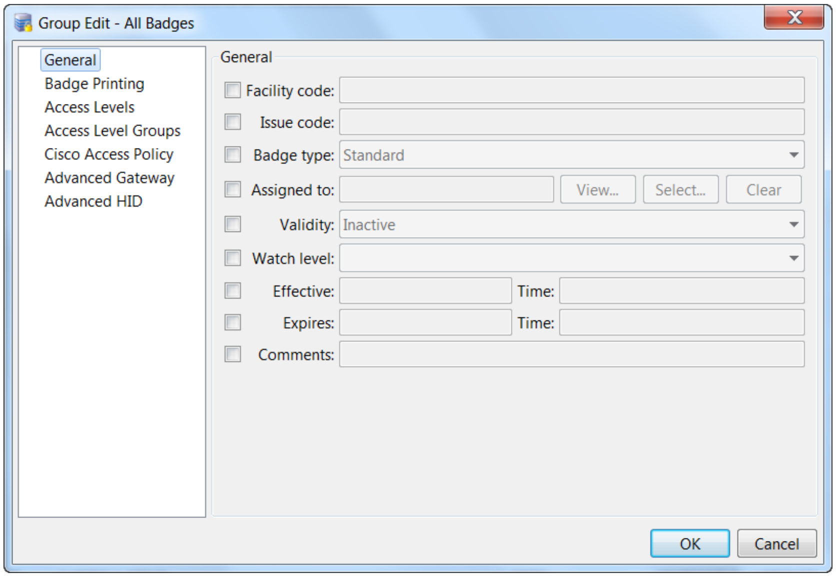
c. Select **Contractor** in the **Personnel type** field.

d. Click **OK** to filter the badges to contractor personnel types.

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

Step 3 In the Badges window, click the **Group Edit...** button to open the **Group Edit...** window, as shown in Figure 3-13.

Figure 3-13 Group Edit - General Window



Group Edit - All Badges

General
Badge Printing
Access Levels
Access Level Groups
Cisco Access Policy
Advanced Gateway
Advanced HID

General

□ Facility code:

□ Issue code:

□ Badge type: Standard

□ Assigned to: View... Select... Clear

□ Validity: Inactive

□ Watch level:

□ Effective: Time:

□ Expires: Time:

□ Comments:

OK Cancel

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

Step 5 Click **OK**.

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

Search

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

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

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

CHAPTER 4

Configuring User Access for the ICPAM Desktop Client

This chapter describes how to configure operators for the ICPAM 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 ICPAM Desktop Software, page 3-2.

Contents

Defining User Profiles for Desktop Application Access

Profiles are pre-defined sets of access privileges that define the ICPAM 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 Logins Settings, page 17-10), the following changes occur in this module:

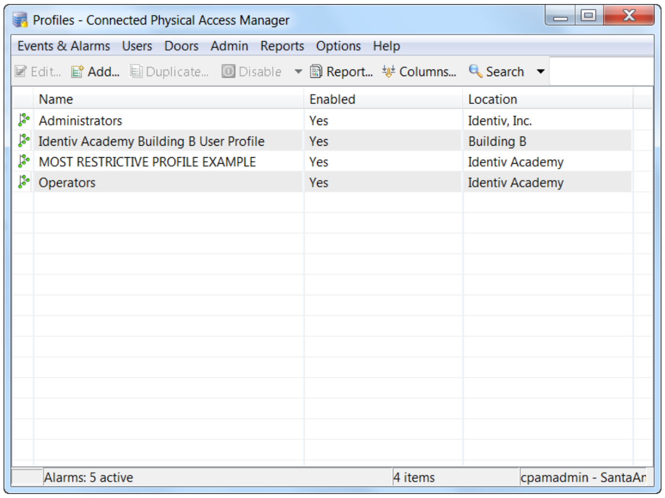
- While creating user profiles, the application prompts the user to select hierarchical location for a specific user profile.
- When the profile enhancement feature is set, the administrator profile cannot be reused even by the cpamadmin, i.e the cpamadmin cannot assign the administrator profile to any 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.

Figure 4-1 Profiles Module Main Page



Name	Enabled	Location
Administrators	Yes	Identiv, Inc.
Identiv Academy Building B User Profile	Yes	Building B
MOST RESTRICTIVE PROFILE EXAMPLE	Yes	Identiv Academy
Operators	Yes	Identiv Academy

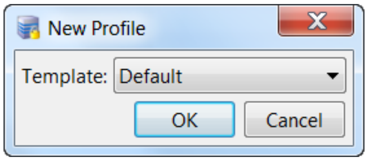
Alarms: 5 active 4 items cpamadmin - SantaAr

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

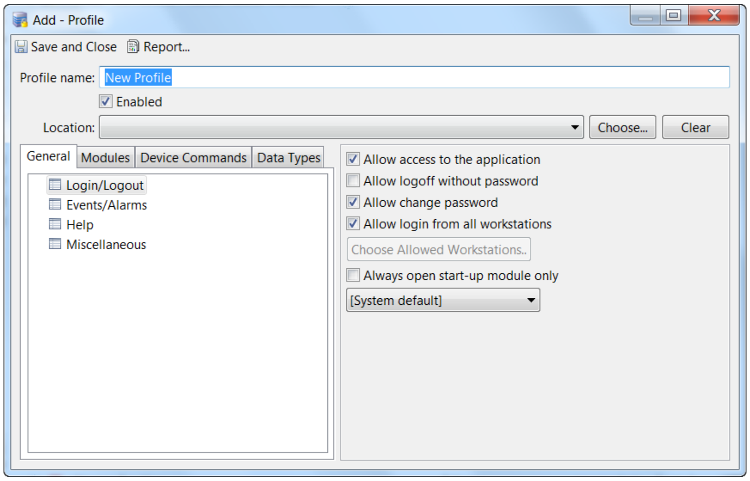
Figure 4-2 Profile Templates



Template: Default

Step 4 Click **OK** to open the Add Profile screen,

Figure 4-3 Add Profile



Profile name: New Profile

☑ Enabled

Location:

☑ Allow access to the application

□ Allow logoff without password

☑ Allow change password

☑ Allow login from all workstations

□ Always open start-up module only

[System default]

Step 5 Enter the basic profile settings:

- Profile name
- Enabled
- 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 4-1.

Table 4-1 General Settings: Profile Module

Field	*Description*
Login/Logout	
Allow access to the application	Allows users to access the application.
Allow logoff without password	Allows users to logoff without the password.
Allow change password	Allows users to change password.
Allow login from all workstations	Allows users to log in to the application from different work stations.
Events/Alarms: Alarm Annotations (Ack., Clear, Comment)	
Allow annotations	Allows users to acknowledge, clear, and comment alarms. Click the **Filter** button to define the events that trigger the action.
Allow multiple annotations	Allows users to acknowledge, clear, and comment multiple alarms at one time.
Allow clearing of unacknowledged alarms	Allows users to clear unacknowledged alarms from the active devices.
Allow clearing of active device alarms	Allows users to clear alarms from active devices.
Require comment on clearing alarms	Allows users to clear the alarms that are not required anymore.

Table 4-1 General Settings: Profile Module (continued)

Field	*Description*
Events/Alarms: On new alarms	
Open Alarms Module	Automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open Manage Alarm window	Opens automatically to acknowledge/comment/clear the alarms. Click the **Filter** button to define the events that trigger the action.
Open map	Automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show recorded video	Displays recorded video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show live video	Displays live video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show camera grid	Allows the user to view the video stream in a grid format.
Help: defines access to the different help systems.	
Allow access to help documentation	Allows users to access help documentation.
Enable context menu in help browser	Allows users to view the help context menu.
Allow access to help PDF	Allows users to access the help PDF. To access the help PDF, Adobe PDF is required.
Miscellaneous	
Allow issuing device command as default	Allows users to issue device commands directly to hardware.
Allow access to external hyperlinks	Allows users to access external hyperlinks.
Require device commands to be commented	Requires users to enter a comment with each device command issued in the system.
Allow editing from right-click menus	Allows users to access the right-click Edit menu.
Allow edit preferences	Allows users to edit preferences.
Rich client: Open modules in new window	Allows users to open modules in a new window.

Step 7 Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 4-5.

a. Select a ICPAM module.

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

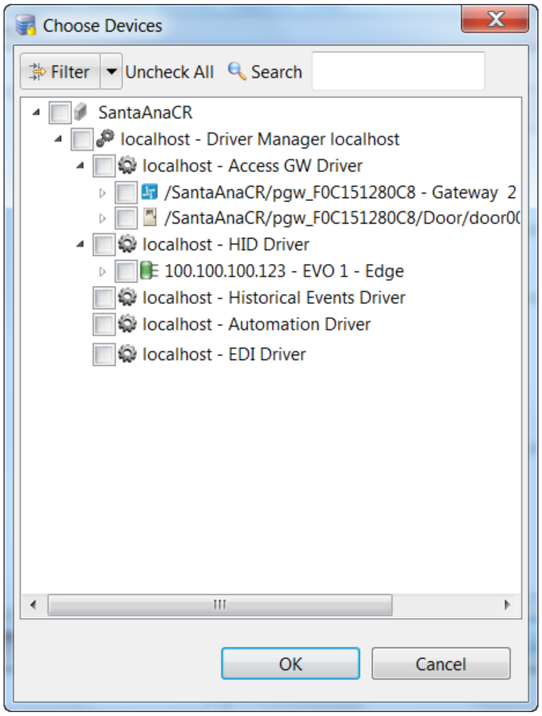
c. (Optional) Use the **Default Filter** with modules such as Event, Badge, and Personnel to define the filter applied when a user opens the module.

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:

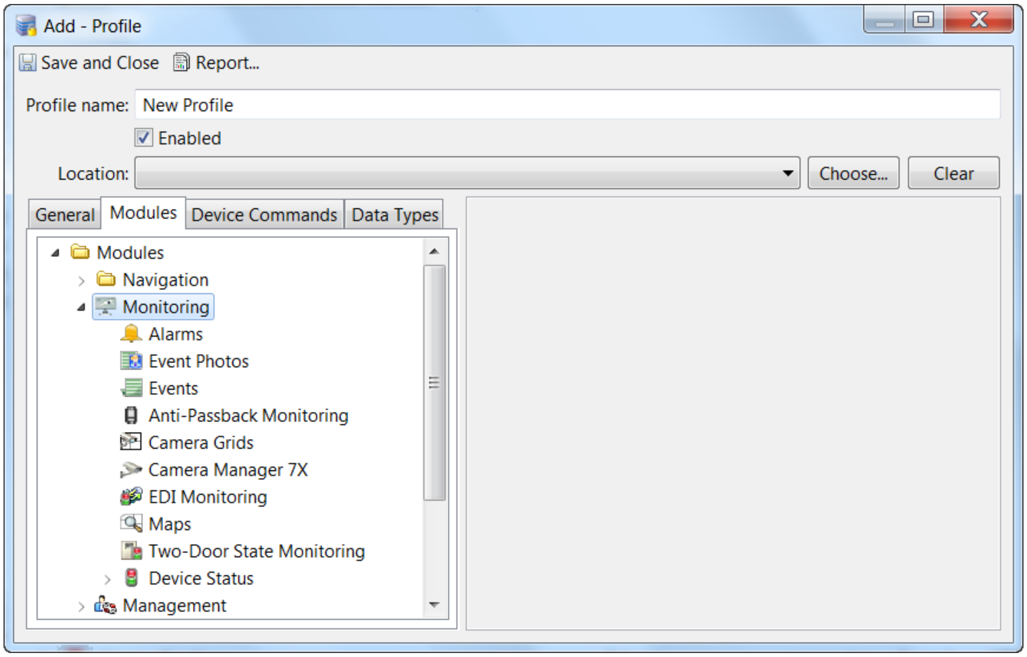
- Create a profile with access to the Events module, as described in the previous steps.
- Click **Default Filter**, as shown in Figure 4-5.
- Select the **Device** tab.
- Click **Choose**.
- In the Choose Devices window, expand the physical driver device tree and select a door.

Figure 4-4 Choose Device


Choose Devices
Filter
Uncheck All
Search
SantaAnaCR
localhost - Driver Manager localhost
localhost - Access GW Driver
/SantaAnaCR/pgw_F0C151280C8 - Gateway 2
/SantaAnaCR/pgw_F0C151280C8/Door/door0(
localhost - HID Driver
100.100.100.123 - EVO 1 - Edge
localhost - Historical Events Driver
localhost - Automation Driver
localhost - EDI Driver
OK
Cancel

- Click **OK** to save the changes and close the windows.

Figure 4-5 Profile-Modules Tab



Add - Profile

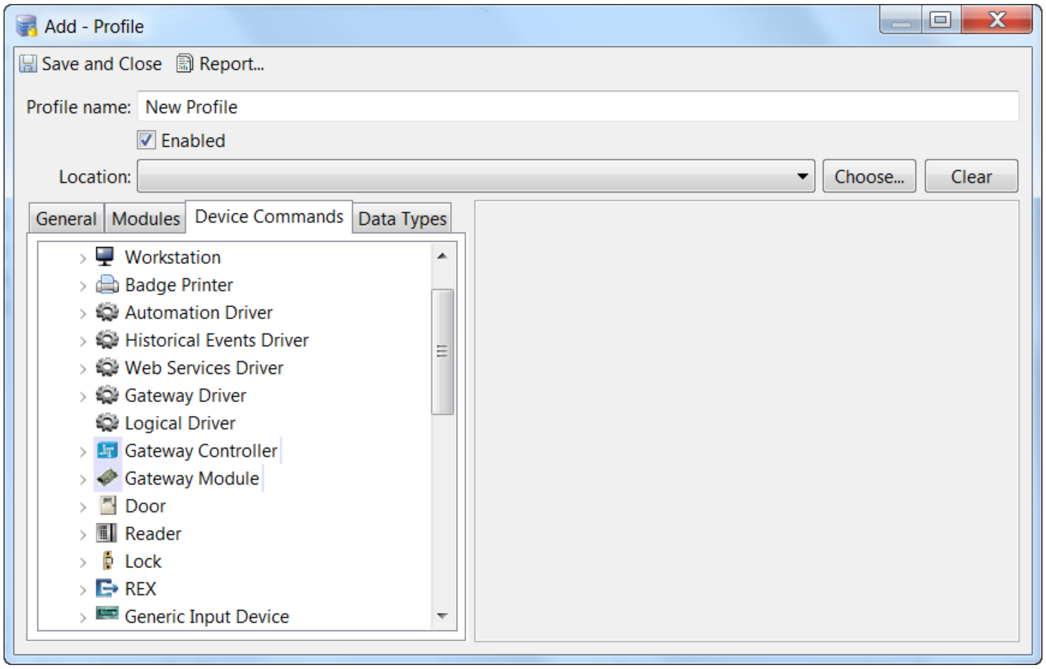
Profile name: New Profile

☑ Enabled

Location:

Step 8 Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 4-6).

Figure 4-6 Profiles- Device Commands Tab



Add - Profile

Profile name: New Profile

☑ Enabled

Location:

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

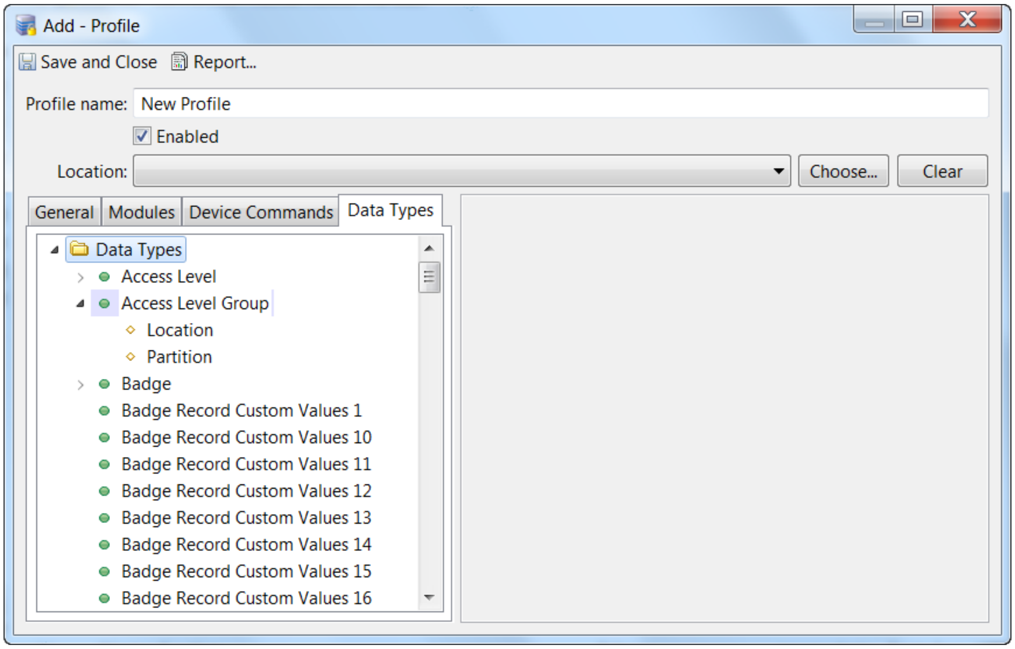
b. Highlight a command.

c. Select the following options:

- **Allow Command to be issued:**
  - **Default**: If user has access to issue device commands, the command access is enabled by default.
  - **No**: Deny access to the command.
  - **Yes**: Allow access to the command.
- **Filter**: Apply a filter to limit the devices for the command.

Step 9 Click the **Data Types** tab to define the data available to the profile.

Figure 4-7 Profiles-Data Type



Profile name: New Profile

☑ Enabled

Location:

- Data Types
  - Access Level
  - Access Level Group
    - Location
    - Partition
  - Badge
  - Badge Record Custom Values 1
  - Badge Record Custom Values 10
  - Badge Record Custom Values 11
  - Badge Record Custom Values 12
  - Badge Record Custom Values 13
  - Badge Record Custom Values 14
  - Badge Record Custom Values 15
  - Badge Record Custom Values 16

a. Select a module and the type of data in the list.

b. To restrict the data, check the check boxes for the following properties:

Table 4-2 Profile: Data Types

Field	Description
View	Allows the user to view the selected data type.
Create	Allows the user to add and create the selected data types.
Modify	Allows the user to modify existing data.
Delete	Allows the user to delete data.

Step 10 Click **Save and Close** to save the profile settings.

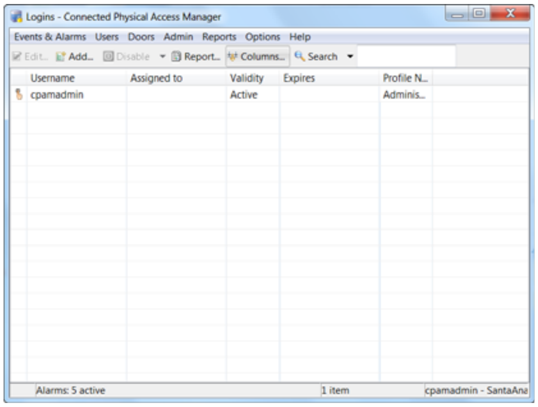
Step 11 Assign the profile to one or more ICPAM operators using the **Logins** module. See Creating User Login Accounts and Assigning Profiles.

Creating User Login Accounts and Assigning Profiles

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

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

Figure 4-8 Logins Module Main Window


Logins - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Disable Report... Columns... Search

Username	Assigned to	Validity	Expires	Profile N...
cpamadmin		Active		Adminis...

Alarms: 5 active 1 item cpamadmin - SantaAna

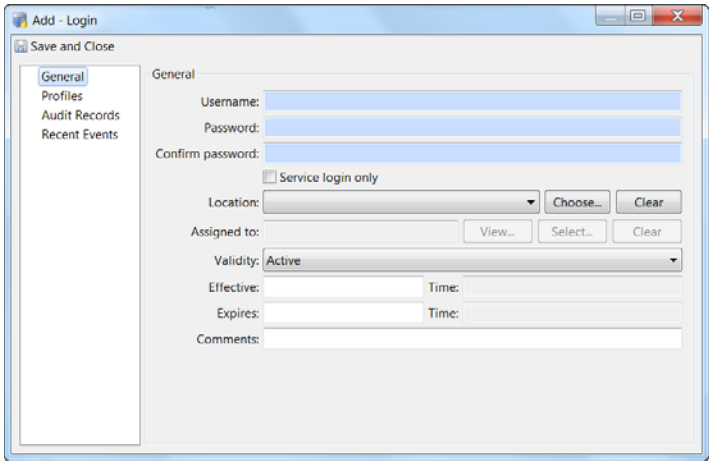
Step 2 Do one of these procedures:

- 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 4-3 describes the field properties.

Figure 4-9 Add Login: General Tab



□ Service login only

Validity: Active

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

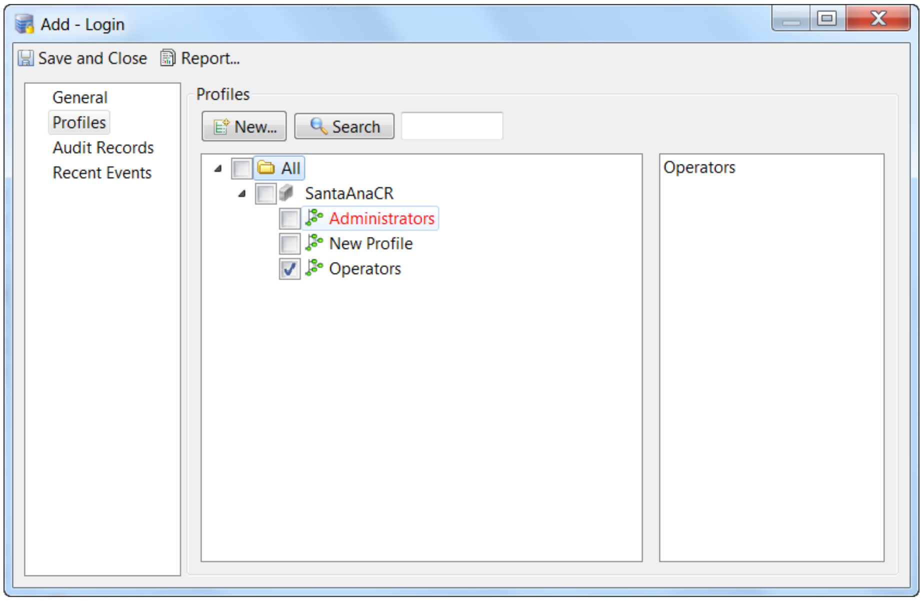
Table 4-3 General Tab Fields.

Field	**Description**
Username	Required. The username of the login.
Password	Required. Password to access the system.
Confirm password	Required. The value must be entered exactly as it was in the **Password** field.
Location	This field specifies the login location of a user. Each login location can be accessed only by users belonging to that specific location.
Assigned to	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”.
Validity	**Active** or **Inactive**. Only active accounts can access the system.
Effective	The beginning date the user can log in. If left blank, the user can log in immediately.
Time	The login time of the user.
Expires	The day the login expires and access is denied. If left blank, access is allowed indefinitely.
Time	The time the user login expires.
Site	Read-only. A site is a single instance of a ICPAM database.
Comments	Comments or notes about the login.

Step 4 To create a location-restricted user:

a. Select the **Profiles** tab.

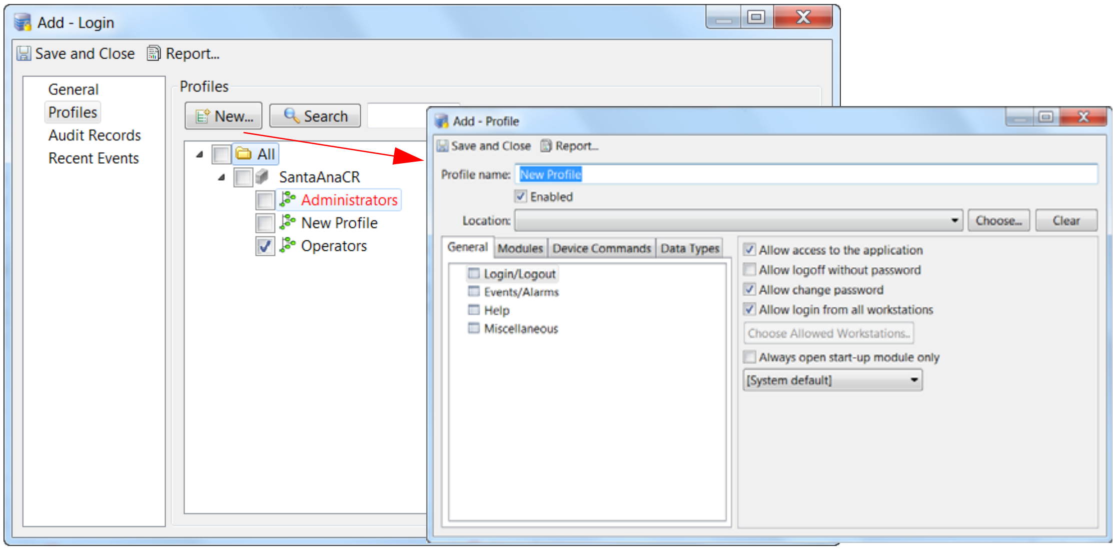
Figure 4-10 Add Login Profiles



☑ Operators

b. To create a new profile, click **New...** A new page opens like Figure 4-11.

Figure 4-11 Add Profile



Profile name: New Profile

☑ Enabled

☑ Allow access to the application
□ Allow logoff without password
☑ Allow change password
☑ Allow login from all workstations
□ Always open start-up module only
[System default]

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

- 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 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 Logins Settings, page 17-10), the user actions are not restricted to the locations. The configuration settings now reflects the ICPAM 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 4-12
- Create the LDAP User Account in ICPAM, page 4-14

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 selected:

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

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

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

For more information, see the following:

- LDAP Example: User Principal Name, page 4-13
- LDAP Example: sAMAccountName, page 4-14

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

Table 4-4 LDAP System Configuration Settings

Field	Description
Enable LDAP	Click the check box to enable or disable LDAP support.
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.

Table 4-4 LDAP System Configuration Settings (continued)

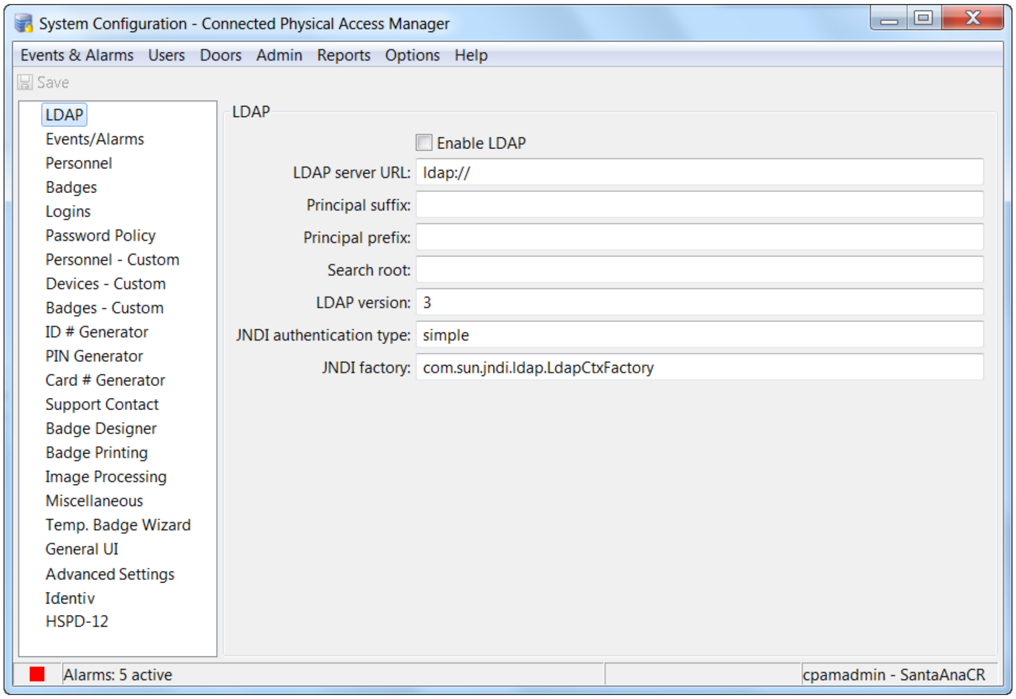
Field	Description
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: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

Step 4 Stop and start the ICPAM application from the web admin page to enable the changes.

LDAP Example: User Principal Name

In the example shown in Figure 4-12, the user principal name is `cpsm.user@ad1.cpamlab`. The ICPAM user login must be the same (`cpsm.user`).

Figure 4-12 User Principal LDAP Configuration Example



LDAP

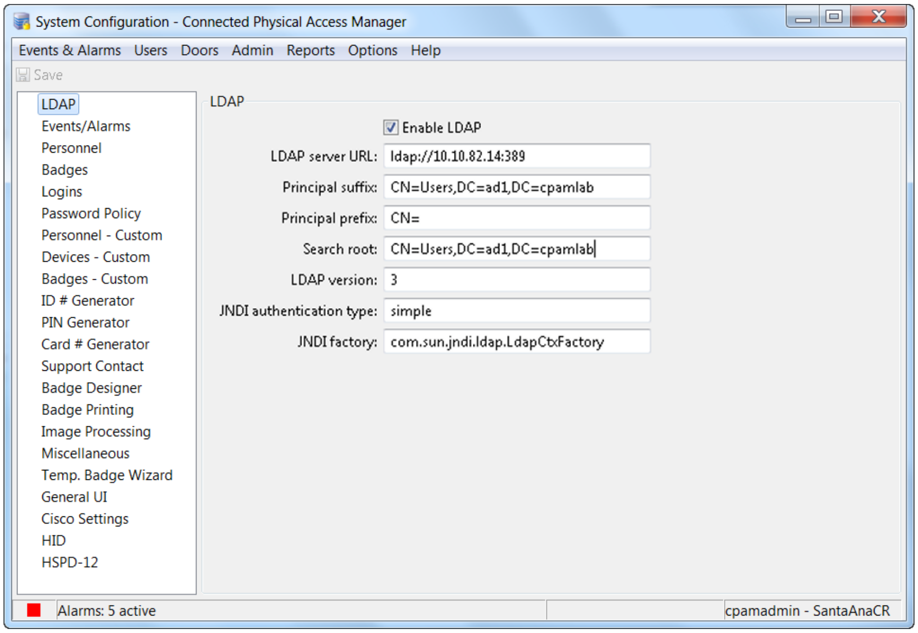
☐ Enable LDAP

LDAP server URL: ldap://
Principal suffix:
Principal prefix:
Search root:
LDAP version: 3
JNDI authentication type: simple
JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

LDAP Example: sAMAccountName

In the example shown in Figure 4-13, the user login is the same as the samaccount name (`cpsmuser`).

Figure 4-13 sAMAccountName: LDAP Configuration Example



LDAP

☑ Enable LDAP

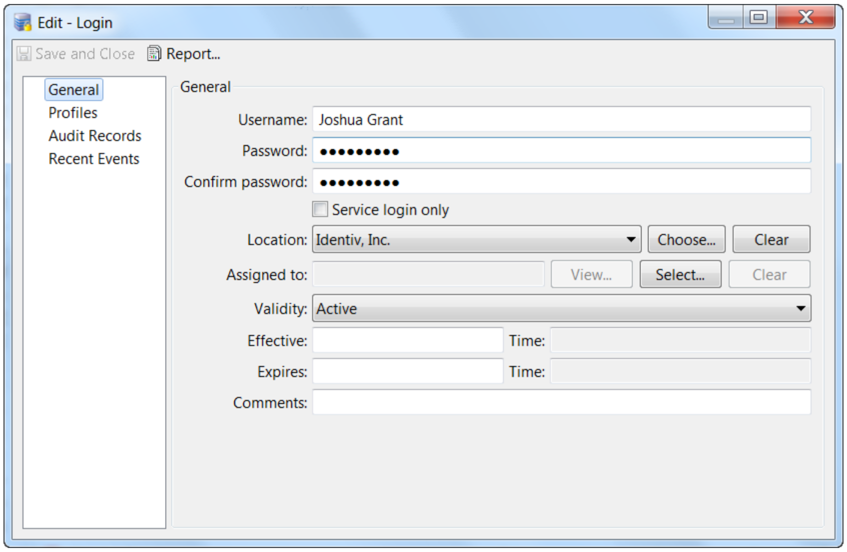
LDAP server URL: ldap://10.10.82.14:389
Principal suffix: CN=Users,DC=ad1,DC=cpamlab
Principal prefix: CN=
Search root: CN=Users,DC=ad1,DC=cpamlab
LDAP version: 3
JNDI authentication type: simple
JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

Create the LDAP User Account in ICPAM

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

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

Figure 4-14 Login Window: LDAP Login Type



Username: Joshua Grant
Password: •••••••••
Confirm password: •••••••••
□ Service login only
Location: Identiv, Inc.
Assigned to:
Validity: Active
Effective: Time:
Expires: Time:
Comments:

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 ICPAM application was restarted (see Configure the LDAP Server, page 4-12).

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

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

Step 5 Click **Profiles** and select the user's ICPAM profiles. See Defining User Profiles for Desktop Application Access, page 4-1 for more information.

Note ICPAM does not synchronize the LDAP profiles.

Step 6 Click **Save and Close**.

Viewing Audit Records for Changes to Usernames

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

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

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

Step 3 Select **Audit Records**, as shown in Figure 4-15.

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

Figure 4-15   Logins Audit Records Window

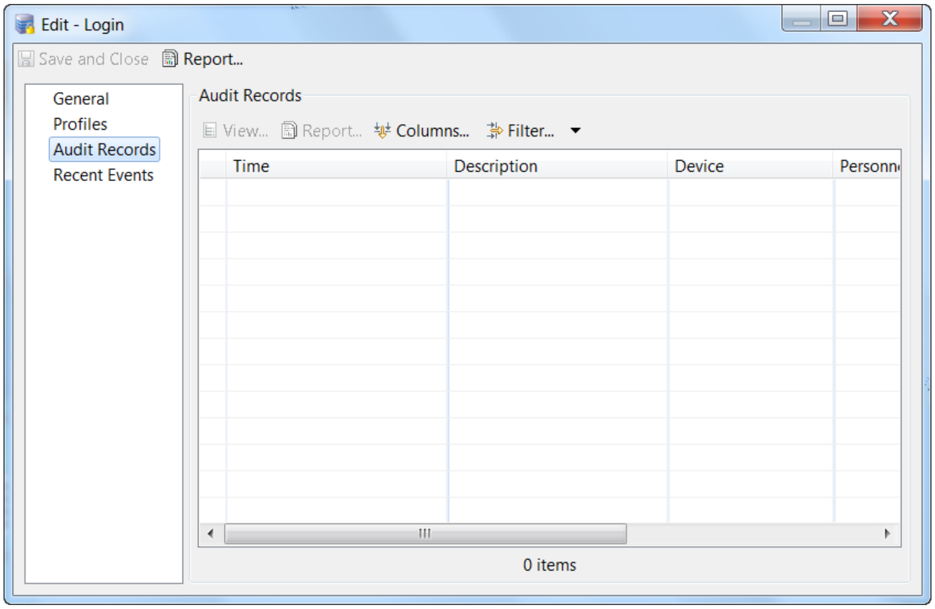


Table 4-5   Logins Module: Audit Records Fields

Field	Description
Time	The time and date when the modification occurred.
Time Received	The time and date when the modification was saved.
Site	The site where the modification occurred. A site is a single instance of a ICPAM database.
Type	The type of change.
Log code	An abbreviated code uniquely identifying the type of change.
Priority	A priority used for sorting events and alarms. Positive priorities are above normal priority, while negative priorities are below normal priority. Zero is normal.
Description	A description of the change.
Device	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.

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

Field	Description
Credential	The username used when the modification occurred. Click **View** to display and revise details for the username.
Personnel record	The name of the operator associated with the modification (if the login was associated with a personnel record at the time).
Data	Additional information about the modification.
View Current...	Opens a new window displaying the current settings.
View Before...	Opens a new window displaying the settings before the change was made.
View After...	Opens a new window displaying the settings after the change was made.

Managing Desktop Client Passwords

- Changing Your Password, page 4-17
- Changing Another User's Password, page 4-17
- Managing the cpamadmin Login and Password, page 4-18

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 4-8 for instructions.

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

Managing the *cpamadmin* Login and Password

The **cpamadmin** login and password are created during the initial server setup, as described in Chapter 2, "Configuring and Monitoring the ICPAM Server". After the initial setup, however, the **cpamadmin** login and password for the desktop client are managed independently of the server login: changes to the desktop login do not effect the server login. See Changing or Recovering the Server Password, page 2-40 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.

CHAPTER 5

Understanding Controller and Door Configurations

This chapter describes the concepts used to configure controllers, doors, and their respective templates.

A door configuration is a collection of devices, such as locks and readers, connected to a controller and configured in ICPAM. To configure a door, add a controller to ICPAM and then assign one or more door configurations to the controller using the pre-defined door templates. Door configuration templates include common sets of devices and configurations to simplify access control configuration. Controllers and the associated doors can be configured either before or after the controller 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 8, "Configuring Door and Device Templates" for more information.

Contents

Provisioned (Pre-Populated) vs. Discovered Controller Configurations

You can configure a gateway in ICPAM before or after the module is added to the network.

Note See also Configuration Management in Provisioned vs. Discovered Configurations, page 7-14.

Provisioned (Pre-Populated) Configuration

A *provisioned* configuration occurs when a gateway configuration is entered in ICPAM before the module is brought online. If the controller serial number matches the existing ICPAM configuration when the module is added to the network, ICPAM automatically downloads the existing configuration to the module.

- Subsequent changes to the configuration must be manually applied, as described in Applying Configuration Changes, page 7-12.
- If the controller connects to ICPAM and does not have a configuration (such as after a hard reset), the latest configuration applied to that controller is downloaded.

Discovered Configuration

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

The controller is assigned a name based on "gw_" and the serial number. For example, if the controller serial number is `FHH112900XX`, the name of the discovered controller configuration in ICPAM will be `gw_FHH112900XX`.

After the controller 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 ICPAM appliance over the IP network. If the serial number for the controller or an attached expansion module already exists in the ICPAM configuration, the controller is not added.

Viewing Device and Door Configuration

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

Once the controllers and door configurations are added to ICPAM, you can view the configurations in a device view that lists the controllers, 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.

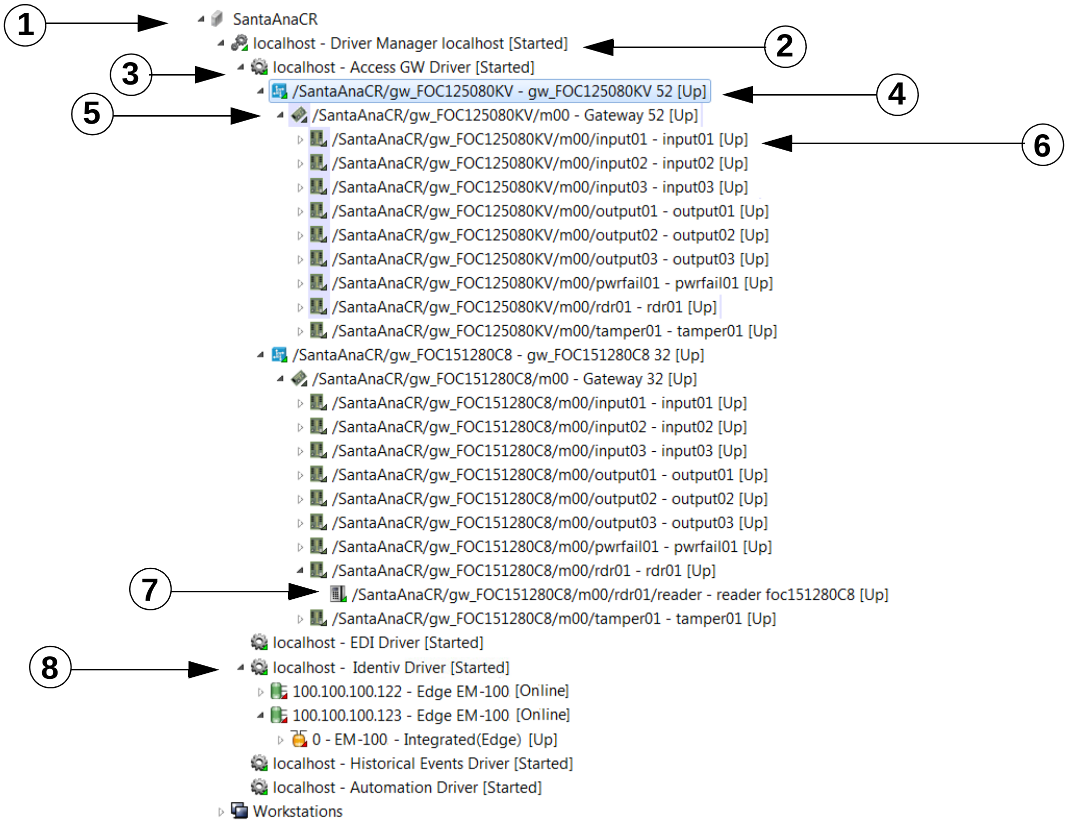
- Viewing Doors and Devices in the Hardware Tree View, page 5-4
- Hardware Manager in ICPAM 2.1, page 5-6
- Viewing Doors and Devices by Location, page 5-7
  - Creating the Location Map, page 5-8
  - Changing the Location of a Device or Door, page 5-9
  - Location-Restricted User Permissions, page 5-9

Viewing Doors and Devices in the Hardware Tree View

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

To open the device view, select **Hardware Tree** from the **Doors** menu. In the Hardware Tree window, select **Device** from the **View** menu. Controllers are listed by name (such as Cisco Gateway or EM-100 Controller) and represented by a blue icon, as shown in Figure 5-1. Click the box next to the icon to expand the hierarchical tree and view the expansion modules and other devices associated with the gateway.

Figure 5-1 Expanded Hardware Tree: Controllers and Related Devices



```
◢ SantaAnaCR
  ◢ localhost - Driver Manager localhost [Started]
    ◢ localhost - Access GW Driver [Started]
      ◢ /SantaAnaCR/gw_FOC125080KV - gw_FOC125080KV 52 [Up]
        ◢ /SantaAnaCR/gw_FOC125080KV/m00 - Gateway 52 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/input01 - input01 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/input02 - input02 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/input03 - input03 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/output01 - output01 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/output02 - output02 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/output03 - output03 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/pwrfail01 - pwrfail01 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/rdr01 - rdr01 [Up]
          ▷ /SantaAnaCR/gw_FOC125080KV/m00/tamper01 - tamper01 [Up]
      ◢ /SantaAnaCR/gw_FOC151280C8 - gw_FOC151280C8 32 [Up]
        ◢ /SantaAnaCR/gw_FOC151280C8/m00 - Gateway 32 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/input01 - input01 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/input02 - input02 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/input03 - input03 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/output01 - output01 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/output02 - output02 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/output03 - output03 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/pwrfail01 - pwrfail01 [Up]
          ◢ /SantaAnaCR/gw_FOC151280C8/m00/rdr01 - rdr01 [Up]
              /SantaAnaCR/gw_FOC151280C8/m00/rdr01/reader - reader foc151280C8 [Up]
          ▷ /SantaAnaCR/gw_FOC151280C8/m00/tamper01 - tamper01 [Up]
      localhost - EDI Driver [Started]
    ◢ localhost -  Identiv Driver [Started]
      ▷ 100.100.100.122 - Edge EM-100 [Online]
      ◢ 100.100.100.123 - Edge EM-100 [Online]
        ▷ 0 - EM-100 - Integrated(Edge) [Up]
      localhost - Historical Events Driver [Started]
      localhost - Automation Driver [Started]
  ▷ Workstations
```

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

Tip The names of all hardware tree elements are editable, including drivers, controllers, expansion modules, and door devices.

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

Table 5-1 Elements of the Device Tree

	Type	Description
1	Location	Read-only. A location is a single instance of a ICPAM 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 ICPAM only have a single database, and hence a single location. Multiple locations are used in larger configurations, such as a company with offices in distant locations that have a ICPAM database at each office.
2	Driver Manager	Read-only. The Driver Manager enables ICPAM hardware and software drivers, such as the GW Driver, Identiv EM-100 Driver, Automation Driver, Cisco VSM Driver, or the EDI Driver. The Driver Manager cannot be deleted. **Note** If you disable the Driver Manager then all the drivers, doors, gateway controllers 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 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 controller driver is an example of a device driver. Device drivers enable software and hardware functionality. Additional device drivers include the 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 is added for each controller device. The modules and devices configured on the gateway are listed below the gateway and include the gateway controller module, any expansion modules and the other devices attached to the module interfaces. Figure 5-1 shows an example hardware tree with the gateways, expansion modules, and other devices. To add a gateway to the configuration, right-click on the Access GW Driver and select **New Gateway Controller**.
5	Access Control Modules	Modules include the gateway, reader, input and output modules. Each configured module is listed under the controller, including the controller itself. **Note** The gateway module is displayed by default. Expansion modules are displayed only if added to the configuration. For information and instructions to install modules, see the *Cisco Physical Access Gateway User Guide*. For instructions to configure modules, see Chapter 7, "Configuring Doors".
6	Module Interface	Each module includes a set of interfaces for connecting door hardware and other devices. For descriptions of each module interface, see the *Cisco Physical Access Gateway User Guide*.

Table 5-1 Elements of the Device Tree (continued)

	Type	Description
7	Devices	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".
8	Identiv Driver	Devices associated with the EM-100 controller. For more on this, refer to Modifying Identiv EM-100 Drivers, page 6-37.

Hardware Manager in ICPAM 2.1

In ICPAM 2.1, if the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), the following changes are impacted in this module:

- The Hardware Tree module displays the controllers, expansion modules and other devices based on the user's hierarchical location only.
- The controller 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 and physical driver – Access GW Driver and local host – 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) controller is in another location (not of the location-restricted user), the controller is still visible to the location-restricted user and the user can execute commands on this controller.

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 ICPAM. Otherwise the ICPAM appliance retains its behavior as in the previous version (CPAM 1.5.1).

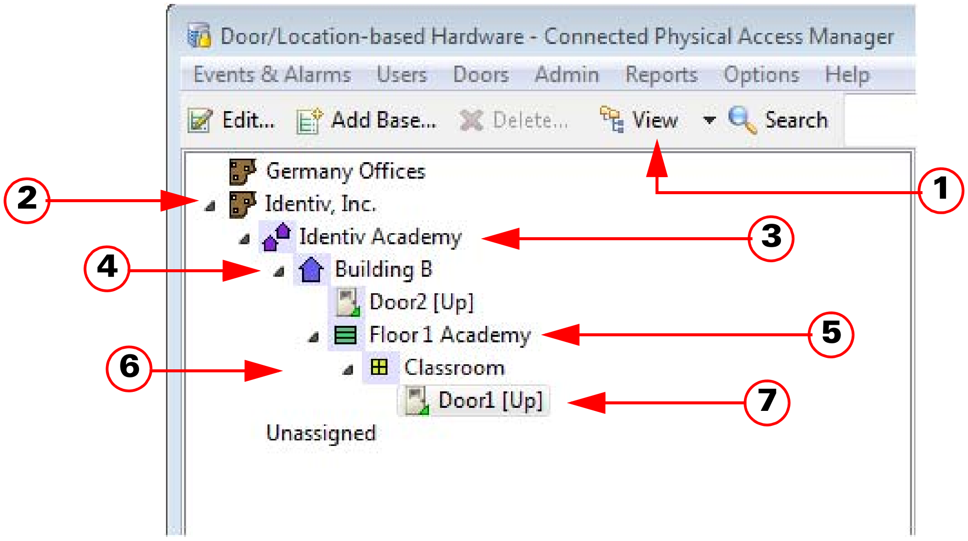
Viewing Doors and Devices by Location

Since gateways and related equipment are installed for specific locations, you can view door configurations in a hierarchical location map, as shown in Figure 5-2. This map is available in both the Hardware Tree module and the Door/Location-based Hardware 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 location, and assign the door configurations to a campus, building, floor, area, or sub-area. You can name the locations as needed, and place the doors at any level of the location hierarchy.

Figure 5-2 shows the location view in the Hardware Tree module. Select **Location** in the **View** menu to display the map. Although you can modify the door configurations from this view, you cannot change the location map. See Creating the Location Map, page 5-8 for more information.

Figure 5-2 Hierarchical Location View of Door/Location-Based Hardware



1	View Menu	**5**	Floor
2	Base	**6**	Area
3	Campus	**7**	Door
4	Building		

Tip

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

Creating the Location Map

To create or modify the location map for door configurations, select Door/Location-based Hardware from the Doors menu. This map is also displayed in the Hierarchical Location view of the Hardware Tree module, as described in Viewing Doors and Devices by Location, page 5-7.

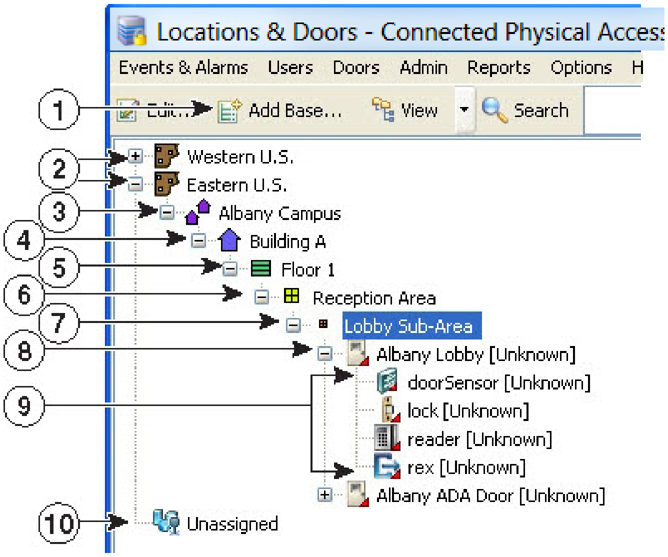
Figure 5-3 shows a sample location map. You can use any combination of map elements, such as campus, building, and floor.

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

- To create a new base, click the **Add Base...** button in the tool bar 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, right-click the driver appropriate to the controller (either EM-100 Driver or GW Access Driver) and select **Add Door**... For more on this, see Chapter 7, "Configuring Doors".

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

Figure 5-3 Door/Location-based Hardware: Main Window



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

1	Add Base... button	**6**	Area
2	Base	**7**	Sub-Area
3	Campus	**8**	Door
4	Building	**9**	Devices
5	Floor	**10**	Unassigned[1]

[1] Unassigned includes Doors and Devices that are not assigned to a location.

Changing the Location of a Device or Door

To change the location of a door or device (including controllers, 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.

Procedure

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** from the Doors menu.

- **Door/Location-based Hardware**: Select a device or door from the **View** menu.
- **Hardware Tree**: Select **Location** from the **View** menu.

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

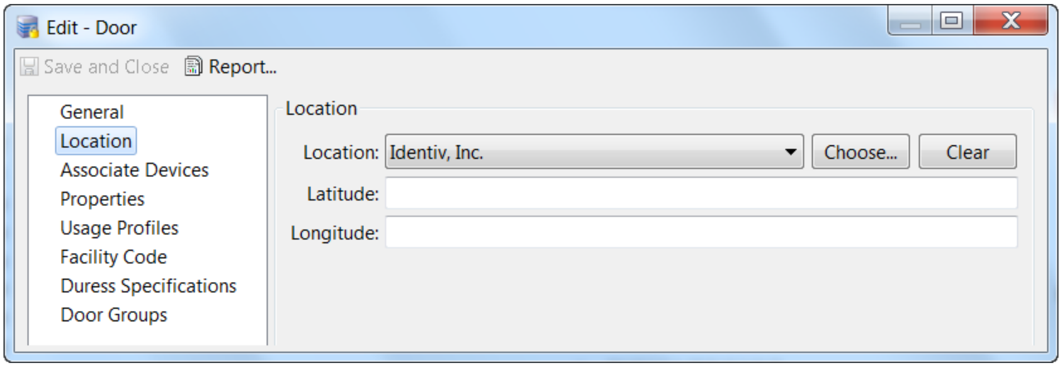
Step 3 Change the location for the device or door:

- 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 **Location** from the drop-down menu, as shown in Figure 5-4. You can also click the **Choose** button to select a location from the location map.

Figure 5-4 Editing the Location for a Door or Device



Location: Identiv, Inc.

Latitude:

Longitude:

Note If the location constraint is enabled (Logins Settings, page 17-10), the location-restricted users are allowed to change location to any location/sub location only under their hierarchical location.

Location-Restricted User Permissions

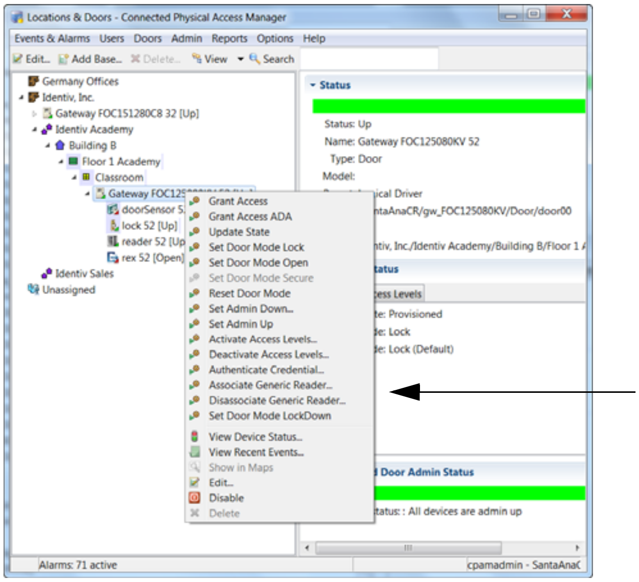
Location and Doors is the module where the location hierarchy is defined. The location hierarchy is defined as Base > Campus > Building > Floor > Area > Sub-Area.

After the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), 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 are 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 options for other locations (such as BVDC, for example) are grayed out (see Figure 5-5).

Figure 5-5 Door/Location-Based Options for Unprivileged Nodes



Status: Up
Name: Gateway FOC125080KV 52
Type: Door
Model:
ical Driver
ntaAnaCR/gw_FOC125080KV/Door/door00
ntiv, Inc./Identiv Academy/Building B/Floor 1 A
te: Provisioned
le: Lock
le: Lock (Default)
tatus: : All devices are admin up
Alarms: 71 active
cpamadmin - SantaAnaC

location-restricted user cannot execute device commands on devices from unprivileged nodes

- The unassigned node (location) 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.

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

Note These points are applicable only when the profile enhancement feature is set in the system configuration of the ICPAM; otherwise the ICPAM 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 on of the options described in this section:

- Viewing a Status Summary for All Devices, page 5-11
- Viewing the Status for a Single Door, Device or Driver, page 5-12
- Monitoring Device Errors, page 5-14
- Viewing the Recent Events for a Device or Driver, page 5-15

- Generating a Gateway Driver System Sanity Report, page 5-16

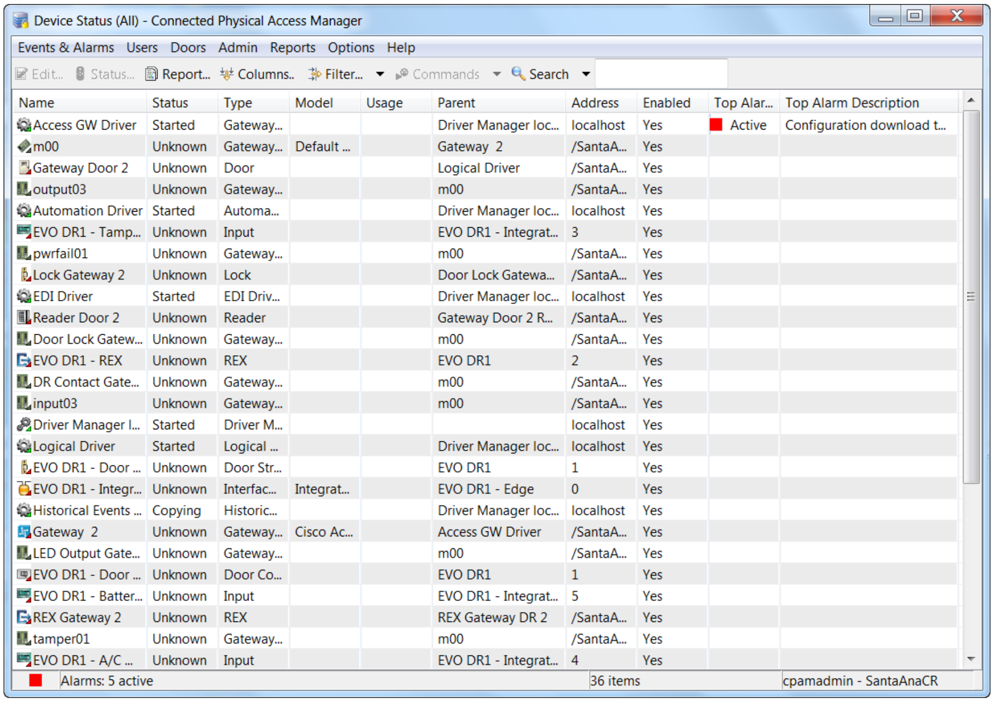
Viewing a Status Summary for All Devices

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

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

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

Figure 5-6 Device Status: Main Menu



Name	Status	Type	Model	Usage	Parent	Address	Enabled	Top Alar...	Top Alarm Description
Access GW Driver	Started	Gateway...			Driver Manager loc...	localhost	Yes	🟥 Active	Configuration download t...
m00	Unknown	Gateway...	Default ...		Gateway 2	/SantaA...	Yes		
Gateway Door 2	Unknown	Door			Logical Driver	/SantaA...	Yes		
output03	Unknown	Gateway...			m00	/SantaA...	Yes		
Automation Driver	Started	Automa...			Driver Manager loc...	localhost	Yes		
EVO DR1 - Tamp...	Unknown	Input			EVO DR1 - Integrat...	3	Yes		
pwrfail01	Unknown	Gateway...			m00	/SantaA...	Yes		
Lock Gateway 2	Unknown	Lock			Door Lock Gatewa...	/SantaA...	Yes		
EDI Driver	Started	EDI Driv...			Driver Manager loc...	localhost	Yes		
Reader Door 2	Unknown	Reader			Gateway Door 2 R...	/SantaA...	Yes		
Door Lock Gatew...	Unknown	Gateway...			m00	/SantaA...	Yes		
EVO DR1 - REX	Unknown	REX			EVO DR1	2	Yes		
DR Contact Gate...	Unknown	Gateway...			m00	/SantaA...	Yes		
input03	Unknown	Gateway...			m00	/SantaA...	Yes		
Driver Manager l...	Started	Driver M...				localhost	Yes		
Logical Driver	Started	Logical ...			Driver Manager loc...	localhost	Yes		
EVO DR1 - Door ...	Unknown	Door Str...			EVO DR1	1	Yes		
EVO DR1 - Integr...	Unknown	Interfac...	Integrat...		EVO DR1 - Edge	0	Yes		
Historical Events ...	Copying	Historic...			Driver Manager loc...	localhost	Yes		
Gateway 2	Unknown	Gateway...	Cisco Ac...		Access GW Driver	/SantaA...	Yes		
LED Output Gate...	Unknown	Gateway...			m00	/SantaA...	Yes		
EVO DR1 - Door ...	Unknown	Door Co...			EVO DR1	1	Yes		
EVO DR1 - Batter...	Unknown	Input			EVO DR1 - Integrat...	5	Yes		
REX Gateway 2	Unknown	REX			REX Gateway DR 2	/SantaA...	Yes		
tamper01	Unknown	Gateway...			m00	/SantaA...	Yes		
EVO DR1 - A/C ...	Unknown	Input			EVO DR1 - Integrat...	4	Yes		

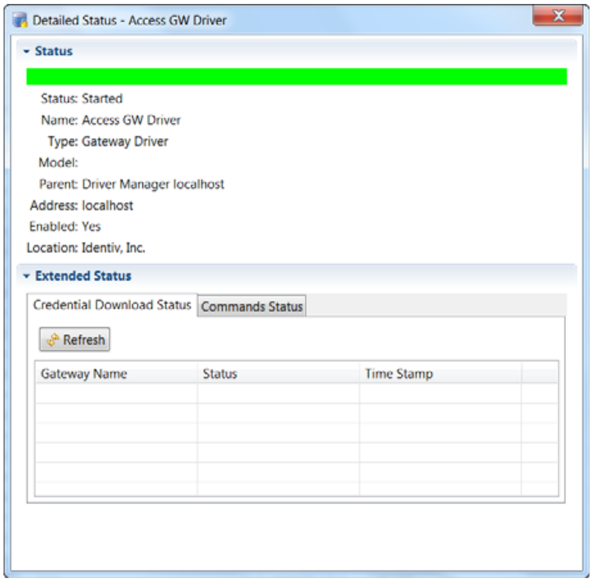
🟥 Alarms: 5 active 36 items cpamadmin - SantaAnaCR

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

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

Step 3 (Optional) Double-click an entry to view additional status details for the device, as shown in Figure 5-7.

Figure 5-7 Device Status: Detail Menu


Detailed Status - Access GW Driver
Status
Extended Status
Credential Download Status
Commands Status
Refresh

Status: Started
Name: Access GW Driver
Type: Gateway Driver
Model:
Parent: Driver Manager localhost
Address: localhost
Enabled: Yes
Location: Identiv, Inc.

Gateway Name	Status	Time Stamp

Step 4 Click the **Extended Status** tabs to view any 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 Tree** or **Door/Location-based Hardware** from the **Doors** menu.

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

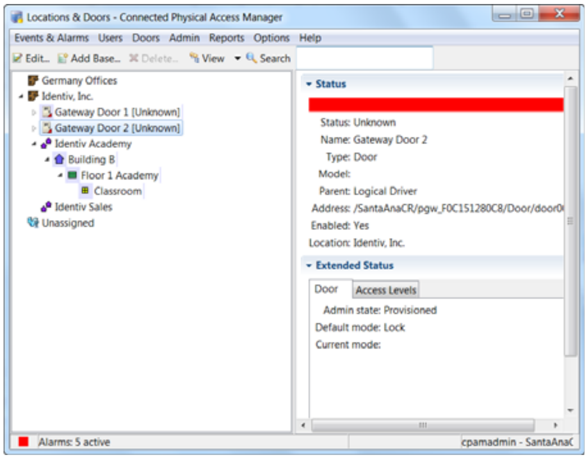
Step 3 Select a door, device, or driver.

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

Tip You can also right click a driver, device or location, and select **View Device Status** from the drop-down menu.

Figure 5-8 shows an example for a door in the Locations & Devices module.

Figure 5-8 Status and Extended Status in the Locations & Devices Module



Germany Offices
Identiv, Inc.
Gateway Door 1 [Unknown]
Gateway Door 2 [Unknown]
Identiv Academy
Building B
Floor 1 Academy
Classroom
Identiv Sales
Unassigned

Status: Unknown
Name: Gateway Door 2
Type: Door
Model:
Parent: Logical Driver
Address: /SantaAnaCR/pgw_F0C151280C8/Door/door0
Enabled: Yes
Location: Identiv, Inc.

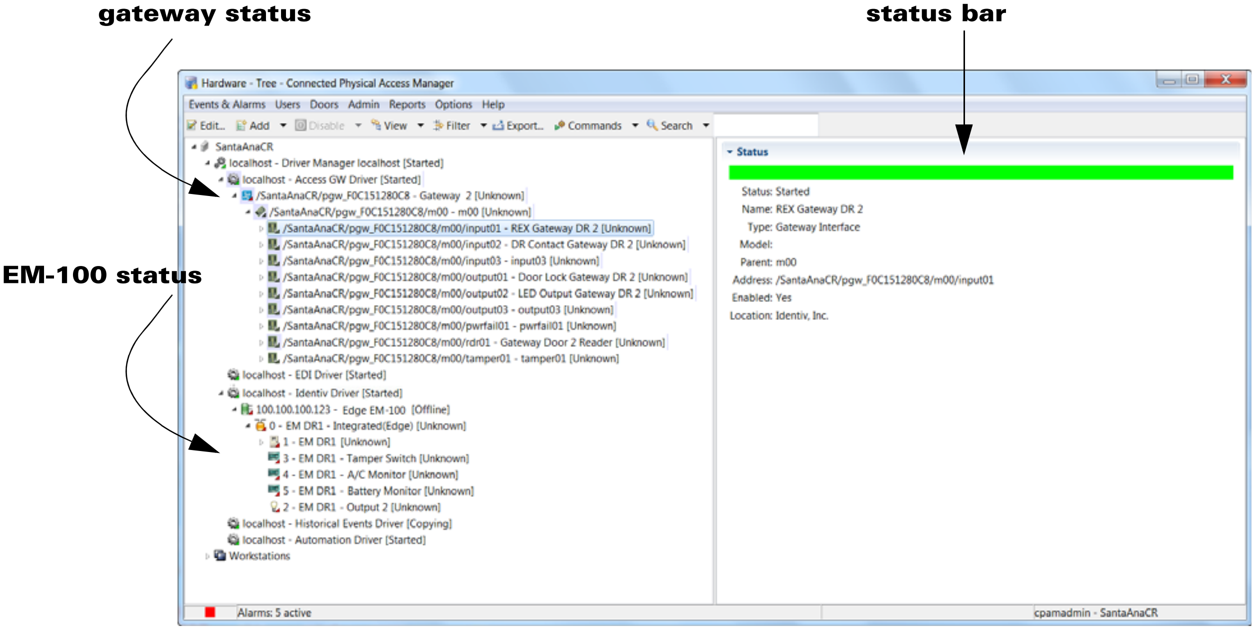
Admin state: Provisioned
Default mode: Lock
Current mode:

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 controller, controller, door, or driver is signified by the color in the icon, and the color bar in the Status field, as shown in Figure 5-9.

Figure 5-9 Device Status Colors



SantaAnaCR
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/SantaAnaCR/pgw_F0C151280C8 - Gateway 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00 - m00 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/input01 - REX Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/input02 - DR Contact Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/input03 - input03 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/output01 - Door Lock Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/output02 - LED Output Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/output03 - output03 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/pwrfail01 - pwrfail01 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/rdr01 - Gateway Door 2 Reader [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/tamper01 - tamper01 [Unknown]
localhost - EDI Driver [Started]
localhost - Identiv Driver [Started]
100.100.100.123 - Edge EM-100 [Offline]
0 - EM DR1 - Integrated(Edge) [Unknown]
1 - EM DR1 [Unknown]
3 - EM DR1 - Tamper Switch [Unknown]
4 - EM DR1 - A/C Monitor [Unknown]
5 - EM DR1 - Battery Monitor [Unknown]
2 - EM DR1 - Output 2 [Unknown]
localhost - Historical Events Driver [Copying]
localhost - Automation Driver [Started]
Workstations

Status: Started
Name: REX Gateway DR 2
Type: Gateway Interface
Model:
Parent: m00
Address: /SantaAnaCR/pgw_F0C151280C8/m00/input01
Enabled: Yes
Location: Identiv, Inc.

	Color	Example	Description
1	Green	🟩	The device is Up and the configuration is current.
2	Dark Green	🟩	(Controllers and gateways only) The controller is Up, but has configuration changes that have not been applied (downloaded). See Applying Configuration Changes to Controllers, page 7-12.
3	Red	🟥	The device is in Down or Unknown state.
4	Green, Dark Green, or Red	🟩	The Status bar color also signifies the device or door status.

Monitoring Device Errors

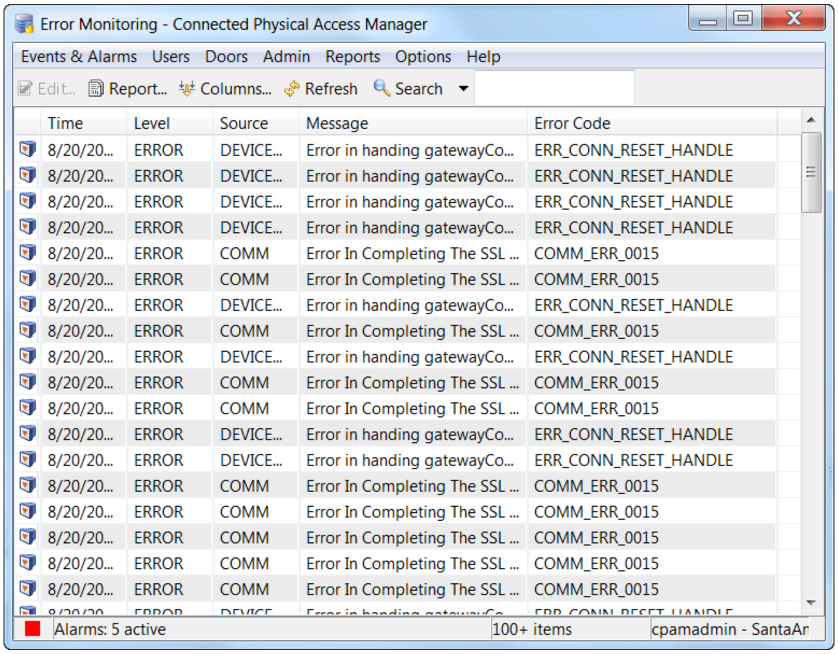
To view a summary of the errors that occurred in the ICPAM system, do the following:

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

The main window displays a summary of the errors for all devices, as shown in Figure 5-10.

By default, the errors are sorted chronologically, most recent first.

Figure 5-10 Error Monitoring: Main Window



Time	Level	Source	Message	Error Code
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE

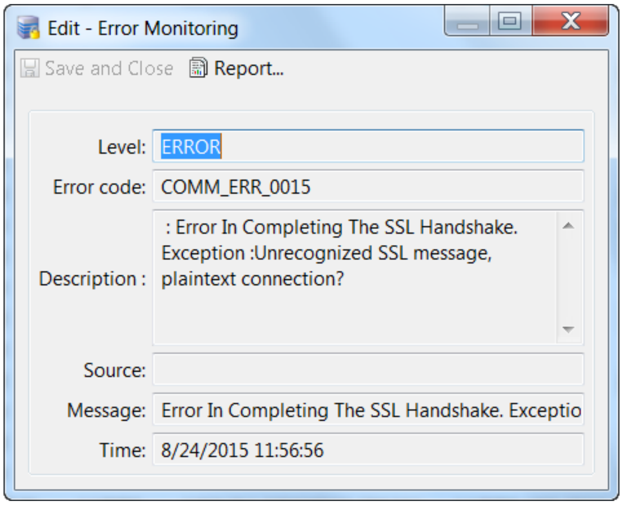
🟥 Alarms: 5 active 100+ items cpamadmin - SantaAr

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

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

Step 3 (Optional) Double-click an entry to view additional status details for the device, as shown in Figure 5-11.

Figure 5-11 Error Monitoring: Detail Menu



Edit - Error Monitoring

Level: ERROR

Error code: COMM_ERR_0015

Description : : Error In Completing The SSL Handshake. Exception :Unrecognized SSL message, plaintext connection?

Source:

Message: Error In Completing The SSL Handshake. Exceptio

Time: 8/24/2015 11:56:56

Viewing the Recent Events for a Device or Driver

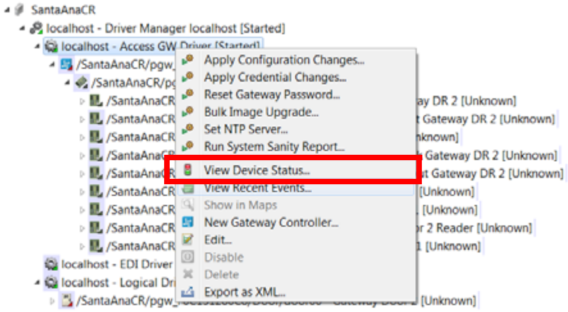
To view a list of recent events for a device or driver, do the following:

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** from the **Doors** menu.

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

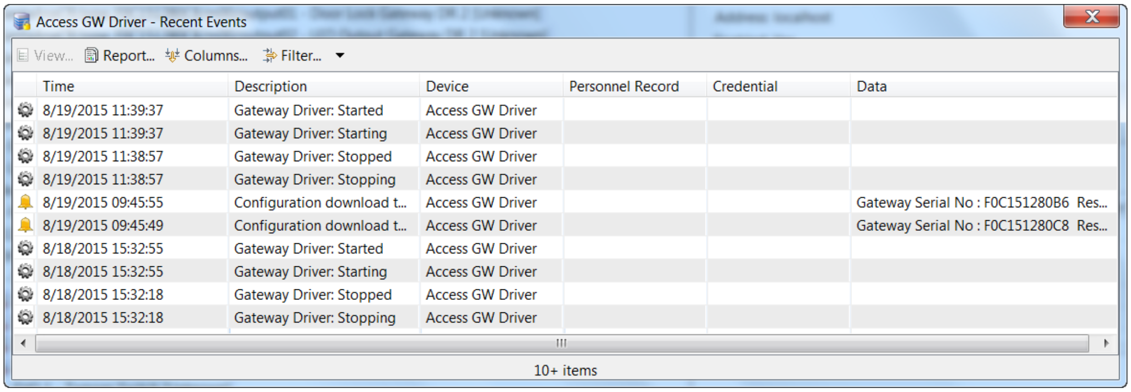
Step 3 Right-click the device or driver, and select **View Recent Events** from the drop-down menu, as shown in Figure 5-12.

Figure 5-12 View Recent Events Menu



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

Figure 5-13 Recent Events



Access GW Driver - Recent Events
View... Report... Columns... Filter...

Time	Description	Device	Personnel Record	Credential	Data
8/19/2015 11:39:37	Gateway Driver: Started	Access GW Driver			
8/19/2015 11:39:37	Gateway Driver: Starting	Access GW Driver			
8/19/2015 11:38:57	Gateway Driver: Stopped	Access GW Driver			
8/19/2015 11:38:57	Gateway Driver: Stopping	Access GW Driver			
8/19/2015 09:45:55	Configuration download t...	Access GW Driver			Gateway Serial No : F0C151280B6 Res...
8/19/2015 09:45:49	Configuration download t...	Access GW Driver			Gateway Serial No : F0C151280C8 Res...
8/18/2015 15:32:55	Gateway Driver: Started	Access GW Driver			
8/18/2015 15:32:55	Gateway Driver: Starting	Access GW Driver			
8/18/2015 15:32:18	Gateway Driver: Stopped	Access GW Driver			
8/18/2015 15:32:18	Gateway Driver: Stopping	Access GW Driver			

10+ items

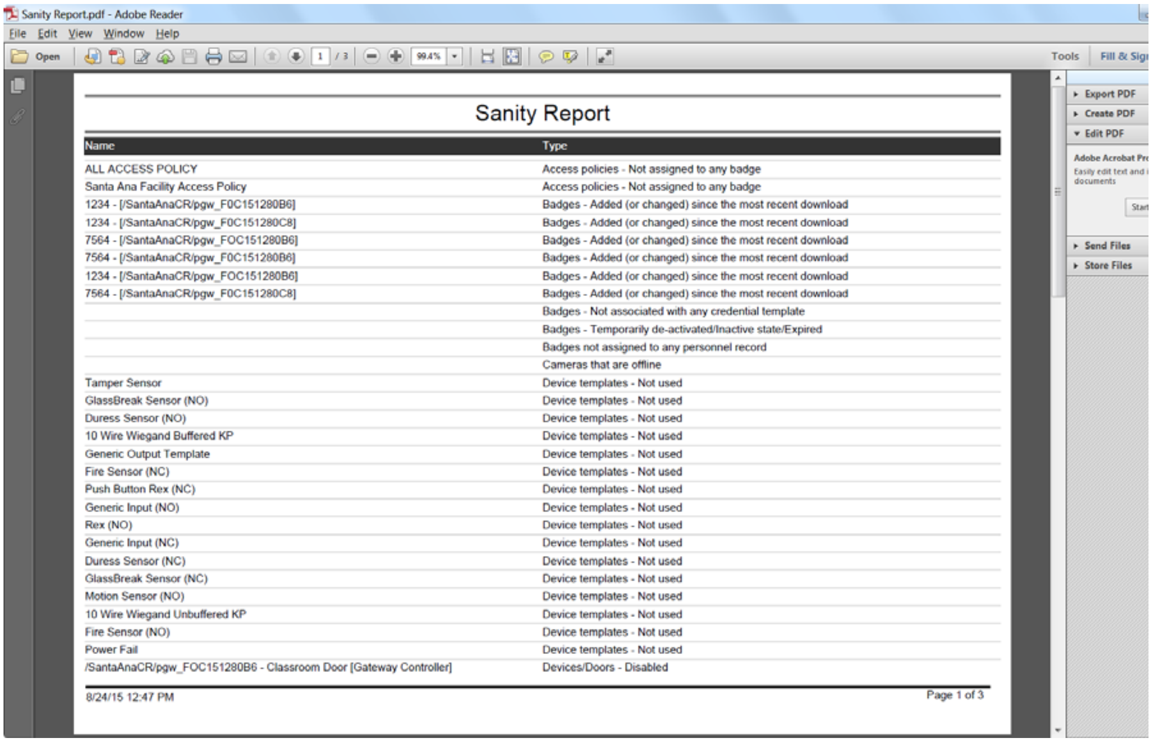
See Viewing Events, Alarms, and Audit Trail Records, page 12-3 for more information.

Generating a Gateway Driver System Sanity Report

System sanity reports provide information about potential system inconsistencies. For example, it includes a summary of doors that are administratively `Down`, devices and doors that are disabled, and other information. Sanity reports can be viewed online, or saved to your computer in a variety of formats.

Figure 5-14 shows a sample report.

Figure 5-14 System Sanity Report Example



Sanity Report

Name	Type
ALL ACCESS POLICY	Access policies - Not assigned to any badge
Santa Ana Facility Access Policy	Access policies - Not assigned to any badge
1234 - [/SantaAnaCR/pgw_F0C151280B6]	Badges - Added (or changed) since the most recent download
1234 - [/SantaAnaCR/pgw_F0C151280C8]	Badges - Added (or changed) since the most recent download
7564 - [/SantaAnaCR/pgw_FOC151280B6]	Badges - Added (or changed) since the most recent download
7564 - [/SantaAnaCR/pgw_F0C151280B6]	Badges - Added (or changed) since the most recent download
1234 - [/SantaAnaCR/pgw_FOC151280B6]	Badges - Added (or changed) since the most recent download
7564 - [/SantaAnaCR/pgw_F0C151280C8]	Badges - Added (or changed) since the most recent download
	Badges - Not associated with any credential template
	Badges - Temporarily de-activated/Inactive state/Expired
	Badges not assigned to any personnel record
	Cameras that are offline
Tamper Sensor	Device templates - Not used
GlassBreak Sensor (NO)	Device templates - Not used
Duress Sensor (NO)	Device templates - Not used
10 Wire Wiegand Buffered KP	Device templates - Not used
Generic Output Template	Device templates - Not used
Fire Sensor (NC)	Device templates - Not used
Push Button Rex (NC)	Device templates - Not used
Generic Input (NO)	Device templates - Not used
Rex (NO)	Device templates - Not used
Generic Input (NC)	Device templates - Not used
Duress Sensor (NC)	Device templates - Not used
GlassBreak Sensor (NC)	Device templates - Not used
Motion Sensor (NO)	Device templates - Not used
10 Wire Wiegand Unbuffered KP	Device templates - Not used
Fire Sensor (NO)	Device templates - Not used
Power Fail	Device templates - Not used
/SantaAnaCR/pgw_FOC151280B6 - Classroom Door [Gateway Controller]	Devices/Doors - Disabled

8/24/15 12:47 PM Page 1 of 3

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

Sanity reports include the following topics:

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

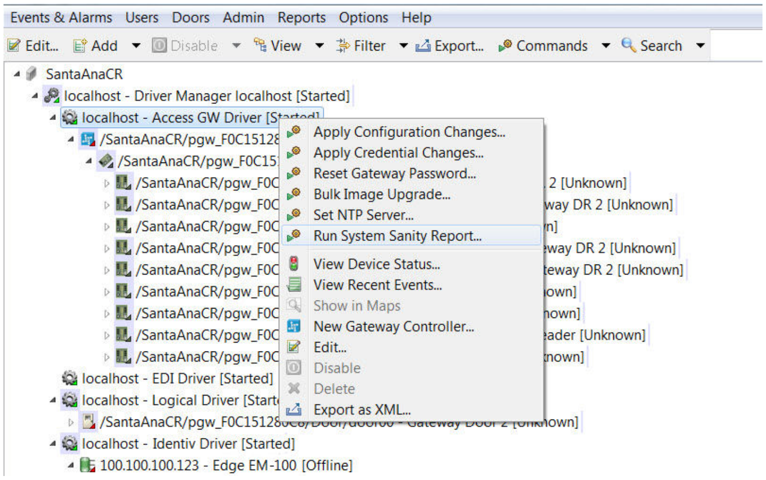
Procedure

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

Step 1 Select Hardware Tree from the Doors menu.

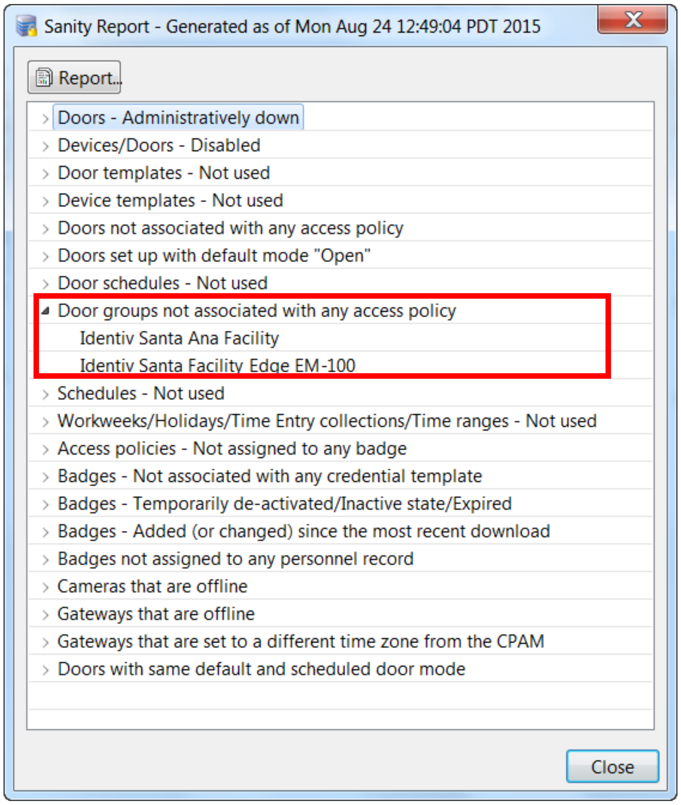
Step 2 Right-click the **Access GW Driver** and select **Run System Sanity Report**, as shown in Figure 5-15.

Figure 5-15 System Sanity Report Command


Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Disable View Filter Export... Commands Search
SantaAnaCR
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/SantaAnaCR/pgw_F0C15128
/SantaAnaCR/pgw_F0C15
/SantaAnaCR/pgw_F0C
2 [Unknown]
way DR 2 [Unknown]
n]
way DR 2 [Unknown]
teway DR 2 [Unknown]
own]
nown]
ader [Unknown]
nown]
localhost - EDI Driver [Started]
localhost - Logical Driver [Start
/SantaAnaCR/pgw_F0C15128
Gateway Door 2 [Unknown]
localhost - Identiv Driver [Started]
100.100.100.123 - Edge EM-100 [Offline]
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Set NTP Server...
Run System Sanity Report...
View Device Status...
View Recent Events...
Show in Maps
New Gateway Controller...
Edit...
Disable
Delete
Export as XML...

Step 3 In the Sanity Report window, expand the menu for a topic, as shown in Figure 5-16.

Figure 5-16 System Sanity Report Window


Sanity Report - Generated as of Mon Aug 24 12:49:04 PDT 2015

Report...

- Doors - Administratively down
- Devices/Doors - Disabled
- Door templates - Not used
- Device templates - Not used
- Doors not associated with any access policy
- Doors set up with default mode "Open"
- Door schedules - Not used
- Door groups not associated with any access policy
  - Identiv Santa Ana Facility
  - Identiv Santa Facility Edge EM-100
- Schedules - Not used
- Workweeks/Holidays/Time Entry collections/Time ranges - Not used
- Access policies - Not assigned to any badge
- Badges - Not associated with any credential template
- Badges - Temporarily de-activated/Inactive state/Expired
- Badges - Added (or changed) since the most recent download
- Badges 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 CPAM
- Doors with same default and scheduled door mode

Close

In Figure 5-16, the topic `Door groups not associated with any access policy` is expanded to show that the `Lobby Door Group` is not associated with any access policy.

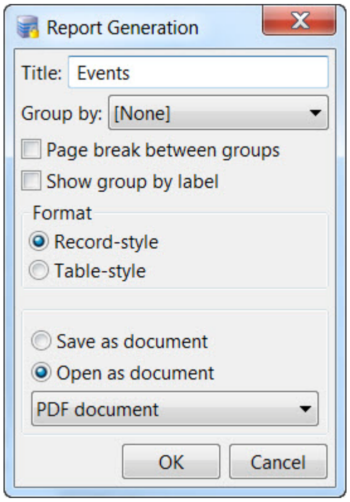
Note If a topic does not display any information when expanded, then no criteria meets that condition.

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

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

b. In the Report Generation window (Figure 5-17), select the **Format** for the report.

Figure 5-17 System Sanity Report Settings



Title: Events

Group by: [None]

□ Page break between groups

□ Show group by label

Format

● Record-style

○ Table-style

○ Save as document

● Open as document

PDF document

c. Select the report output.

- **Open in report**
- **Save as document**
- **Open as document**

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

e. Click **OK**.

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

Note A sample sanity report is shown in Figure 5-14 on page 5-16.

Understanding Door Configurations and Templates

This section includes the following information

Overview

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, ICPAM supports door and device templates. Templates enable 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 controller.

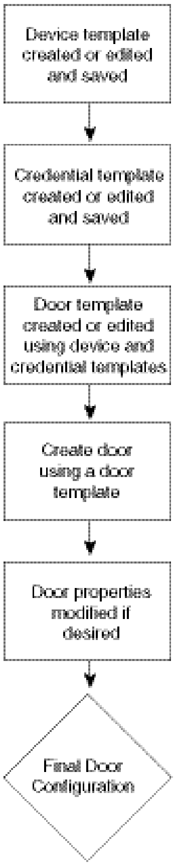
Since a door configuration references a door template, all template settings or changes to those settings are reflected by the door. You can easily override most template settings for a single door by deselecting the Default check box next to each field and entering a custom value. The current door setting 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, and records). With ICPAM you create 10 different door templates instead of 500 individual door configurations. You also have full flexibility to change settings for a single door, or groups of doors.

Sequence for Configuring Templates and Doors

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

Figure 5-18 Sequence for Configuring Templates and Doors


Device template created or edited and saved
Credential template created or edited and saved
Door template created or edited using device and credential templates
Create door using a door template
Door properties modified if desired
Final Door Configuration

Tip See also Installation and Configuration Summary, page 1-3.

Door Configurations and Templates

Door configurations are sets of device hardware assigned to a controller. 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. There are two types of REX buttons:
  - Push button REX: this button is used to trigger the system to directly unlock the lock associated with the door. For example, a Push Button REX fixed on a door latch is pressed to trigger the lock to open the door.

    - Non-push button REX: A Non-Push Button REX has no effect on the lock associated with the door. For example, when a push bar on the door is pressed it retracts the door latch causing the door to open.

- **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 controller. Door templates contain pre-defined device configurations.

- Adding New Doors, page 7-2: this method uses a step-by-step script that prompts you to add a controller 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 7-2: using this method, the controller must already be entered in the system, usually after a Discovered Configuration, or when adding an additional door configuration to an existing controller.

Template Types

There are six 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 controller such as the time zone, support for one or two doors, the attached expansion modules, and the door templates assigned to the controller. Changes to a gateway template do not impact configured controllers (only new controller configurations).
- Controller Templates: define the basic attributes of the Identiv EM-100 controller, such as time zone, support for doors, and door templates assigned to the controller.
- Understanding Door Templates: define a set of door hardware devices and settings. Door templates are assigned to controllers to simplify door configuration. Door templates also reference device templates (see below) to simplify device configuration.

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

- Understanding Device Templates: define typical settings for devices, such as locks and sensors. Device templates are used to help define door templates.
- Understanding Gateway 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 9-22. 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 controllers. Only new controller 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.

Tip The names of all hardware elements are editable, including drivers, controllers, expansion modules, and door devices.

- 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 without Templates, page 6-2

Gateway templates are used when configuring a new controller in the Hardware Tree module. For instructions to use gateway templates, see Configuring Gateways Using Existing Templates, page 6-7.

Tip To create an exact copy of a gateway configuration for a single controller, see Cloning a Gateway Configuration, page 6-33.

Controller Templates

Identiv EM-100 controller templates enable the system configurator to pre-define the door and device attributes to include in a new controller. To create a controller template, save the template from a previously configured device, as described in Creating Custom EM-100 Controller Configurations without Templates, page 6-15.

Controller templates are used when configuring a new controller in the Hardware Tree module. For instructions on how to use controller templates, see Configuring EM-100 Controllers Using Existing Templates, page 6-17.

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 controller using one of the following methods:

- Configuring Gateways Using Existing Templates, page 6-7

- Adding Doors Using Door Templates, page 7-2

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

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

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

To create and modify door templates, see Chapter 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 controller 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 ICPAM 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.

Related Documentation

- Chapter 6, "Configuring Controllers"
- Chapter 7, "Configuring Doors"
- Chapter 8, "Configuring Door and Device Templates"

Understanding Virtual 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. Virtual Credential Templates specify the card data format for a reader, and are used to configure reader device templates.

Note The virtual credential template can be used for either gateway credentials or Identiv EM-100 controller credentials.

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 Creating a Virtual Credential Template, page 8-17 for more information.

Understanding Gateway Credential Templates

Gateway Credential Templates specify the card data format for a reader connected to a gateway, and are used to configure reader device templates associated with that reader.

Note The gateway credential template is used for gateway credentials only. If this template is for both gateway and controller use, use the Virtual Credential Template instead.

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 Creating a Gateway Credential Template, page 8-15 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 Tree module, or to door templates. See Configuring Reader LED Profiles, page 8-21 for more information.

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

- Configuring the Default and Scheduled Door Modes, page 5-33

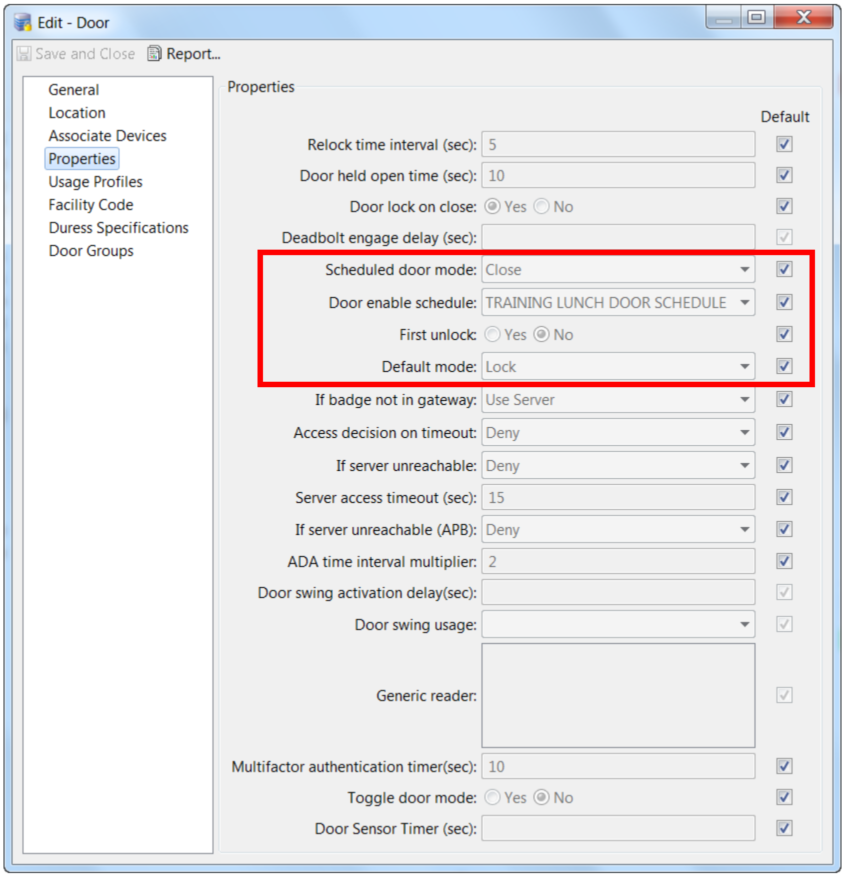
Overview

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

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

To configure door modes and door schedules, use the door Properties window shown in Figure 5-19.

Figure 5-19 Door Properties Window



		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

The door Properties window includes the following four fields:

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

- The **Door enable schedule**: specifies a door schedule for the times and days when a different door mode is applied. If you select a schedule, the schedule will override the default mode for the times and days defined in the schedule. See Understanding the Scheduled Door Mode, page 5-28.
- **Scheduled door mode**: the mode used when the door scheduled is applied.
- **First unlock**. determines if the schedule is activated only after the first successful badge swipe. The door remains in default mode until a badge is used to access the door, even after the beginning time for the schedule. See Understanding First Unlock Impact on the Scheduled Mode, page 5-29

Tip See Configuring the Default and Scheduled Door Modes, page 5-33 to create a schedule and apply it to a door. See also Step 6 in Configuring Door Templates, page 8-2.

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 dead bolt is applied.

The *Default* mode defines the door mode at all times unless overridden by a door schedule or door mode command. See Understanding the Default Door Mode, page 5-28.

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

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

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

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

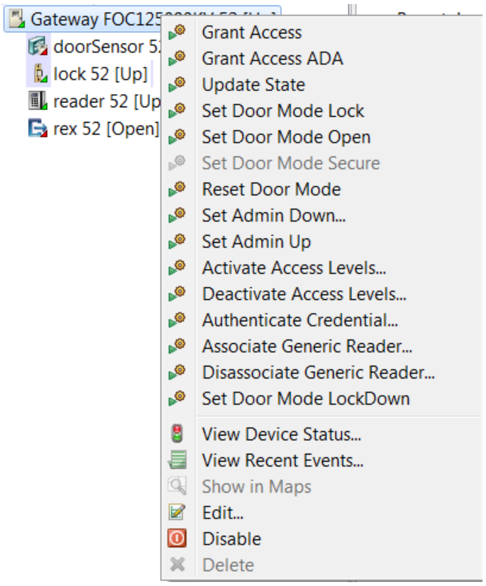
Viewing the Door Mode Status

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

Figure 5-20 also shows the door mode commands used to override the Current and Default mode. In this example, if the user selects the command **Set Door Mode Lock**, the door will stay in Lock mode until another door mode command is selected, or the controller is reset. For more information, see Manually

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

Figure 5-20 Door Mode Commands and Status



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 5-33 for instructions to create a schedule and apply it to a door.

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

To override a door schedule, see Manually Override the Door Mode Using Commands, page 5-29.

Understanding First Unlock Impact on the Scheduled Mode

First Unlock ensures that the door schedule (and associated mode) is activated only if a user successfully swipes a badge to access the door. This is useful in situations such as a snow day, when employees may not be able to reach work. The door is not automatically unlocked unless a badge holder is physically present. When the door is accessed with a valid badge, the door schedule is activated and the Scheduled Door Mode is applied. See Configuring the Default and Scheduled Door Modes, page 5-33 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 controller is reset, or after a power failure to the controller.

Applying First Unlock

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

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

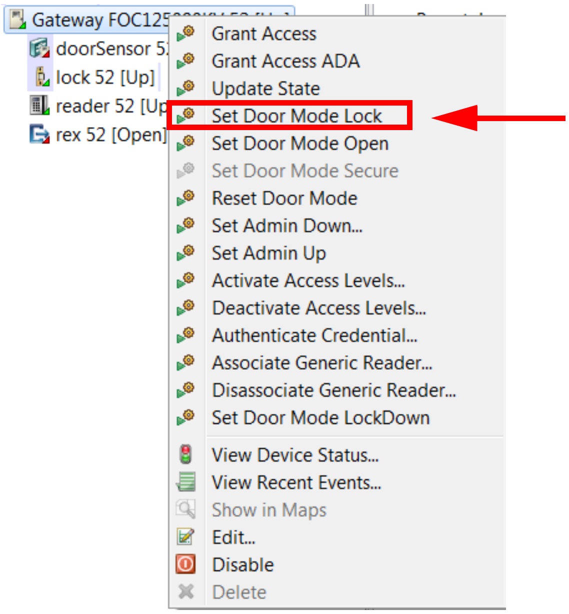
- Manually Override the Door Mode Using Commands, page 5-29
- Impact of Controller Reset on the Default and Scheduled Modes, page 5-31

Manually Override the Door Mode Using Commands

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

For example, in Figure 5-21 the current mode is Close (Scheduled). Right click the door and select **Set Door Mode Lock**. The current mode is changed to Lock (Override), as shown in Figure 5-22 on page 5-31.When a door in the override mode door schedules do not take affect, the door will remain in the manually assigned mode and will not resume scheduled operations until the door mode is manually reset.

Figure 5-21 Selecting a Door Mode Command

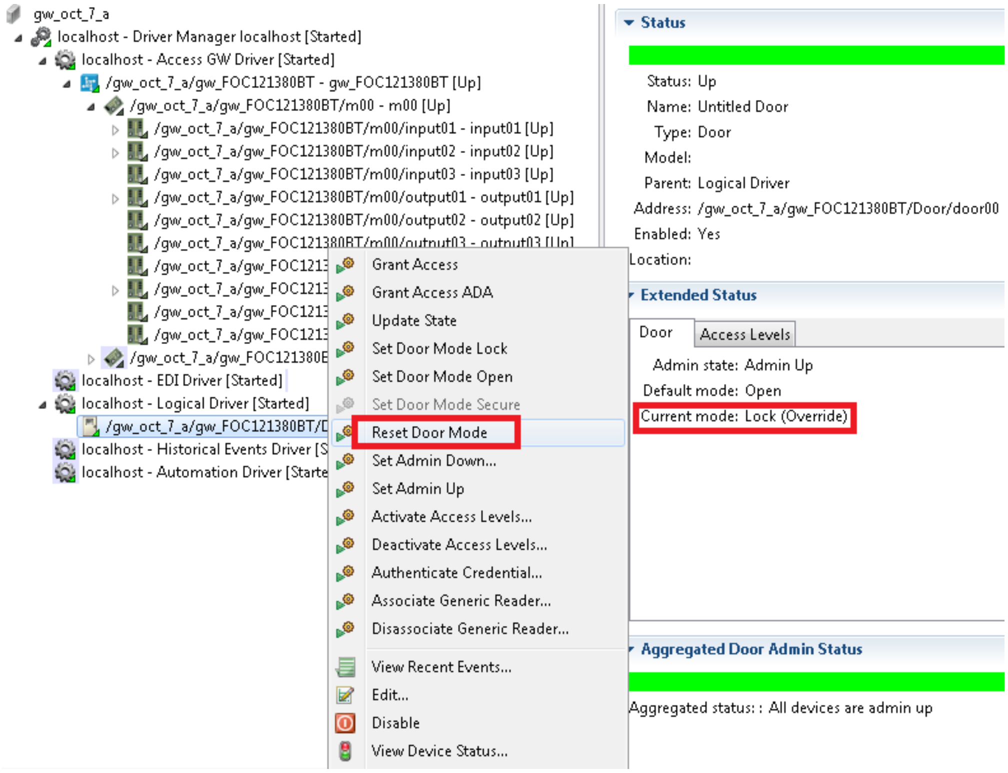


The current mode remains Lock (Override) until you do one of the following:

- 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 controller, as described in Impact of Controller Reset on the Default and Scheduled Modes, page 5-31. Resetting the controller has the same affect as the **Reset Door Mode** command.

For example, in Figure 5-22 the current door mode is Lock (Override). The door stays in the override mode until you select another door mode or reset the controller. 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.

Figure 5-22 Reset Door Modes Command


gw_oct_7_a
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/gw_oct_7_a/gw_FOC121380BT - gw_FOC121380BT [Up]
/gw_oct_7_a/gw_FOC121380BT/m00 - m00 [Up]
/gw_oct_7_a/gw_FOC121380BT/m00/input01 - input01 [Up]
/gw_oct_7_a/gw_FOC121380BT/m00/input02 - input02 [Up]
/gw_oct_7_a/gw_FOC121380BT/m00/input03 - input03 [Up]
/gw_oct_7_a/gw_FOC121380BT/m00/output01 - output01 [Up]
/gw_oct_7_a/gw_FOC121380BT/m00/output02 - output02 [Up]
/gw_oct_7_a/gw_FOC121380BT/m00/output03 - output03 [Up]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
/gw_oct_7_a/gw_FOC121380BT/D
localhost - Historical Events Driver [S
localhost - Automation Driver [Starte
Grant Access
Grant Access ADA
Update State
Set Door Mode Lock
Set Door Mode Open
Set Door Mode Secure
Reset Door Mode
Set Admin Down...
Set Admin Up
Activate Access Levels...
Deactivate Access Levels...
Authenticate Credential...
Associate Generic Reader...
Disassociate Generic Reader...
View Recent Events...
Edit...
Disable
View Device Status...
Status
Extended Status
Door
Access Levels
Aggregated Door Admin Status

Status: Up
Name: Untitled Door
Type: Door
Model:
Parent: Logical Driver
Address: /gw_oct_7_a/gw_FOC121380BT/Door/door00
Enabled: Yes
Location:

Admin state: Admin Up
Default mode: Open
Current mode: Lock (Override)

Aggregated status: : All devices are admin up

Impact of Controller Reset on the Default and Scheduled Modes

When a controller 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 controller is reset using the **Reset Gateway** command, or when the controller 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 controller goes off and comes back on at 9 am (during the scheduled mode), the controller is reset. Since First Unlock is configured, and the door returns to the default state (Lock) until a badge is swiped to reactive the scheduled door mode (Close).

Example 2

- The default door mode is **Lock** (physically closed and locked).
- The scheduled door mode from 8 am to 5 pm is **Close** (physically closed and unlocked).

- At 3 pm, the guard manually sets the door to Lock mode and goes to break (see Manually Override the Door Mode Using Commands, page 5-29).
- First Unlock is set to **No**.

While the guard is away, another use invokes the Reset Gateway command in ICPAM. Since the First Unlock feature is not configured, the scheduled mode is immediately applied and the door is placed in **Close** (physically closed and unlocked). The door is now unlocked even though the guard is absent.

Understanding Door Schedule Entries in ICPAM 2.1

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
- 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 ICPAM. 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 controller 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 ICPAM 2.1 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.

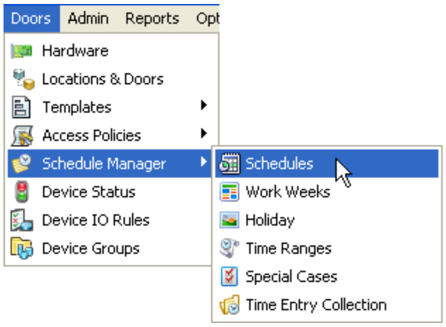
Since this location occasionally suffers snow storms that close roads and delay traffic, we want to keep the door locked in the morning until the receptionist (or another employee) arrives and accesses the door with a badge, even if they arrive after the scheduled unlock time of 8 am. (the door should 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 11-9.

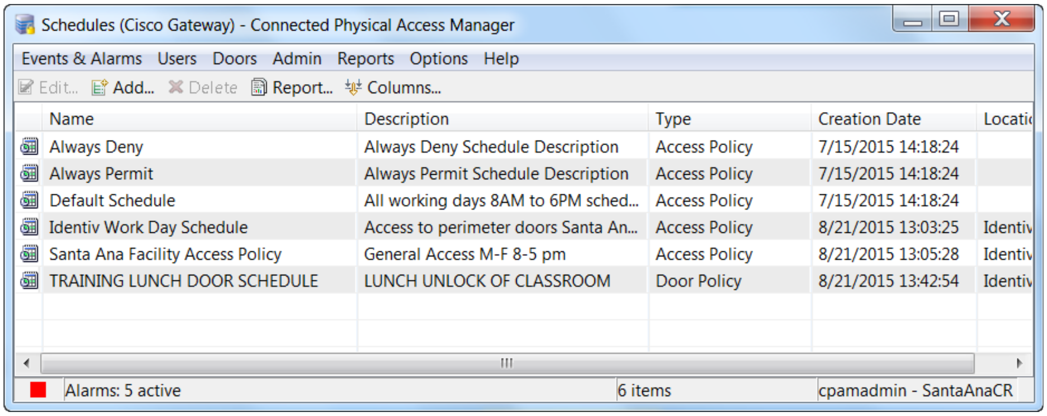
Step 1 Create a schedule for the door.

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

a. Select **Schedules** from the **Schedule Manager** submenu under the **Doors** menu.



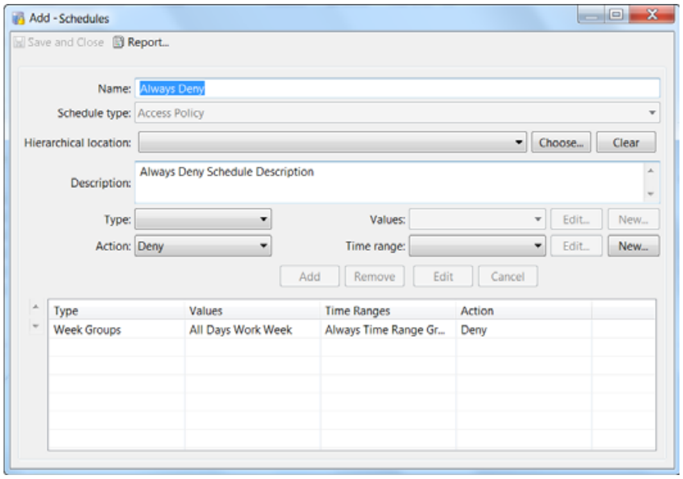
The Schedules list appears like this example:



Name	Description	Type	Creation Date	Locati
Always Deny	Always Deny Schedule Description	Access Policy	7/15/2015 14:18:24	
Always Permit	Always Permit Schedule Description	Access Policy	7/15/2015 14:18:24	
Default Schedule	All working days 8AM to 6PM sched...	Access Policy	7/15/2015 14:18:24	
Identiv Work Day Schedule	Access to perimeter doors Santa An...	Access Policy	8/21/2015 13:03:25	Identiv
Santa Ana Facility Access Policy	General Access M-F 8-5 pm	Access Policy	8/21/2015 13:05:28	Identiv
TRAINING LUNCH DOOR SCHEDULE	LUNCH UNLOCK OF CLASSROOM	Door Policy	8/21/2015 13:42:54	Identiv

Alarms: 5 active 6 items cpamadmin - SantaAnaCR

b. Click **Add...**



Name: Always Deny
Schedule type: Access Policy
Hierarchical location:
Description: Always Deny Schedule Description
Type:
Values:
Action: Deny
Time range:

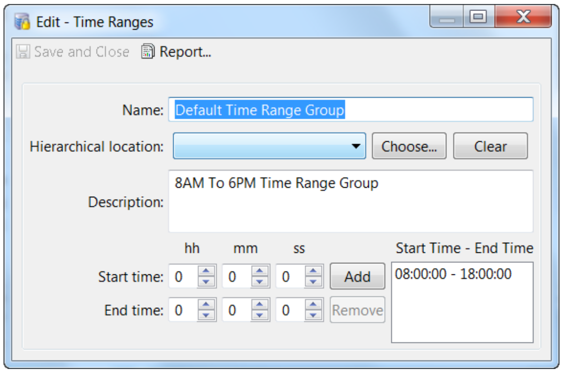
Type	Values	Time Ranges	Action
Week Groups	All Days Work Week	Always Time Range Gr...	Deny

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**. Create a custom **Time Range** for the schedule (for example: “8-5, minus lunch”):



Name: Default Time Range Group
Hierarchical location:
Description: 8AM To 6PM Time Range Group

	hh	mm	ss
Start time:	0	0	0
End time:	0	0	0

Start Time - End Time
08:00:00 - 18:00:00

- 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**.

g. In the Add Schedule window, select the new range (**8-5, minus lunch**) from the **Time Range** menu.

h. Click **Add** to add the schedule to the list.

i. Click **Save and Close** to create the door schedule. The door schedule appears in the Schedules window.

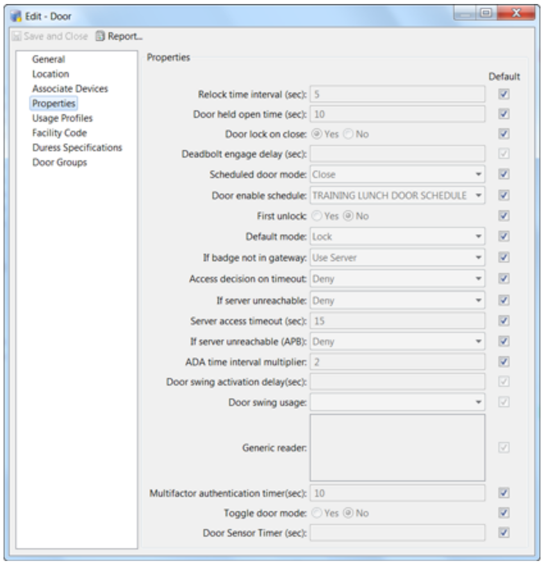
Tip The schedule is not active until you apply it to a door, as described in the following steps.

Step 2 Open the door configuration Properties window.

a. Select **Hardware Tree** or **Door/Location-based Hardware** from the **Doors** menu.

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

c. Select **Properties**.



Properties

		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

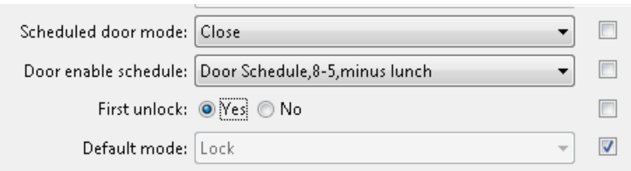
Tip To create or modify a door template with these settings, select **Door Templates** from the Doors menu, in the Templates submenu. See Configuring Door Templates, page 8-2.

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.



Scheduled door mode:	Close	☐
Door enable schedule:	Door Schedule,8-5,minus lunch	☐
First unlock:	● Yes ○ No	☐
Default mode:	Lock	☑

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

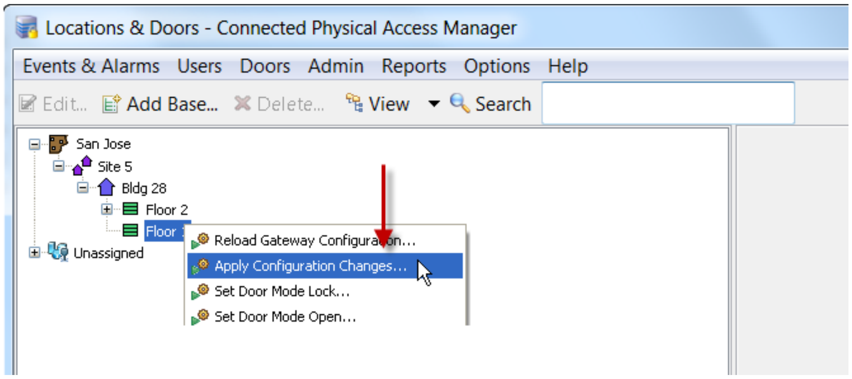
c. For **Scheduled door mode**, select **Close**. The door is physically closed during the door schedule hours, but the lock is not applied.

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.

Step 4 Apply the door configuration changes.

Right-click a location or controller and select **Apply Configuration Changes**.


Locations & Doors - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
San Jose
Site 5
Bldg 28
Floor 2
Floor 1
Unassigned
Reload Gateway Configuration...
Apply Configuration Changes...
Set Door Mode Lock...
Set Door Mode Open...

Note Controllers 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 Controller and Expansion Module Serial Numbers
- Displaying the ICPAM Appliance Serial Number

Locating Controller and Expansion Module Serial Numbers

Serial numbers for the controller and other expansion modules are available at the following locations:

- Printed on the back label of the module case.
- Listed in the **Show Inventory** screen of the controller administration tool (direct PC connection). See *Cisco Physical Access Gateway User Guide* for more information.
- Listed in the ICPAM Controller properties. Open the Hardware Tree module device view, right-click on the module, select **Edit** and then **Properties**.

Displaying the ICPAM Appliance Serial Number

To view the appliance serial number, do the following:

Step 1 Log on to the ICPAM Server Administration utility:

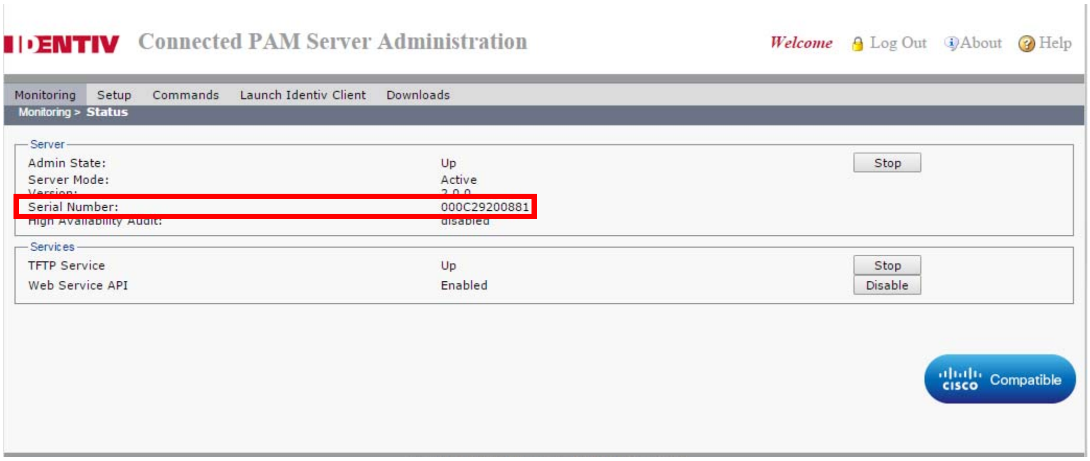
- For a direct connection, see Configuring ICPAM on Virtual Machine (VM), page 2-16.
- For an Internet connection, open a web browser and enter the IP address used for the ICPAM Server Administration utility. See Logging on to the ICPAM Server Administration Utility, page 2-2, or ask your system administrator for assistance.

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

Step 2 Select the Monitoring tab, and then select Status, as shown in Figure 5-23.

Step 3 Refer to the entry for Serial Number.

Figure 5-23 ICPAM Appliance Serial Number



Admin State: Up
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

TFTP Service Up
Web Service API Enabled

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 6

Configuring Controllers

This chapter provides instructions on how to add and modify controller configurations. In addition, it details how to clone, replace, and delete controllers as well as change gateway passwords and modify driver 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 Controller Configurations, page 5-1 for more information.

Contents

Configuring New Controllers

You can add a new controller in one of two ways:

- Creating Custom Gateway Configurations without Templates, page 6-2
- Configuring Gateways Using Existing Templates, page 6-7
- Creating Custom EM-100 Controller Configurations without Templates, page 6-15
- Configuring EM-100 Controllers Using Existing Templates, page 6-17

Each is explained in this section.

Creating Custom Gateway Configurations without Templates

To create a door, a gateway configuration must first be created that defines the modules and devices attached to the gateway. There are essentially two ways of doing this:

- Create a gateway from scratch
- Create a gateway using an existing gateway template

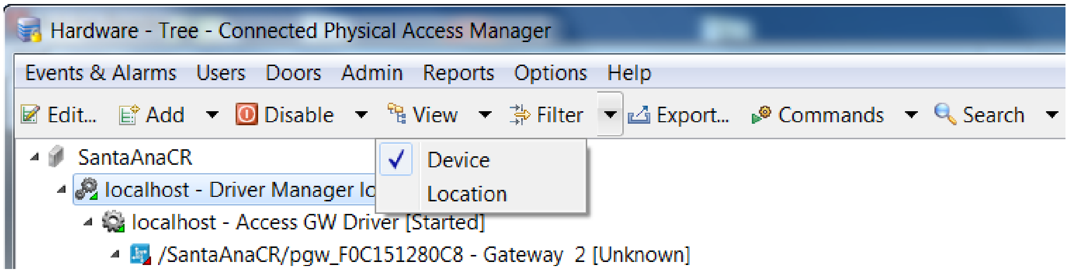
Procedure

Complete the following instructions to create a custom gateway configuration without using an existing gateway template, and then save it as a template. You can also clone the configuration for use with another gateway.

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

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

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

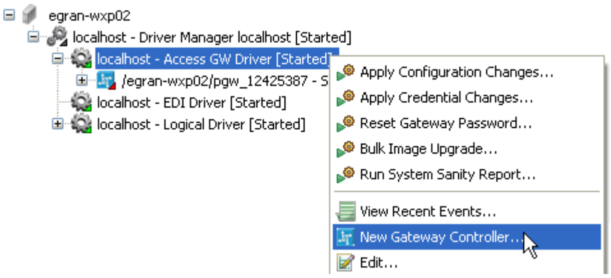

Hardware - Tree - Connected Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Edit...
Add
Disable
View
Filter
Export...
Commands
Search
SantaAnaCR
localhost - Driver Manager lo
localhost - Access GW Driver [Started]
/SantaAnaCR/pgw_F0C151280C8 - Gateway 2 [Unknown]
✓ Device
Location

Tip See also Viewing Doors and Devices in the Hardware Tree View, page 5-4.

Step 2 Add a controller.

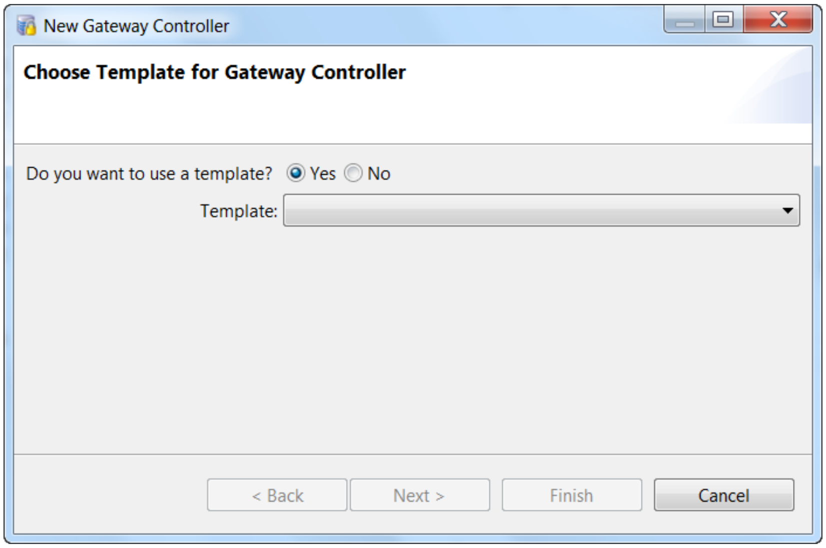
a. Right-click the selected Access GW Driver.

b. From the drop-down list, select **New Gateway Controller**.


egran-wxp02
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/egran-wxp02/pgw_12425387 - S
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Run System Sanity Report...
View Recent Events...
New Gateway Controller...
Edit...

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

Click **Next** to continue.



New Gateway Controller

Choose Template for Gateway Controller

Do you want to use a template? ● Yes ○ No

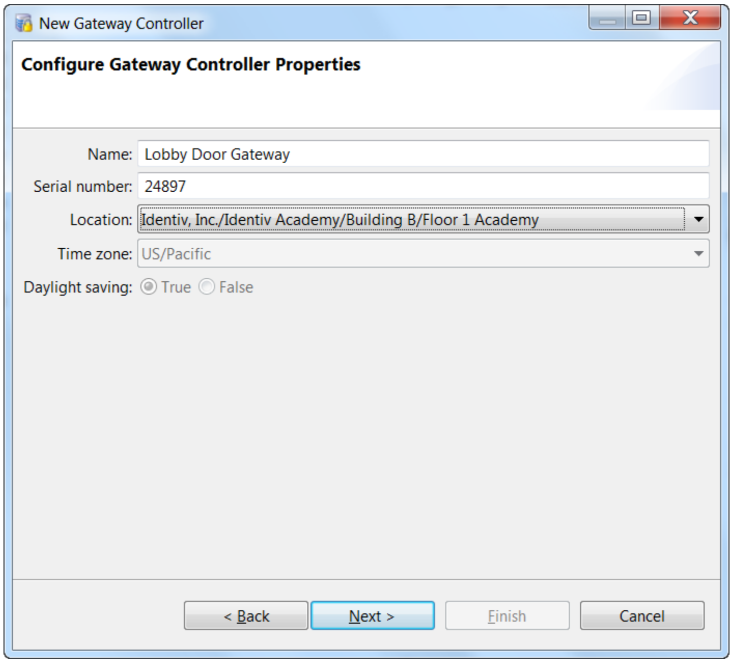
Template:

Step 4 Enter the basic gateway properties.

- **a.** **Name**: enter a descriptive name to identify the controller.
- **b.** **Serial Number**: enter the serial number. See Locating Serial Numbers, page 5-37.
- **c.** **Location**: the assigned location of the module. See Creating the Location Map, page 5-8.
- **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.



Name: Lobby Door Gateway

Serial number: 24897

Location: Identiv, Inc./Identiv Academy/Building B/Floor 1 Academy

Time zone: US/Pacific

Daylight saving: ● True ○ False

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 controller.

a. **Serial Number**: enter the serial number. See Locating Serial Numbers, page 5-37.

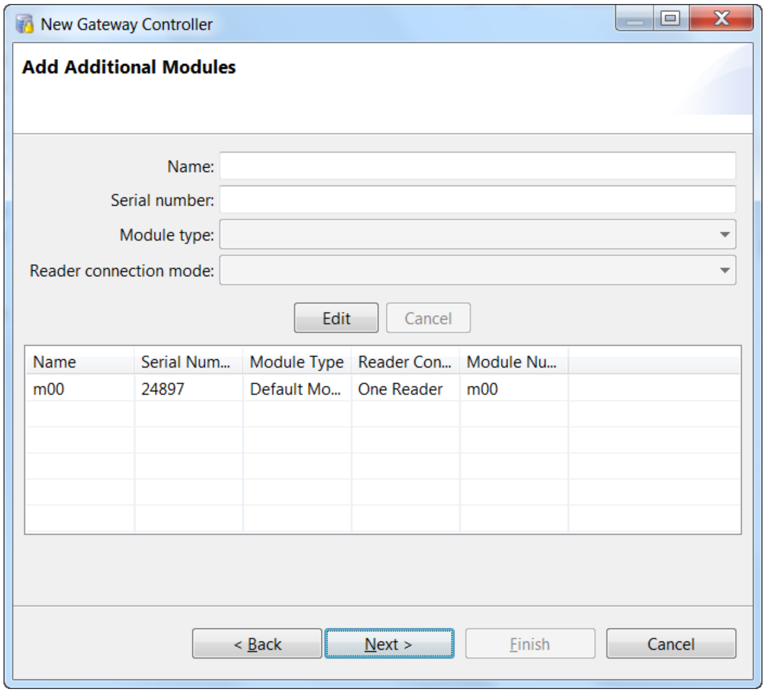
b. **Module Type**: select Reader, Input, or Output.

c. **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.



Add Additional Modules

Name	Serial Num...	Module Type	Reader Con...	Module Nu...
m00	24897	Default Mo...	One Reader	m00

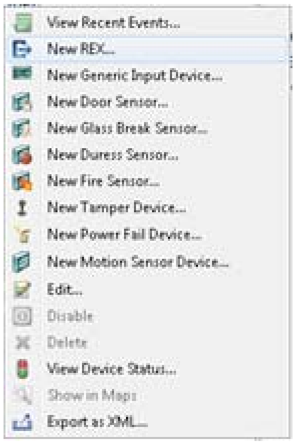
Tip To modify the module list, select a module and click **Edit** or **Remove**.

Step 6 (Optional) Add devices to the gateway or expansion module interfaces.

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

a. Expand the hardware tree to view the gateway or expansion module interfaces.

b. Right-click an interface and select a device for the interface. For example: **New REX**.



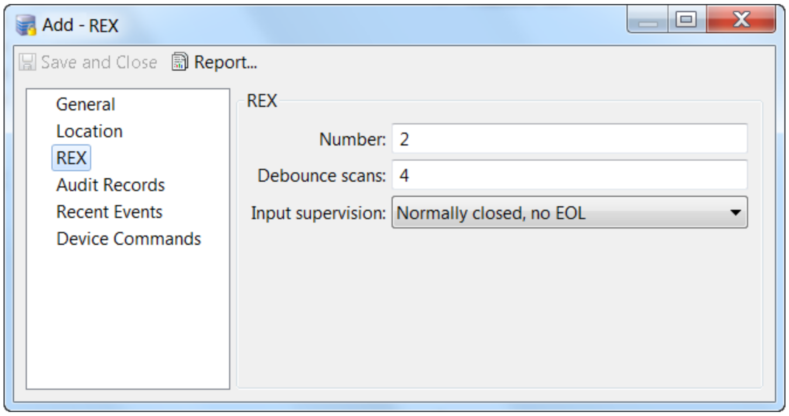
c. In the device window, select **REX** and enter the device settings.

– Select a **Template name** to populate the fields.

– To override the template settings, deselect the **Default** check box next to each field.

- To restore the default template setting, re-select the **Default** check box.
- In the REX tab, enter the **Debounce Timer(ms)** value.

d. Click **Save and Close**.



Number: 2

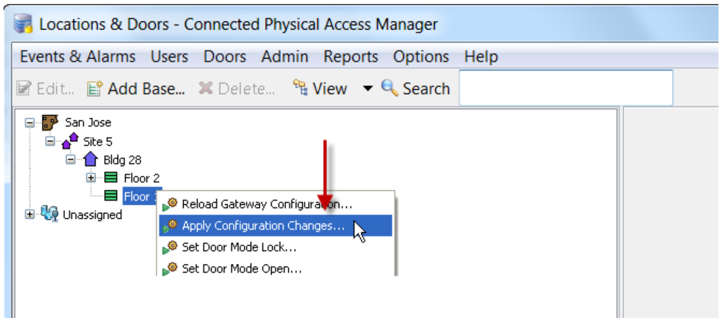
Debounce scans: 4

Input supervision: Normally closed, no EOL

e. Repeat these steps for each device connected to the gateway.

Step 7 Apply the configuration changes to download the new settings to the devices.

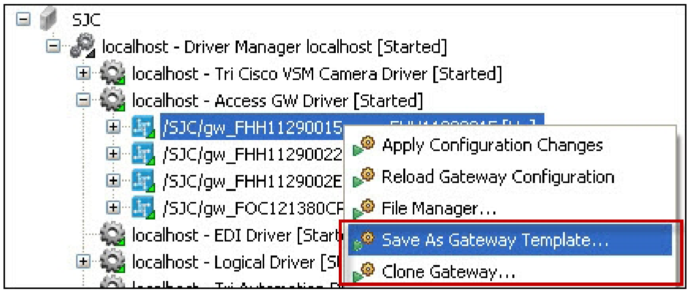
- To update all gateways: right-click the required Access GW Driver and select **Apply Configuration Changes**.
- To update a single gateway: right-click the gateway and select **Apply Configuration Changes**.



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 7-12.

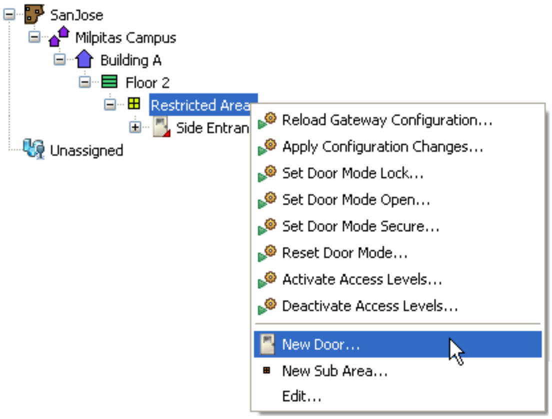
Step 8 (Optional) Create a gateway template from the new configuration.

- Right-click on the required 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 6-2).


SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [Started]
localhost - Access GW Driver [Started]
/SJC/gw_FHH11290015
/SJC/gw_FHH11290022
/SJC/gw_FHH1129002E
/SJC/gw_FOC121380CF
localhost - EDI Driver [Start
localhost - Logical Driver [St
Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
Clone Gateway...

- Select **Clone Gateway** to create an exact copy of a gateway configuration for a single gateway. See Cloning a Gateway Configuration, page 6-33.

Step 9 (Optional) Add the door configuration that use the ports on the gateway. See Adding New Doors, page 7-2.

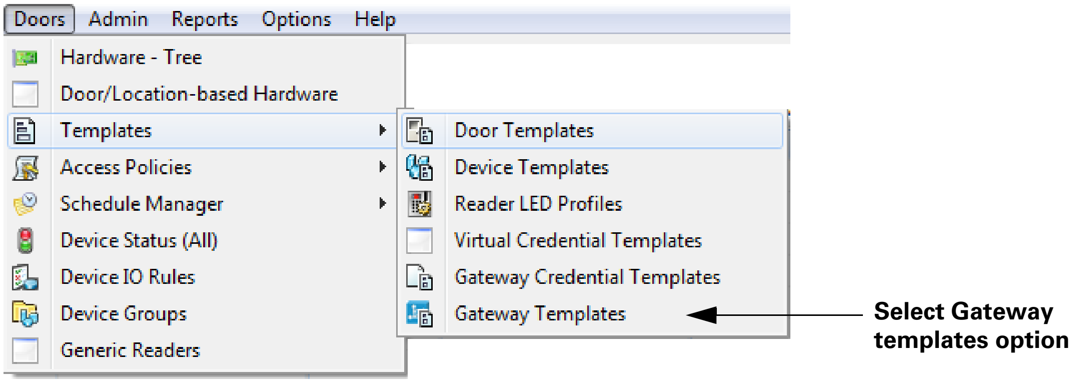


Configuring Gateways Using Existing Templates

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 view the existing templates, select **Gateway Templates** from the **Doors** menu in the **Templates** submenu.

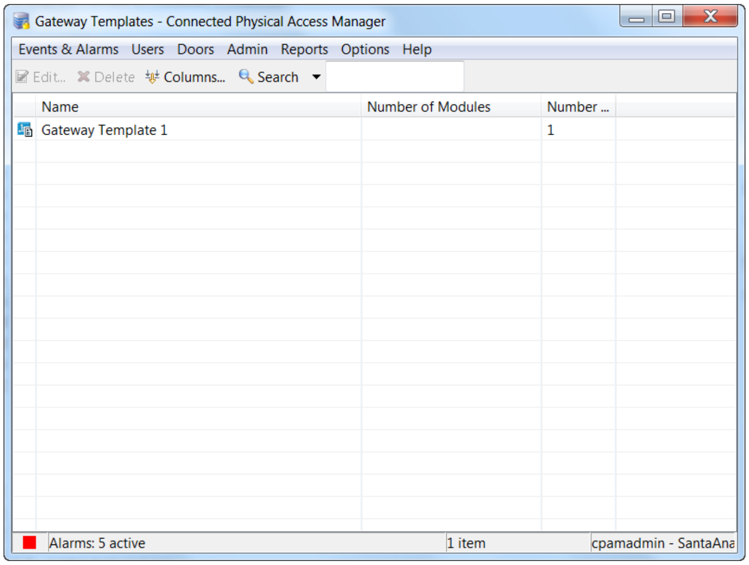
Figure 6-1 Gateway Templates Selection



Select Gateway templates option

Figure 6-2 shows the main window. The default gateway templates cannot be changed. Only user-created templates can be modified.

Figure 6-2 Gateway Templates Main Window



Name	Number of Modules	Number ...
Gateway Template 1		1

Alarms: 5 active 1 item cpamadmin - SantaAna

If the template you need is displayed in the gateway templates window, you can use the following procedure to add a gateway to the system.

To create a gateway using a gateway template, use the following procedure.

Step 1 Create the locations for door and devices.

a. Select **Door/Location-based Hardware** from the **Doors** menu.

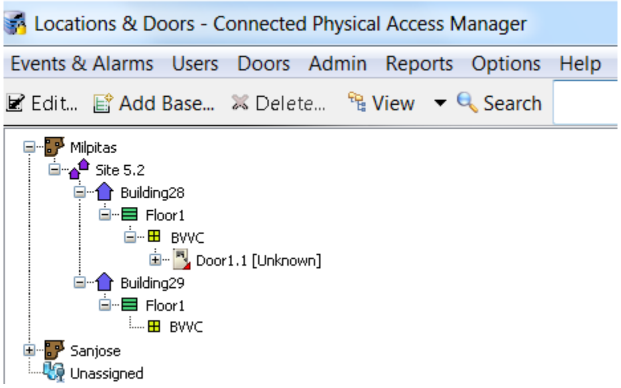
b. To create a new site, click **Add Base**.

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**.

If this has already been done, proceed to Step 2.

Tip You can create any combination of location elements. Door configurations can be assigned to any level of the hierarchical tree.

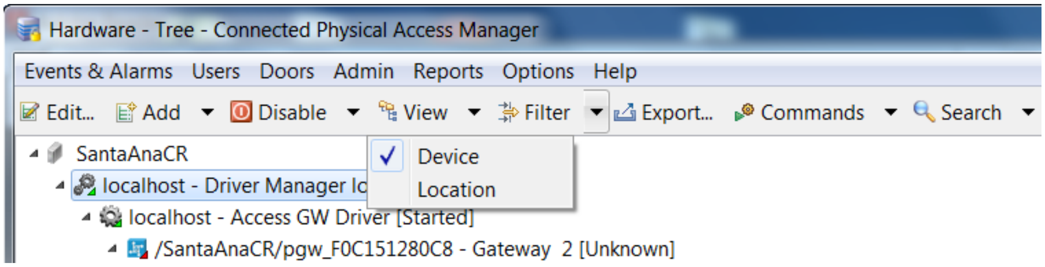

Locations & Doors - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
Milpitas
Site 5.2
Building28
Floor1
BVVC
Door1.1 [Unknown]
Building29
Floor1
BVVC
Sanjose
Unassigned

Step 2 Open the Hardware Tree module.

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

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

Note See Viewing Doors and Devices in the Hardware Tree View, page 5-4 for more information.

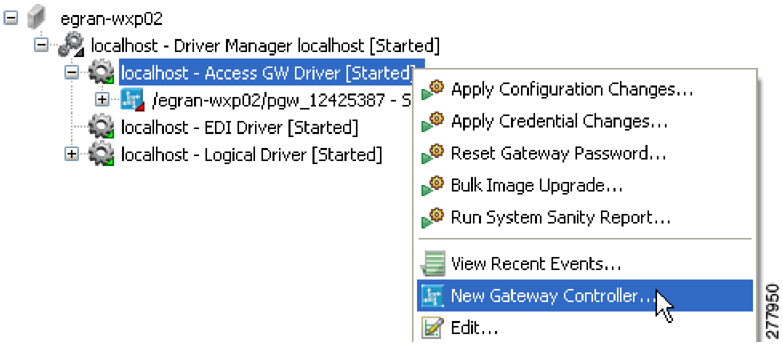

Hardware - Tree - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Disable View Filter Export... Commands Search
SantaAnaCR
localhost - Driver Manager lo
localhost - Access GW Driver [Started]
/SantaAnaCR/pgw_F0C151280C8 - Gateway 2 [Unknown]
✓ Device
Location

Step 3 Add a gateway to ICPAM.

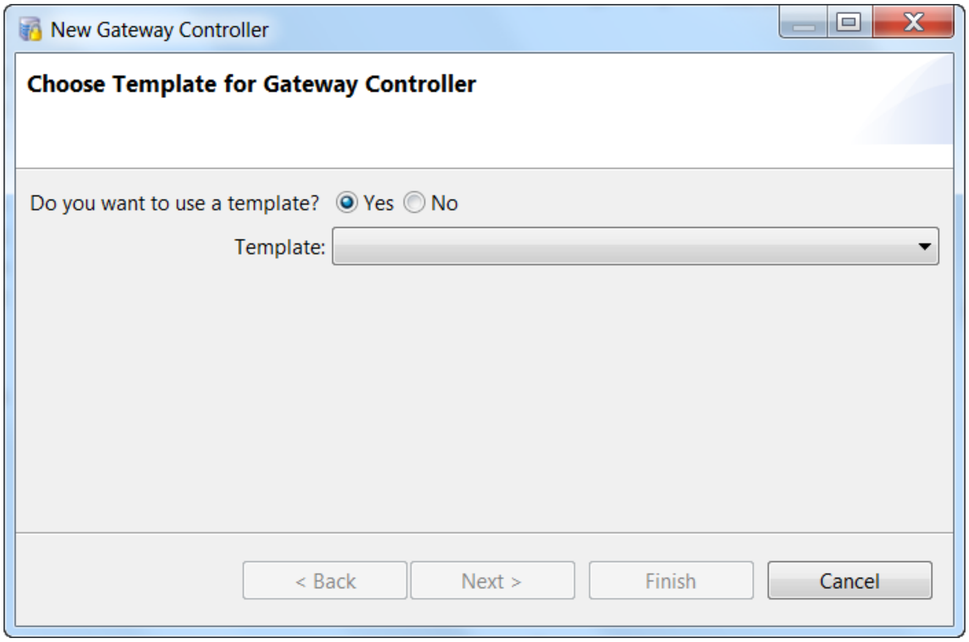
a. Right-click the appropriate Access GW Driver.

b. From the drop-down list, select **New Gateway Controller**.

Note Gateways can also be automatically added to the configuration. See Provisioned (Pre-Populated) vs. Discovered Controller Configurations, page 5-1.


egran-wxp02
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/egran-wxp02/pgw_12425387 - S
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Run System Sanity Report...
View Recent Events...
New Gateway Controller...
Edit...
277950

The Choose Template for Gateway Controller wizard appears.



New Gateway Controller

Choose Template for Gateway Controller

Do you want to use a template? ● Yes ○ No

Template:

Step 4 Select a door template.

a. Select **Yes**.

b. At the **Template** drop-down list, select an existing template.

c. Click **Next**.

Note ICPAM includes sample templates. To create or modify templates, see the "Understanding Door Configurations and Templates" section on page 5-20 and Chapter 8, "Configuring Door and Device Templates".

Step 5 Enter the name, serial number, and location of the controller.

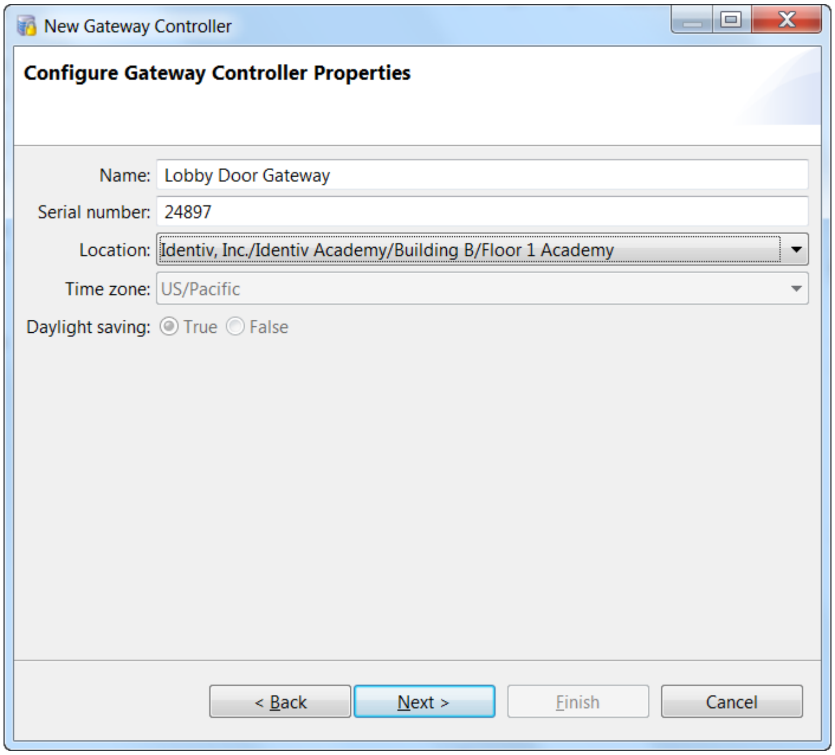
a. **Name**: enter a descriptive name to identify the controller.

b. **Serial Number**: the serial number is unique and cannot be changed. See the "Locating Serial Numbers" section on page 5-37.

c. **Location**: the assigned location of the module. See the "Viewing Doors and Devices by Location" section on page 5-7.

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

d. Click **Next**.



Configure Gateway Controller Properties

Name: Lobby Door Gateway

Serial number: 24897

Location: Identiv, Inc./Identiv Academy/Building B/Floor 1 Academy

Time zone: US/Pacific

Daylight saving: ● True ○ False

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 ().

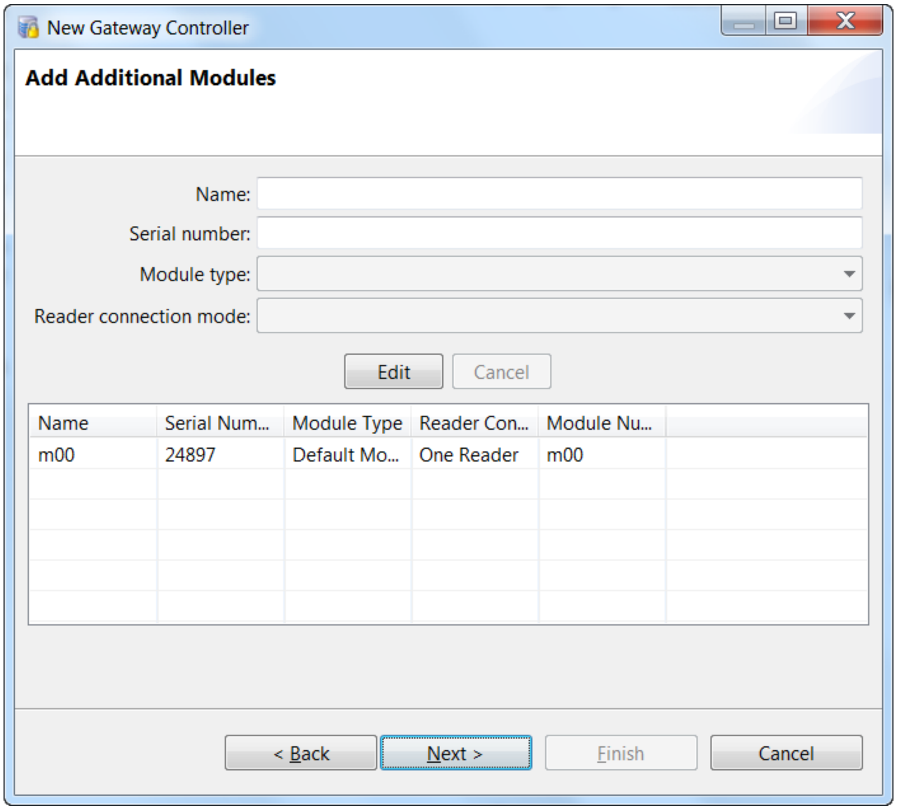
e. (Reader module only) Select the Reader connection mode: one door or two door configuration.

f. Click **Update**.

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

h. Click **Next**

.



Add Additional Modules

Name:
Serial number:
Module type:
Reader connection mode:

Name	Serial Num...	Module Type	Reader Con...	Module Nu...
m00	24897	Default Mo...	One Reader	m00

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 7-2.

a. Select a door template from the list.

b. Click **Edit**.

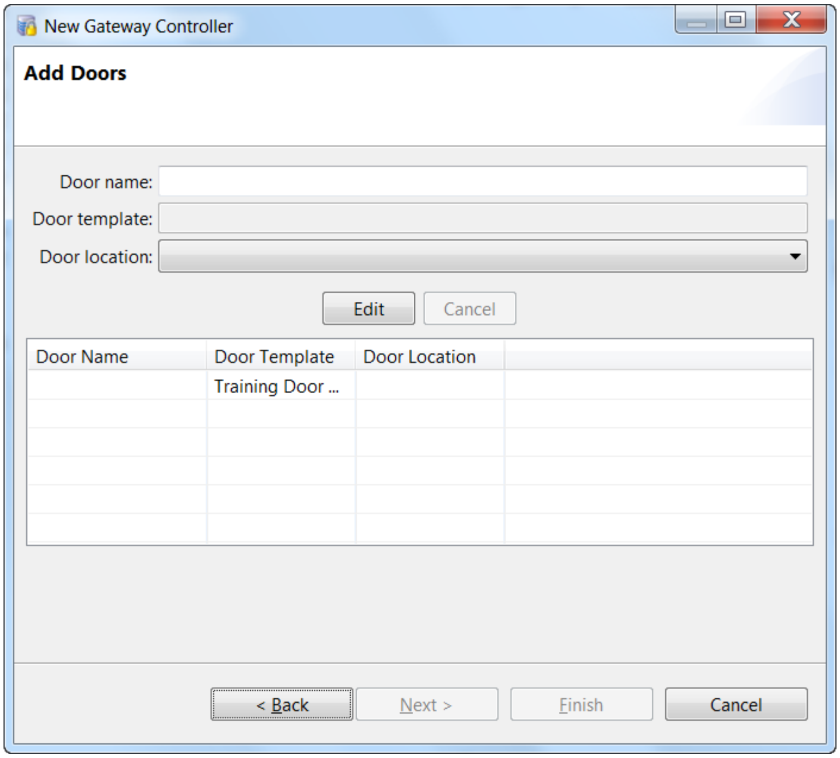
c. Enter the following information:

- **Door Name**: enter a descriptive name for the door.
- **Door Location**: select a location for the door (see Viewing Doors and Devices by Location, page 5-7).

d. Click **Update**.

e. Repeat these steps for each available door.

f. Click **Finish** to create the door configuration(s).



Door Name	Door Template	Door Location
	Training Door ...	

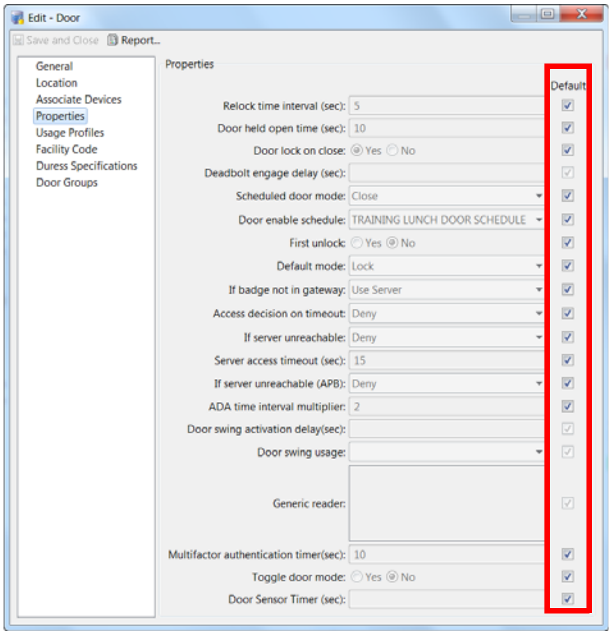
Step 8 (Optional). Modify the door and device properties, if necessary.

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 .).

c. Double click the door or device to open the properties window (or right-click the door and select **Edit**).

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



Edit - Door

Save and Close | Report...

- General
- Location
- Associate Devices
- Properties
- Usage Profiles
- Facility Code
- Duress Specifications
- Door Groups

Properties

		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

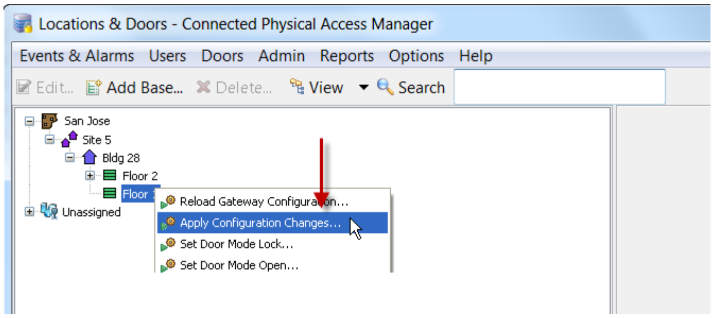
For more information, see the following:

- Chapter 5, "Understanding Controller and Door Configurations"
- Door Configuration Properties, page 8-24
- Device Configuration Properties, page 8-26

Tip You can also modify doors using the Hardware Tree module. Doors are listed under the logical device driver, or in the Hierarchical Locations view.

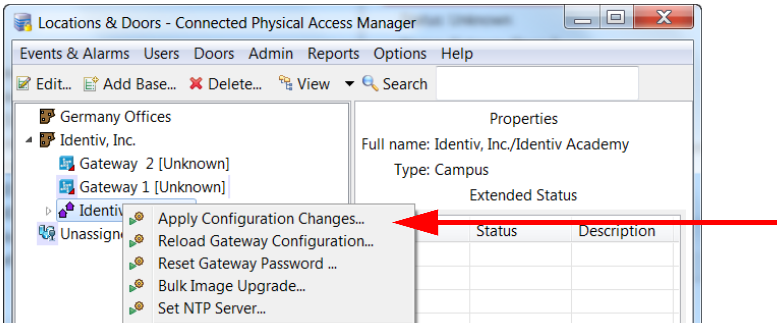
Step 9 Select **Apply Configuration Changes** on the GW Driver or on a specific controller.

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



or

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



Full name: Identiv, Inc./Identiv Academy

Type: Campus

Note Controllers 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.

Step 10 (Optional) Continue Adding New Doors, page 7-2

Note In ICPAM 2.1, you can view the gateways, modules, devices and doors assigned to your location only. For more information, see Location-Restricted User Permissions, page 5-9.

Creating Custom EM-100 Controller Configurations without Templates

To create a door and its attached devices, an Identiv EM-100 controller configuration must first be created that defines the modules and devices attached to the controller.

While ICPAM comes with a default EM-100 template, you can create one or more controller templates by first creating custom controller configurations, then saving them as controller templates for use with the controller wizard (see Configuring EM-100 Controllers Using Existing Templates, page 6-17).

Procedure:

Complete the following instructions to create a custom controller configuration without using an existing controller template, then save it as a template.

Step 1 If required, create the locations for door and devices.

a. Select **Door/Location-based Hardware** from the **Doors** menu.

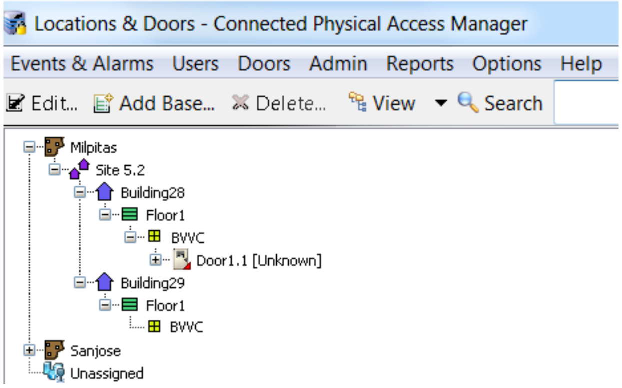
b. To create a new site, click **Add Base**.

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**.

If this has already been done, proceed to Step 2.

Tip You can create any combination of location elements. Door configurations can be assigned to any level of the hierarchical tree.


Locations & Doors - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
Milpitas
Site 5.2
Building28
Floor1
BVVC
Door1.1 [Unknown]
Building29
Floor1
BVVC
Sanjose
Unassigned

Step 2 Open the Hardware Tree module in the Device view.

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

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

Tip See also Viewing Doors and Devices in the Hardware Tree View, page 5-4.

Step 3 Add a controller.

a. From the hardware tree, right-click the Identiv EM-100 Driver.

b. From the drop-down list, select **New Identiv EM-100 Controller...**

The Identiv EM-100 property sheets appear with the General page displayed.

Step 4 Enter the general controller properties.

For details on the fields, refer to Controller General Property Page, page 6-27.

Step 5 Click the **Location** tab and the Location page appears.

Step 6 Specify the location of this controller.

For details on the fields, refer to Controller Location Property Page, page 6-27.

Step 7 Click the **Configuration** tab and the Configuration page appears.

Step 8 Supply fields for this page as required.

For details on this page, refer to Controller Configuration Page, page 6-28.

Step 9 Click the **Calendar and Time Zone** tab. The Calendar and Time Zone page appears.

For details on this page, refer to Controller Calendar and Time Zone Page, page 6-29.

Step 10 Fill out other pages of the property sheet as needed.

Step 11 When you are finished, click the **Save and Close** button.

The new controller appears in the Hardware Tree.

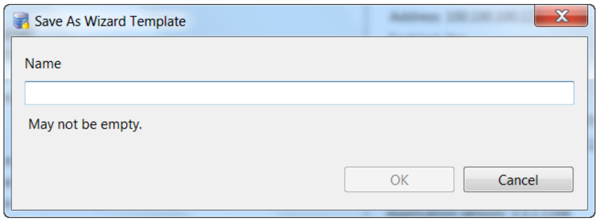
Step 12 Apply the configuration changes to download the new settings to the devices.

- To update all controllers: right-click the parent Identiv EM-100 Driver and select **Apply Configuration Changes...**
- To update a single gateway: right-click the newly-created controller and select **Apply Configuration Changes...**

Note Controllers 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 7-12.

Step 13 (Optional) Create a controller template from the new configuration.

- Right-click on the required controller and select **Save As Wizard Template**. The Save As Wizard Template window appears:

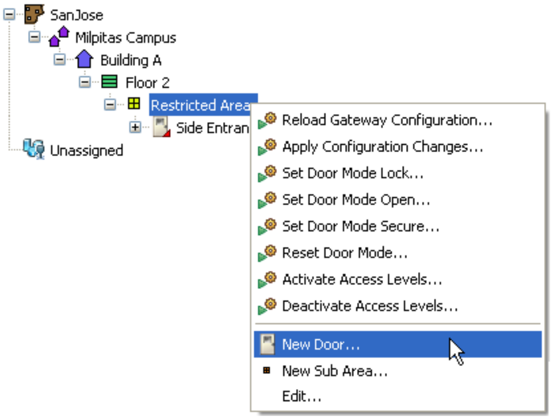


May not be empty.

- Enter a name for the template and click **OK**.

The new controller template is available in the main gateway templates window (see Figure 6-2) and can be used in the EM-100 Controller Wizard. For more on using created controller templates to define still more controllers, refer to Configuring EM-100 Controllers Using Existing Templates, page 6-17.

Step 14 (Optional) Add the door configuration that use the ports on the gateway. See Adding New Doors, page 7-2.



Configuring EM-100 Controllers Using Existing Templates

Use EM-100 controller templates to quickly add a new EM-100 controller configuration. Once the controller is added to the system, you can configure one or more door configurations.

To create an Identiv EM-100 controller using a controller template, use the following procedure.

Step 1 If required, create the locations for door and devices.

a. Select **Door/Location-based Hardware** 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**.

If this has already been done, proceed to Step 2.

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 Tree module.

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

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

Note See Viewing Doors and Devices in the Hardware Tree View, page 5-4 for more information.

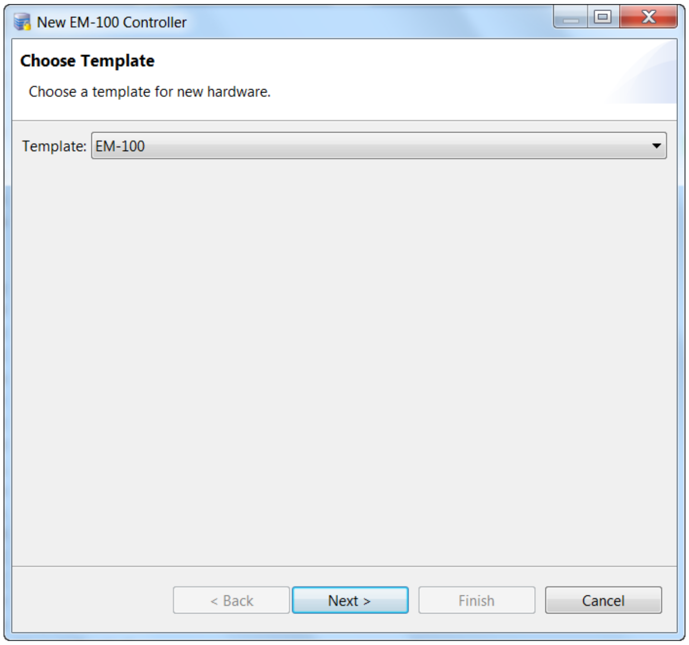
Step 3 Add a controller to ICPAM.

a. Right-click the appropriate Identiv EM-100 Driver.

b. From the drop-down list, select **New Identiv EM-100 Controller Wizard...**

Note Controllers can also be automatically added to the configuration. See Provisioned (Pre-Populated) vs. Discovered Controller Configurations, page 5-1.

The Choose Template for Controller wizard appears.


New EM-100 Controller

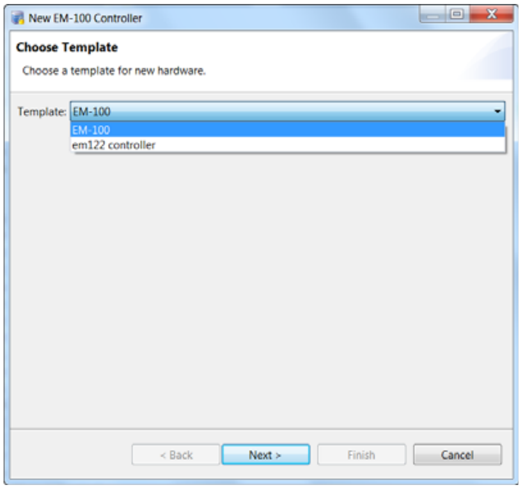
Choose Template

Choose a template for new hardware.

Template: EM-100

Step 4 Select the required controller template from the drop-down list.

All controller templates previously saved using Step 13 in the previous instructions appear in this list.



Choose Template

Choose a template for new hardware.

Template: EM-100

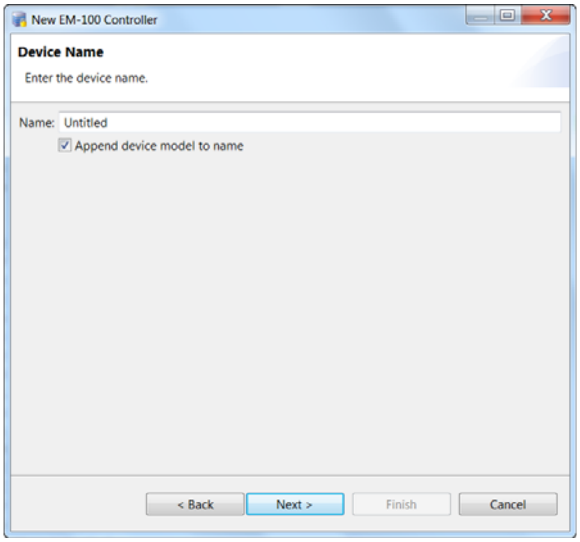
EM-100
em122 controller

All available templates appear in thi drop-down ist.

Note ICPAM includes sample templates. To create or modify templates, see the "Understanding Door Configurations and Templates" section on page 5-20 and Chapter 8, "Configuring Door and Device Templates".

Step 5 Click **Next**.

The next page of the controller wizard appears.



Device Name

Enter the device name.

Name: Untitled

☑ Append device model to name

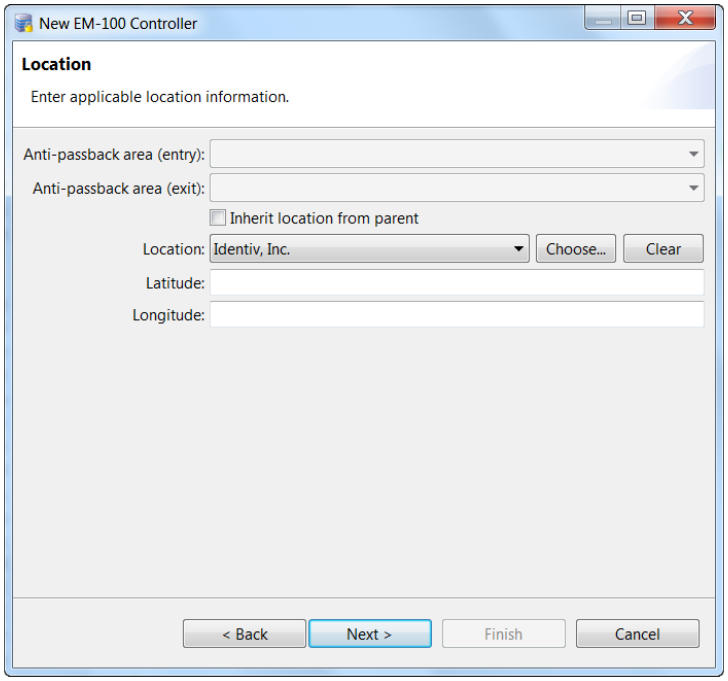
Step 6 Enter the following information.

a. **Name**: enter a descriptive name to identify the controller.

b. **Append device model to the name**: indicate whether the device model should be appended to the name you just entered or uncheck this property to

Step 7 Click **Next**.

The third wizard page appears.



New EM-100 Controller

Location

Enter applicable location information.

Anti-passback area (entry):

Anti-passback area (exit):

□ Inherit location from parent

Location: Identiv, Inc.

Latitude:

Longitude:

Step 8 Edit or enter the fields for this page as required.

a. **Anti-passback area (entry)**: (Optional) From the drop-down list, select the appropriate location where entry to the location associated with this controller occurs.

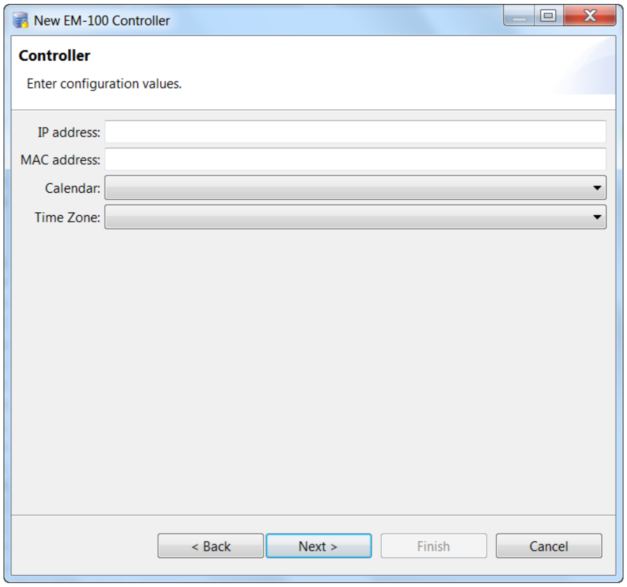
b. **Anti-passback area (exit)**: (Optional) From the drop-down list, select the appropriate location where exit from the location associated with this controller occurs.

c. **Inherit location from parent:** Check this box to indicate that this controller inherits its location from the parent location determined by the position of the driver.

d. **Location**: the assigned location of the module. See the "Viewing Doors and Devices by Location" section on page 5-7.

Step 9 Click **Next**.

The fourth page of the wizard appears.


New EM-100 Controller

Controller

Enter configuration values.

IP address:

MAC address:

Calendar:

Time Zone:

Step 10 Supply the following values.

a. **IP Address**: Enter the appropriate IP address for this device. The address is determined by the controller's setup and is described in the setup instructions in the *ICPAM Installation Guide*.

b. **MAC Address**: (Optional) Enter the MAC address for this controller. The MAC address is located on the EM-100 controller.

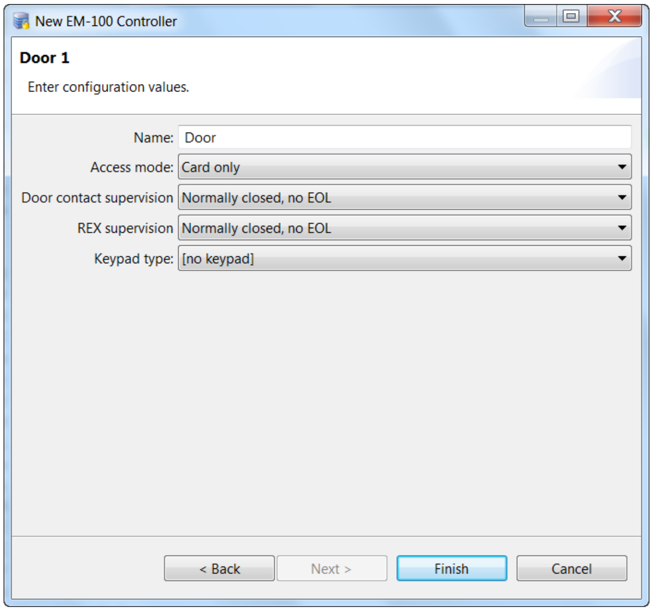
c. **Calendar**: From the drop-down list, select the calendar used for this controller.

d. **Time Zone**: From the drop-down list, select the time zone where this controller is currently located.

For details on this feature, refer to Controller Calendar and Time Zone Page, page 6-29.

Step 11 Click **Next.**

The fifth page of the wizard appears.


New EM-100 Controller

Door 1

Enter configuration values.

Name: Door

Access mode: Card only

Door contact supervision Normally closed, no EOL

REX supervision Normally closed, no EOL

Keypad type: [no keypad]

Step 12 (Optional) Enter configuration values for each door.

Note If door configurations are not included in the controller template, complete these instructions, and continue to Adding Doors Using Door Templates, page 7-2.

a. **Name**: enter a descriptive name for the door.

b. **Access mode**: From the drop-down list, select one of the existing door modes. These include **Card only**, **Code only**, and **Card and Code**.

c. **Door contact supervision**: From the drop-down list, select the type of supervision allowed for contacts associated with this door. Besides the default supervisions, such as Normally Open or Normally Closed, there are supervision modes that the user can customize. For more on this, refer to Input Supervisions in Driver Input Supervision Page, page 6-44.

d. REX supervision: From the drop-down list, select the type of supervision allowed for REXs associated with this door. Besides the default supervisions, such as Normally Open or Normally Closed, there are supervision modes that the user can customize. For more on this, refer to Input Supervisions in Driver Input Supervision Page, page 6-44.

e. Keypad type: From the drop-down list, select the type of keypad used by the reader associated with this door.

Step 13 Click **Finish** to create the door configuration.

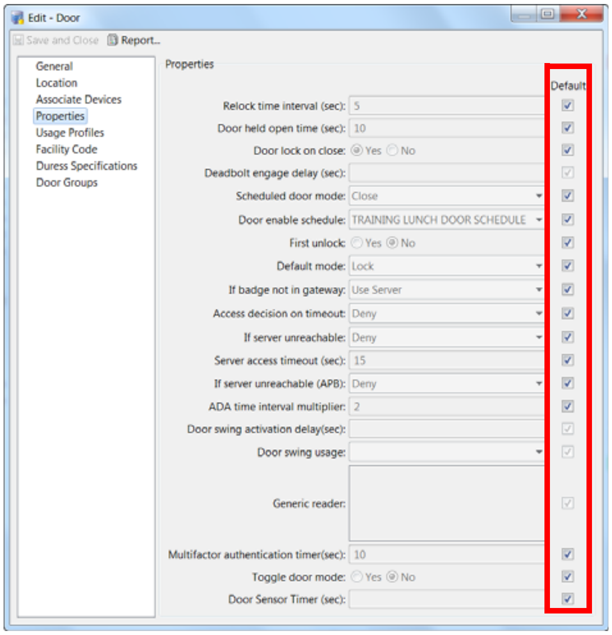
Step 14 (Optional). Modify the door and device properties, if necessary.

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 .).

c. Double click the door or device to open the properties window (or right-click the door and select **Edit**).

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



Properties

		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

For more information, see the following:

- Chapter 5, "Understanding Controller and Door Configurations"
- Door Configuration Properties, page 8-24
- Device Configuration Properties, page 8-26

Tip You can also modify doors using the Hardware Tree module. Doors are listed under the logical device driver, or in the Hierarchical Locations view.

Step 15 Apply Configuration Changes for the specific controller. For more on this, refer to "Applying Configuration Changes to Controllers" section on page 6-31.

Step 16 (Optional) Continue Adding New Doors, page 7-2.

Related Documentation

For more information, see the following:

- Chapter 5, "Understanding Controller and Door Configurations"
- Chapter 8, "Configuring Door and Device Templates"

Modifying Existing Controllers

There are two distinct types of controllers supported by ICPAM:

- Gateway controllers
- Identiv EM-100 controllers

To modify an existing controller, follow this procedure.

Editing Gateway Controllers

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** from the **Doors** menu.

Step 2 Right-click a gateway controller and select **Edit**.

The gateway property sheets appear. For more on these property sheets, refer to Gateway Controller Property Sheets, page 6-24.

Step 3 Make changes to the fields on each page as required.

Step 4 When you are finished, click **Save**.

Step 5 Select **Apply Configuration Changes** on the GW Driver or on a specific controller. For more on this, refer to "Applying Configuration Changes to Controllers" section on page 6-31.

Note Controllers 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.

Editing Identiv EM-100 Controllers

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** from the **Doors** menu.

Step 2 Right-click a Identiv EM-100 controller and select **Edit**.

The Identiv EM-100 controller property sheets appear. For more on this, refer to EM-100 Controller Property Sheets, page 6-26.

Step 3 Make changes to the fields on each page as required.

Step 4 When you are finished, click **Save**.

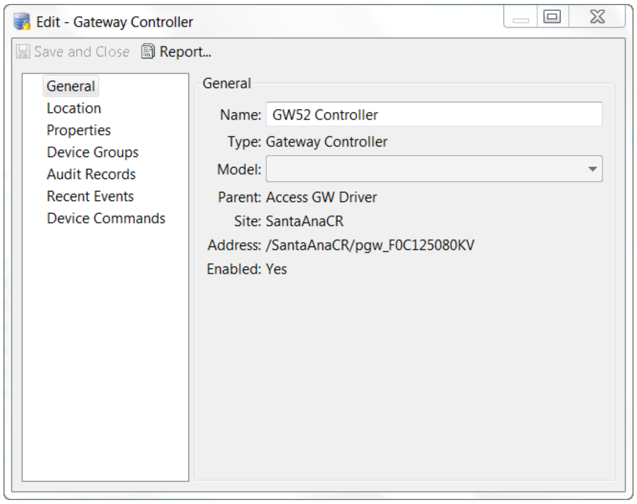
Step 5 Apply configuration changes using the instructions in "Applying Configuration Changes to Controllers" section on page 6-31.

Gateway Controller Property Sheets

When you add or edit an existing gateway controller, the gateway property sheets appear. The most important property pages and the fields on them are explained in the following subsections.

- Gateway General Property Page, page 6-24
- Gateway Location Property Sheet, page 6-25
- Gateway Properties Property Sheet, page 6-26

Gateway General Property Page

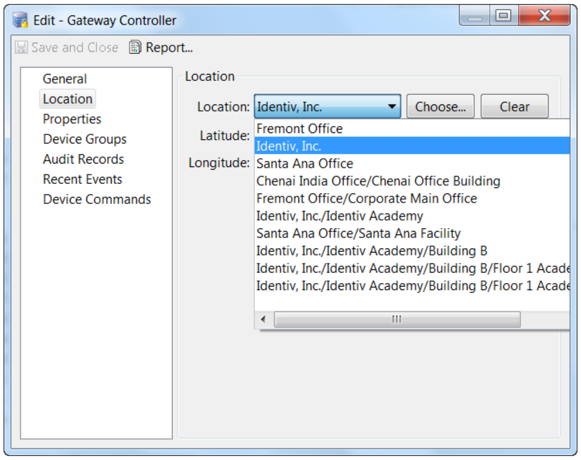


Name: GW52 Controller
Type: Gateway Controller
Model:
Parent: Access GW Driver
Site: SantaAnaCR
Address: /SantaAnaCR/pgw_F0C125080KV
Enabled: Yes

Name	Enter an appropriate name for this gateway controller.
Type	This read only field supplies the type for this controller.
Model	From the drop-down list, select the model of this EM-100. Currently, there is only one model, so this field need not be used.

Parent	This read-only field provides the relationship of this controller to the controllers around it: parent or child.
Site	This read-only field is populated with the current site under which this controller appears in the Hardware Tree.
Address	Check the Enabled box if the address of this controller has been placed on line. Check Inherit enable/disable from parent to separate this controller from its parent controller.
Comments	(optional) Enter any comments describing or giving details for this controller.

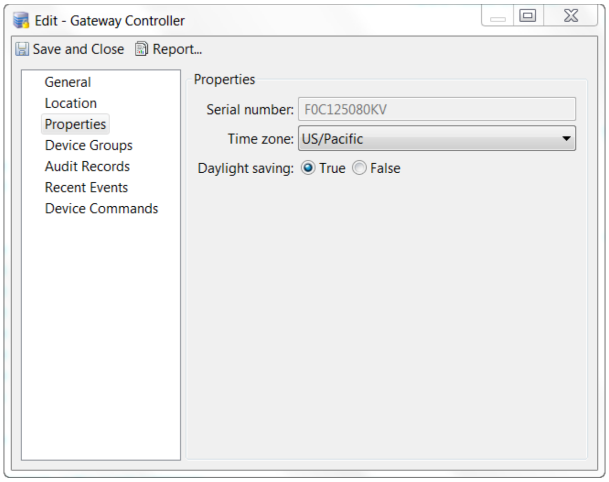
Gateway Location Property Sheet


Edit - Gateway Controller
Save and Close
Report...
General
Location
Properties
Device Groups
Audit Records
Recent Events
Device Commands
Location
Choose...
Clear
Latitude:
Longitude:
Fremont Office
Identiv, Inc.
Santa Ana Office
Chenai India Office/Chenai Office Building
Fremont Office/Corporate Main Office
Identiv, Inc./Identiv Academy
Santa Ana Office/Santa Ana Facility
Identiv, Inc./Identiv Academy/Building B
Identiv, Inc./Identiv Academy/Building B/Floor 1 Acade
Identiv, Inc./Identiv Academy/Building B/Floor 1 Acade

Location: Identiv, Inc.

Location	From the drop-down list, select one of the pre-defined locations or click **Choose** to create and select a new location. For more on this, see the "Viewing Doors and Devices by Location" section on page 5-7.
Latitude	Enter the latitude where this controller is placed. If this controller is attached to a NTP server, the latitude and longitude are automatically populated.
Longitude	Enter the longitude where this controller is placed. If this controller is attached to a NTP server, the latitude and longitude are automatically populated.

Gateway Properties Property Sheet



Edit - Gateway Controller

Save and Close Report...

Properties

Serial number: F0C125080KV

Time zone: US/Pacific

Daylight saving: ● True ○ False

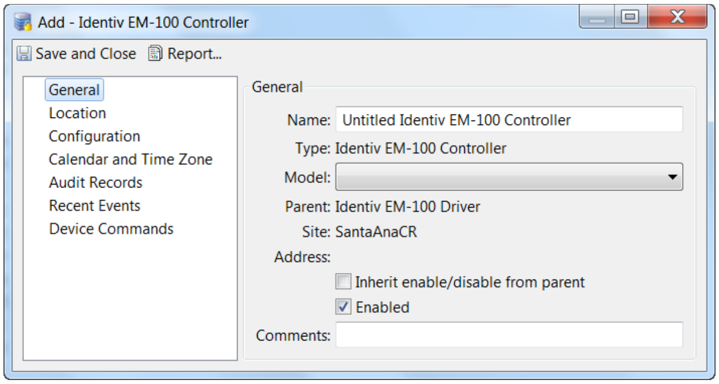
Serial number	The serial number is unique and cannot be changed. See the "Locating Serial Numbers" section on page 5-37.
Time Zone	From the drop-down list, select the time zone in which this gateway is located.
Daylight savings	Click the **True** radio button to indicate that this time zone recognizes daylight savings. Click the **False** radio button to indicate that this time zone does not use daylight savings.

EM-100 Controller Property Sheets

When you add or edit an existing controller, the EM-100 Controller property sheets appear. Each property page and the fields on them are explained in the following subsections.

- Controller General Property Page, page 6-27
- Controller Location Property Page, page 6-27
- Controller Configuration Page, page 6-28
- Controller Calendar and Time Zone Page, page 6-29
- Controller Audit Records Page, page 6-29
- Controller Recent Events Page, page 6-30
- Controller Device Commands, page 6-30

Controller General Property Page



Add - Identiv EM-100 Controller

General

Name: Untitled Identiv EM-100 Controller

Type: Identiv EM-100 Controller

Model:

Parent: Identiv EM-100 Driver

Site: SantaAnaCR

Address:

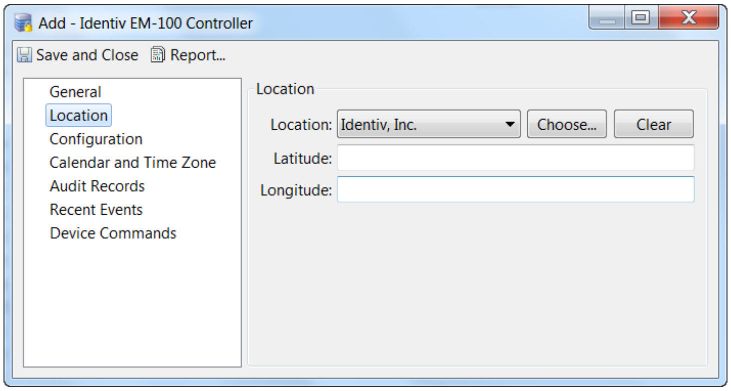
□ Inherit enable/disable from parent

☑ Enabled

Comments:

Name	Enter an appropriate name for this Identiv EM-100 controller.
Type	This read only field supplies the type for this controller.
Model	From the drop-down list, select the model of this EM-100. Currently, there is only one model so this field need not be used.
Parent	This read-only field provides the relationship of this controller to the controllers around it: parent or child.
Site	This read-only field is populated with the current site under which this controller appears in the Hardware Tree.
Address	Check the Enabled box if the address of this controller has been placed on line. Check Inherit enable/disable from parent to separate this controller from its parent controller.
Comments	(optional) Enter any comments describing or giving details for this controller.

Controller Location Property Page



Add - Identiv EM-100 Controller

Location

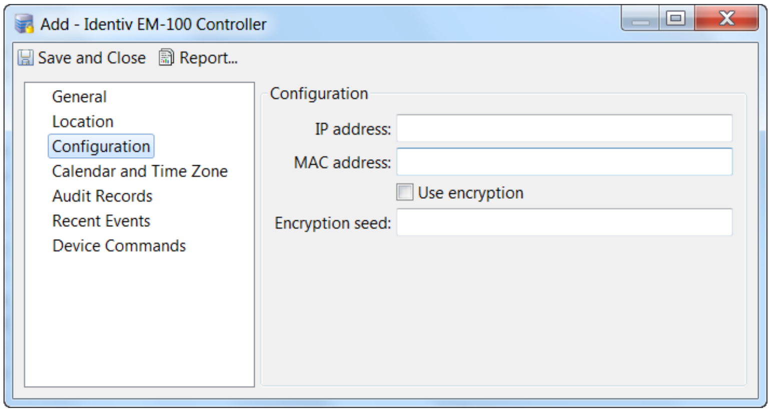
Location: Identiv, Inc.

Latitude:

Longitude:

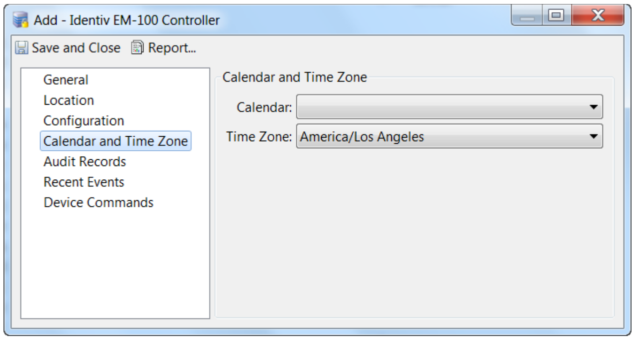
Location	From the drop-down list, select one of the pre-defined locations or click **Choose** to create and select a new location. For more on this, see the "Viewing Doors and Devices by Location" section on page 5-7.
Latitude	Enter the latitude where this controller is placed. If this controller is attached to a NTP server, the latitude and longitude are automatically populated.
Longitude	Enter the longitude where this controller is placed. If this controller is attached to a NTP server, the latitude and longitude are automatically populated.

Controller Configuration Page



IP address	Enter the IP address of this controller. To determine the IP address of this controller, refer to the *ICPAM Installation Guide*.
MAC address	(optional) Enter the MAC address of this controller. To determine the MAC address of this controller, examine the label on the EM-100 controller. When a MAC address is specified, ICPAM can discover the IP address of the controller.
Use encryption	Check this box to implement encryption whenever this controller is communicating with its attached devices and with the ICPAM server.

Controller Calendar and Time Zone Page

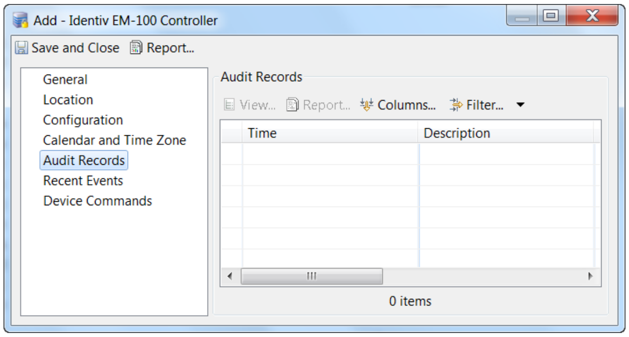


Calendar:

Time Zone: America/Los Angeles

Calendar	From the drop-down list, the calendar used on which to base the time zone.
Time Zone	From the drop-down list, select the time zone where this controller is located. The Time Zone and Daylight Savings setting are not configurable if defined by the template.

Controller Audit Records Page

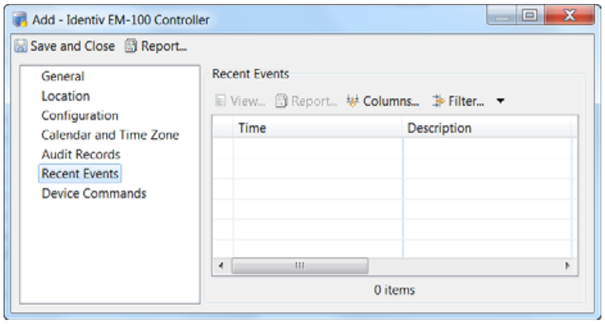


Time	Description

0 items

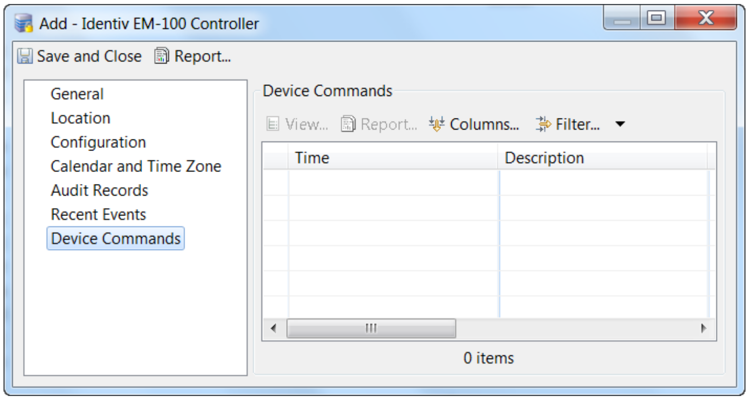
This table displays a list of all audit records detected for this controller. For more on this, see Viewing Audit Records and Events for Personnel Records, page 9-9.

Controller Recent Events Page



This table displays a list of all recent events recorded for this controller. See Viewing the Recent Events for a Device or Driver, page 5-15.

Controller Device Commands



This table displays a list of all device commands associated with this controller. For more on this, see Device Commands, page 7-39.

Applying Configuration Changes

Changes made to a door or device configuration in ICPAM are inactive until applied to the controller. You can apply the configuration changes to a specific controller, to all controllers, or to all controllers in a location. Applying a configuration downloads the revised configuration file to the controller.

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

This section includes the following information.

- Applying Configuration Changes to Controllers, page 6-31
- Configuration Management in Provisioned vs. Discovered Configurations, page 6-32

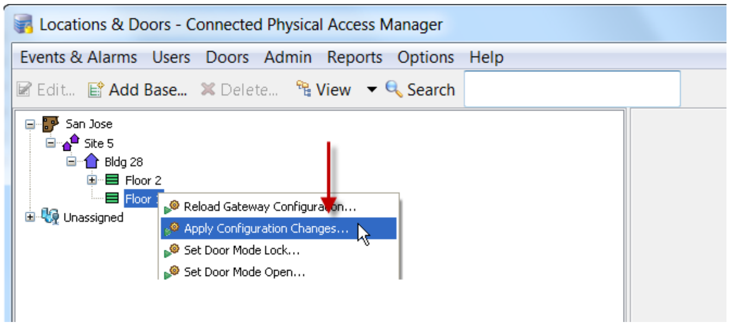
Applying Configuration Changes to Controllers

You can download the configuration to controllers using either the **Hardware Tree** or **Door/Location-based Hardware** modules.

Applying Configuration Changes in the Hardware Tree Module

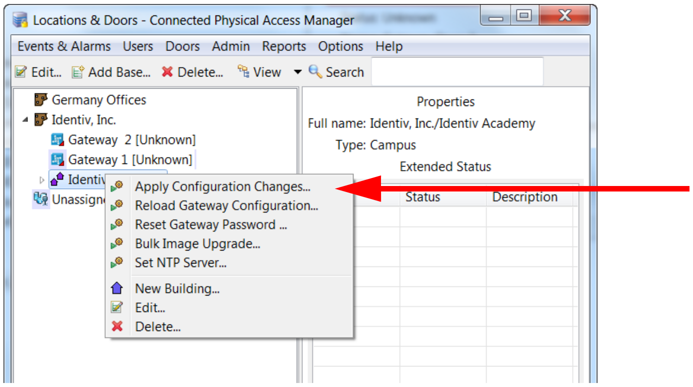
Select **Apply Configuration Changes** on the Identiv or GW Driver or on a specific controller.

- Right-click the designated driver and select **Apply Configuration Changes** to download configuration changes for all controllers.


Locations & Doors - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
San Jose
Site 5
Bldg 28
Floor 2
Floor
Unassigned
Reload Gateway Configuration...
Apply Configuration Changes...
Set Door Mode Lock...
Set Door Mode Open...

or

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


Locations & Doors - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
Germany Offices
Identiv, Inc.
Gateway 2 [Unknown]
Gateway 1 [Unknown]
Identiv
Unassigne
Apply Configuration Changes...
Reload Gateway Configuration...
Reset Gateway Password ...
Bulk Image Upgrade...
Set NTP Server...
New Building...
Edit...
Delete...

Properties

Full name: Identiv, Inc./Identiv Academy

Type: Campus

Extended Status

Status	Description

Note Controllers must be in the Up state, signified by a green triangle in the icon. A dark green triangle means configuration changes that have not been applied. See Understanding Device Status Colors, page 5-13.

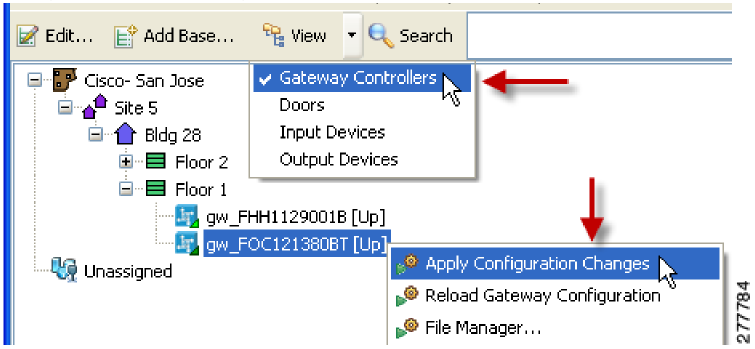
Applying Configuration Changes in the Door/Location-Based Module

Select **Apply Configuration Changes** on the affected controller or on a location.

Specific Controller:

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

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

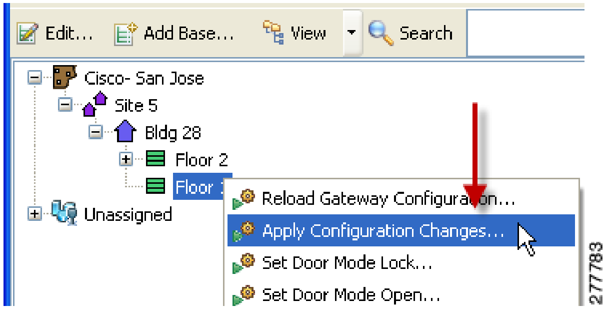


or

Multiple Controllers:

a. Right-click a location icon.

b. Select **Apply Configuration Changes**.



Note Controllers must be in the Up state, signified by a green triangle in the icon. A dark green triangle means configuration changes that have not been applied. See Understanding Device Status Colors, page 5-13.

Configuration Management in Provisioned vs. Discovered Configurations

- In a Provisioned configuration, the configuration is entered before the controller is brought online and the configuration is automatically downloaded when the controller 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 controller is added to the network before a configuration is created. ICPAM automatically creates a basic configuration containing the serial numbers of the controller and any expansion modules. Any subsequent configuration changes must be downloaded using one of the methods described in this section.
- If a controller 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 Controller Configurations, page 5-1 for more information.

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 controller. Changes to the original gateway or to the clone gateway do not effect each other.

Note Cloning can only be done with gateway controllers. Identiv EM-100 controllers do not yet support cloning.

To create a gateway clone, do the following:

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** 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.

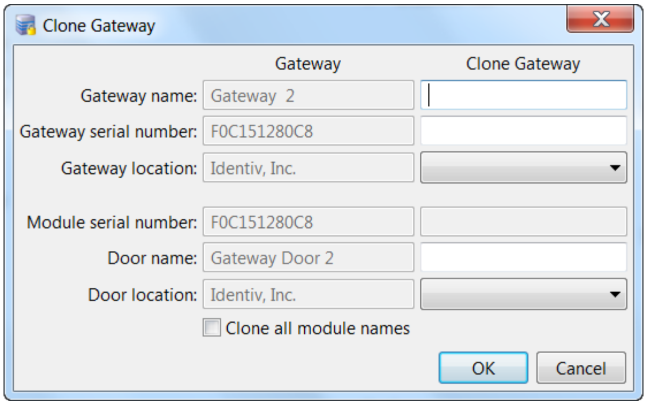
Step 4 (Optional) Click **Clone all module names** to use the source names for the clone configuration.

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 Adding New Doors, page 7-2 for more information.

Figure 6-3 Clone Gateway



	Gateway	Clone Gateway
Gateway name:	Gateway 2	
Gateway serial number:	F0C151280C8	
Gateway location:	Identiv, Inc.	
Module serial number:	F0C151280C8	
Door name:	Gateway Door 2	
Door location:	Identiv, Inc.	

□ Clone all module names

Tip To create a template from a gateway configuration, see Creating Custom Gateway Configurations without Templates, page 6-2.

Replacing a Gateway

Note Replacement can only be done with gateway controllers. Identiv EM-100 controllers do not yet support this feature.

To replace a gateway with a new device, complete the following instructions.

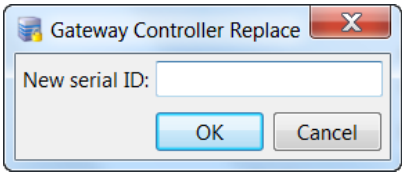
Note The replacement module must be the same as the old module, and all device connections must be the same. All configurations and properties remain the same.

Step 1 Physically remove the old device. ICPAM automatically detects the removal and disables the device configuration.

Step 2 In the **Hardware Tree** 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**.



Gateway Controller Replace

New serial ID:

Step 5 Physically install the replacement gateway or expansion module.

Tip Connect expansion modules to the same gateway interface. The gateway automatically recognizes the new module, and enables the device in ICPAM.

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

Deleting a Controller

To delete a controller, do the following:

Step 1 Enable the Delete functions, as described in Enabling the Delete Options, page 7-17.

Step 2 Disable all devices in all doors associated with the Controller, as described in Disabling or Deleting a Door, page 7-15.

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

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

Step 5 Select **Yes** to confirm.

Step 6 Download the changes to the controller, as described in For more on this process, see Applying Configuration Changes to Controllers, page 6-31.

Changing Gateway Passwords

You can change the password for one or more Gateways in the **Hardware Tree** module, or the **Door/Location-based Hardware** module.

Note This feature is not supported by the Identiv EM-100 controller.

Step 1 Display the gateway or controller:

- Select **Door/Location-based Hardware** from the **Doors** menu and select **Gateway Controllers** from the **View** menu.

  or

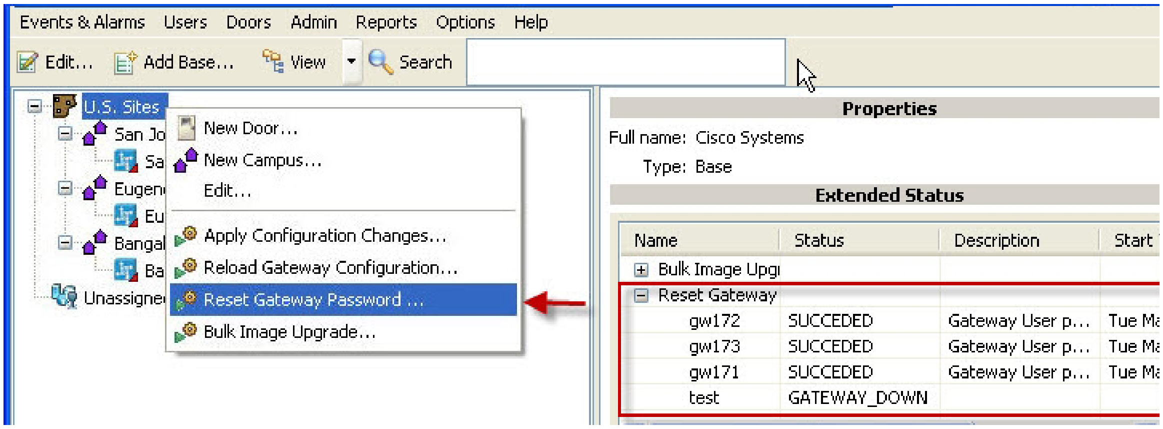
- Select **Hardware Tree** from the **Doors** menu and expand the Access GW Driver device tree.

Step 2 Change the password for one or more gateways:

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

See Figure 6-4 and Figure 6-5 for examples to change the gateway passwords.

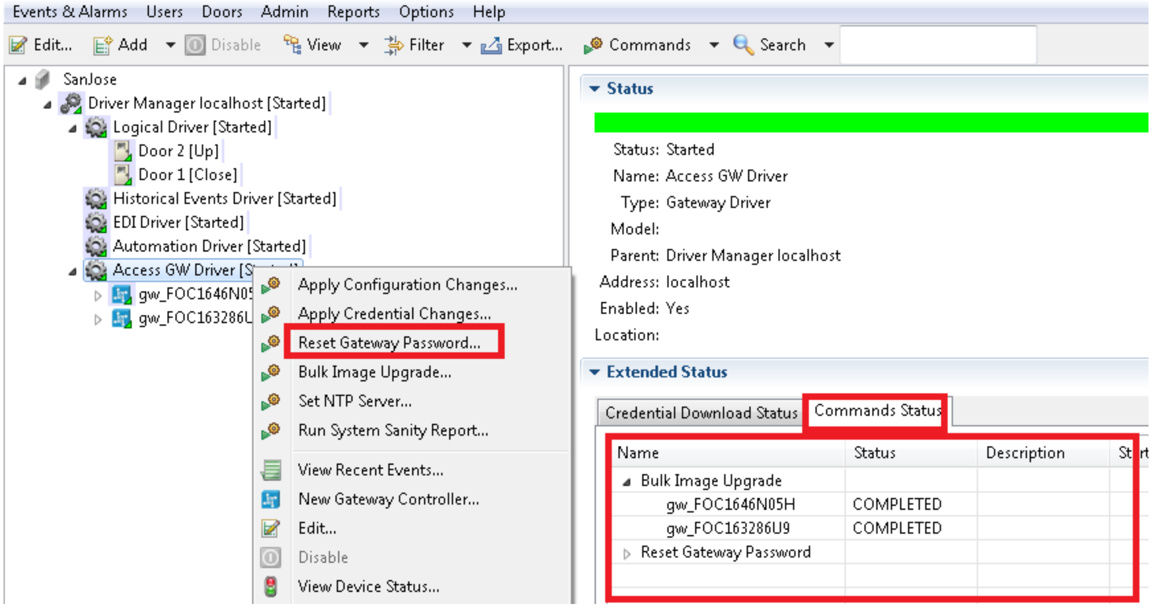
Figure 6-4 Reset Gateway Password from Door/Location-based Hardware



Full name: Cisco Systems
Type: Base

Name	Status	Description	Start
⊞ Bulk Image Upgı			
⊟ Reset Gateway			
gw172	SUCCEDED	Gateway User p...	Tue Ma
gw173	SUCCEDED	Gateway User p...	Tue Ma
gw171	SUCCEDED	Gateway User p...	Tue Ma
test	GATEWAY_DOWN		

Figure 6-5 Reset Gateway Password from Hardware Tree



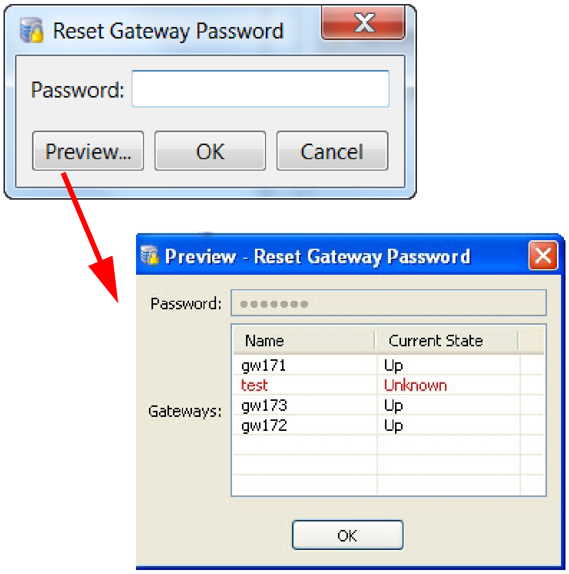
Status: Started
Name: Access GW Driver
Type: Gateway Driver
Model:
Parent: Driver Manager localhost
Address: localhost
Enabled: Yes
Location:

Name	Status	Description	St rt
Bulk Image Upgrade			
gw_FOC1646N05H	COMPLETED		
gw_FOC163286U9	COMPLETED		
Reset Gateway Password			

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

Step 4 Enter a new password and click **OK** (Figure 6-6).

Figure 6-6 Enter a Gateway Password



Password: •••••••

Name	Current State
gw171	Up
test	Unknown
gw173	Up
gw172	Up

Step 5 Verify the status of the change:

- In the **Door/Location-based Hardware** module, select a location. The command status is displayed under Extended Status in the lower right of the screen (see Figure 6-4 on page 6-35).

- In the **Hardware Tree** module, select the required Access GW Driver. Select the Command Status tab under Extended Status in the lower right of the screen (see Figure 6-4 on page 6-35).

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*.

Modifying Driver Configurations

The ICPAM system tree includes many drivers that are installed during setup and configuration. These include the GW Driver and the Identiv EM-100 Driver that can be configured to provide a custom environment for the controllers and devices that are subordinate to them.

- Editing Identiv EM-100 Controllers, page 6-24
- Modifying GW Drivers, page 6-37

Modifying GW Drivers

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** from the **Doors** menu.

Step 2 Right-click a Access GW driver and select **Edit**.

The Edit Gateway driver property sheets appear. For more on these sheets, see Access GW Driver Property Sheets, page 6-38.

Step 3 Make changes to the fields on each page as required.

Step 4 When you are finished, click **Save**.

Step 5 Select **Apply Configuration Changes** on the Identiv Driver or on a specific controller.

Modifying Identiv EM-100 Drivers

Step 1 Select **Hardware Tree** or **Door/Location-based Hardware** from the **Doors** menu.

Step 2 Right-click a Identiv driver and select **Edit**.

The Edit Identiv Driver property sheets appear. For more on these sheets, see Identiv EM-100 Driver Property Sheets, page 6-40.

Step 3 Make changes to the fields on each page as required.

Step 4 When you are finished, click **Save**.

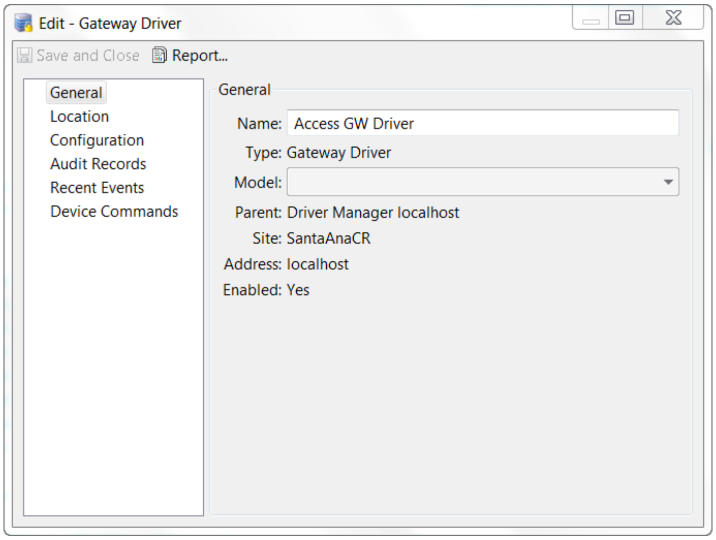
Step 5 Select **Apply Configuration Changes** on the Identiv Driver or on a specific controller.

Access GW Driver Property Sheets

When you select **Edit** from the Access GW Driver option list, a multi-page property sheet appears. Each of these pages and the fields that appear on them are explained on the following pages.

- Gateway Driver General Page, page 6-38
- Gateway Driver Location Property Page, page 6-39
- Gateway Driver Configuration Property Page, page 6-40
- Gateway Driver Recent Events Property Sheet, page 6-40

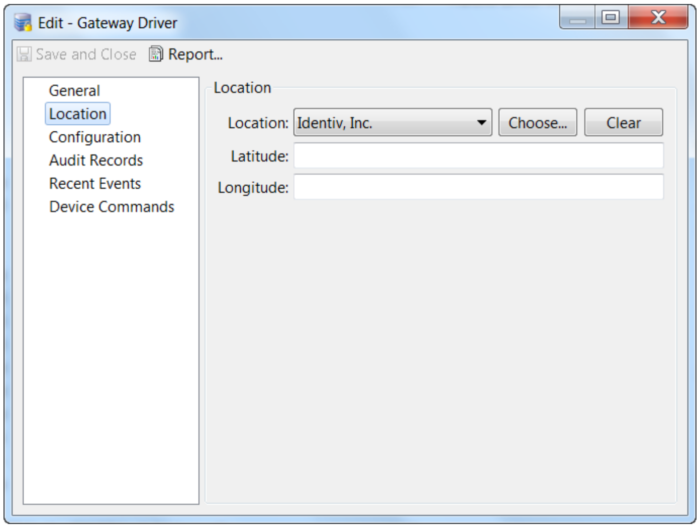
Gateway Driver General Page



Name: Access GW Driver
Type: Gateway Driver
Model:
Parent: Driver Manager localhost
Site: SantaAnaCR
Address: localhost
Enabled: Yes

Name	Enter an appropriate name for this Access GW driver.
Type	This read only field supplies the type for this driver.
Model	From the drop-down list, select the model of this driver. Currently, there is only one driver model so this field need not be used.
Parent	This read-only field provides the relationship of this driver to other drivers: parent or child.
Site	This read-only field is populated with the current site under which this driver appears in the Hardware Tree.
Address	This read-only field indicates the address of the driver.
Enabled	This read-only field indicates whether this driver is enabled or disabled.

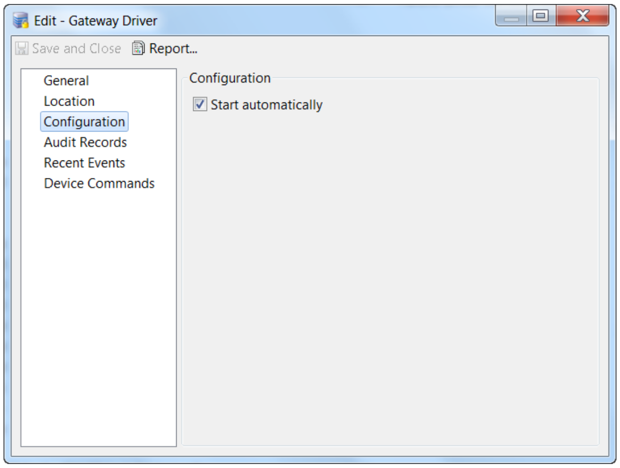
Gateway Driver Location Property Page



Location: Identiv, Inc.
Latitude:
Longitude:

Location	From the drop-down list, select one of the pre-defined locations or click **Choose** to create and select a new location. For more on this, see the "Viewing Doors and Devices by Location" section on page 5-7.
Latitude	(Optional) Enter the latitude where this driver is placed. If this driver is attached to a NTP server, the latitude and longitude are automatically populated.
Longitude	(Optional) Enter the longitude where this driver is placed. If this driver is attached to a NTP server, the latitude and longitude are automatically populated.

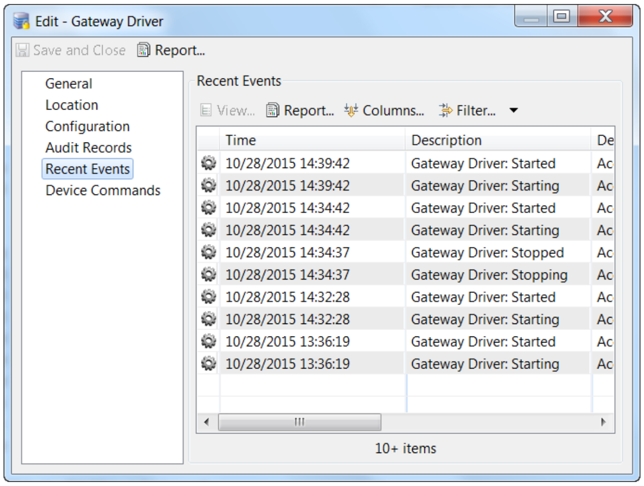
Gateway Driver Configuration Property Page



☑ Start automatically

Start Automatically	Check this box to indicate that the driver is automatically started whenever ICPAM server is started. The default is checked (enabled).

Gateway Driver Recent Events Property Sheet



Time	Description	De
10/28/2015 14:39:42	Gateway Driver: Started	Ac
10/28/2015 14:39:42	Gateway Driver: Starting	Ac
10/28/2015 14:34:42	Gateway Driver: Started	Ac
10/28/2015 14:34:42	Gateway Driver: Starting	Ac
10/28/2015 14:34:37	Gateway Driver: Stopped	Ac
10/28/2015 14:34:37	Gateway Driver: Stopping	Ac
10/28/2015 14:32:28	Gateway Driver: Started	Ac
10/28/2015 14:32:28	Gateway Driver: Starting	Ac
10/28/2015 13:36:19	Gateway Driver: Started	Ac
10/28/2015 13:36:19	Gateway Driver: Starting	Ac

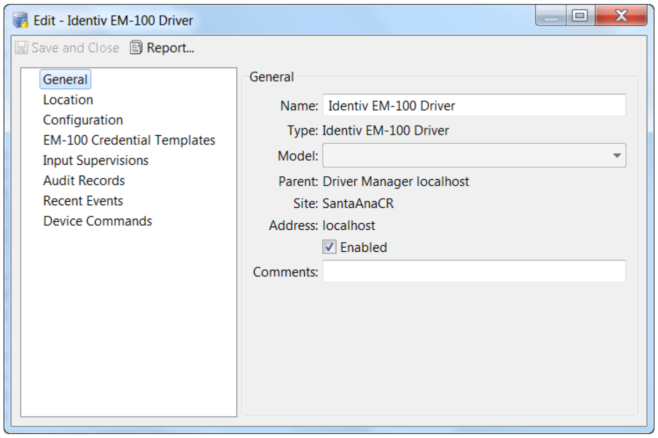
10+ items

This table displays a list of all recent events recorded for this driver. See Viewing the Recent Events for a Device or Driver, page 5-15.

Identiv EM-100 Driver Property Sheets

When you select **Edit** from the Identiv EM-100 Driver option list, a multi-page property sheet appears. Each of these pages and the fields that appear on them are explained on the following pages.

Driver General Page



General

Name: Identiv EM-100 Driver

Type: Identiv EM-100 Driver

Model:

Parent: Driver Manager localhost

Site: SantaAnaCR

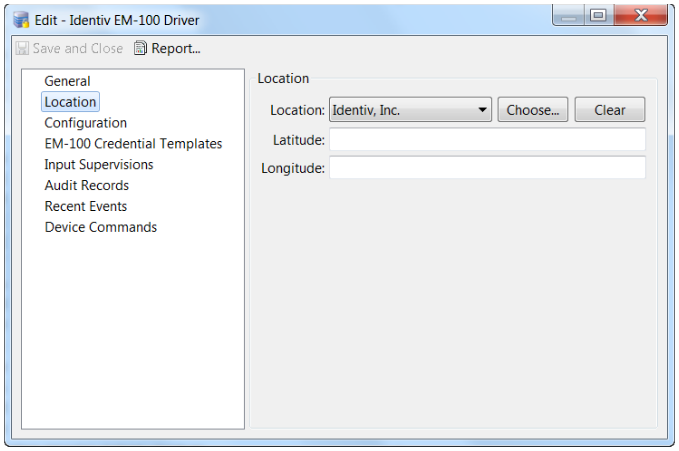
Address: localhost

☑ Enabled

Comments:

Name	Enter an appropriate name for this Identiv EM-100 driver.
Type	This read only field supplies the type for this driver.
Model	From the drop-down list, select the model of this EM-100 driver. Currently, there is only one driver model so this field need not be used.
Parent	This read-only field provides the relationship of this driver to other drivers: parent or child.
Site	This read-only field is populated with the current site under which this driver appears in the Hardware Tree.
Address	Check the Enabled box if the address of this driver has been placed on line.
Comments	(optional) Enter any comments describing or giving details for this driver.

Driver Location Property Page



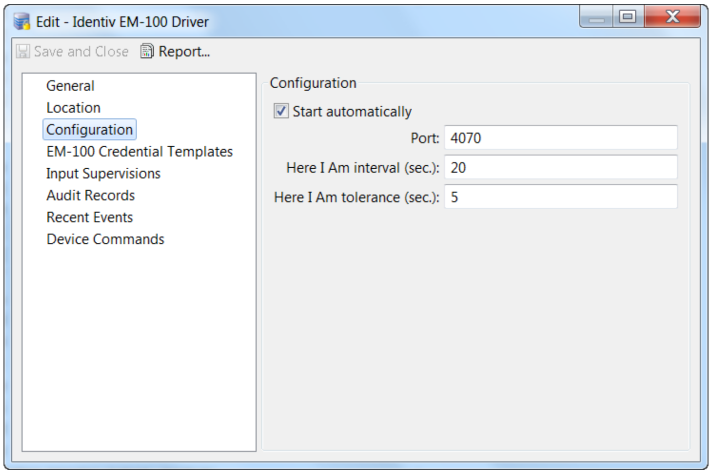
Location: Identiv, Inc.

Latitude:

Longitude:

Location	From the drop-down list, select one of the pre-defined locations or click **Choose** to create and select a new location. For more on this, see the "Viewing Doors and Devices by Location" section on page 5-7.
Latitude	(Optional) Enter the latitude where this driver is placed. If this driver is attached to a NTP server, the latitude and longitude are automatically populated.
Longitude	(Optional) Enter the longitude where this driver is placed. If this driver is attached to a NTP server, the latitude and longitude are automatically populated.

Driver Configuration Page



☑ Start automatically

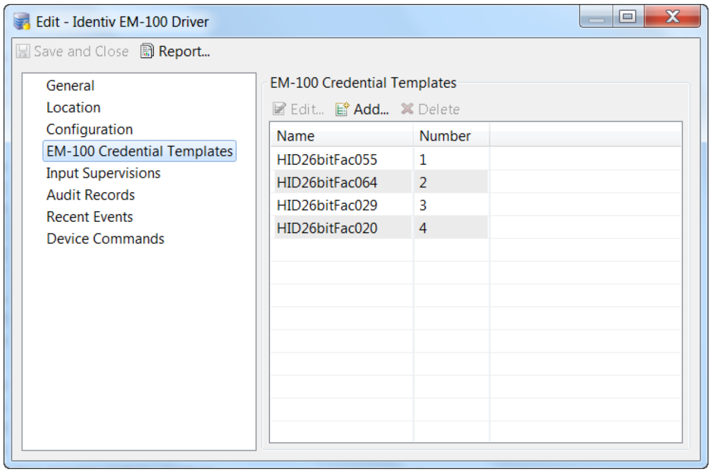
Port: 4070

Here I Am interval (sec.): 20

Here I Am tolerance (sec.): 5

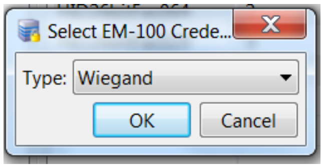
Start Automatically	Check this box to indicate that the driver is automatically started whenever ICPAM server is started. The default is checked (enabled).
Port	Enter the port used by this driver and its associated controllers. The default port is **4070**.
How am I interval	(optional) Enter the interval (in seconds) used to ascertain whether the controller is working properly or not. If this interval is surpassed, the system waits the amount of time specified in the How am I tolerance value, then issues an error message. The default is **20** seconds.
How am I tolerance	(optional) Enter the value in seconds beyond which the interval is tolerated before an error is issued.

Driver EM-100 Credential Templates Page



Name	Number
HID26bitFac055	1
HID26bitFac064	2
HID26bitFac029	3
HID26bitFac020	4

This table indicates the Credential Templates that are already defined for this driver. To add a new template, click **Add...** then enter the name of the new credential template in the Select EM-100 Credential dialog box.



Type: Wiegand

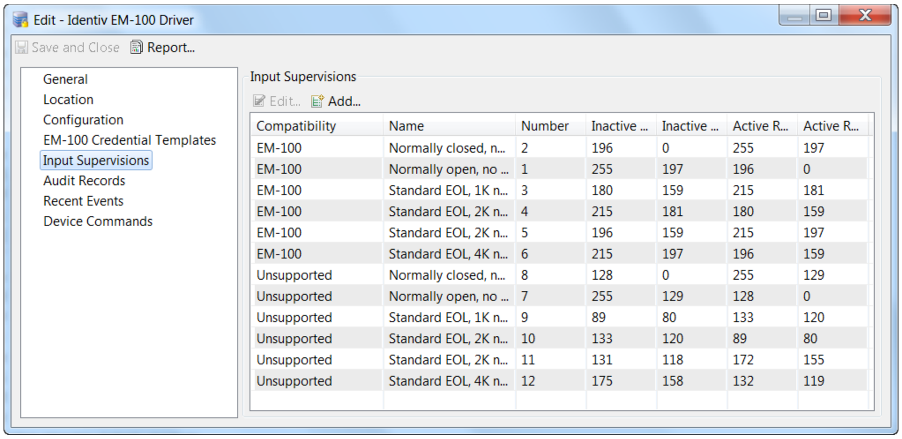
For more on creating credential templates, see Creating a Virtual Credential Template, page 8-17.

To edit an existing template, click to highlight one of the templates in the table then click **Edit...**

To remove one of the templates already assigned to this driver, click to highlight one of the templates from the table, then click **Delete**.

For more on defining credential templates, refer to Creating a Virtual Credential Template, page 8-17.

Driver Input Supervision Page

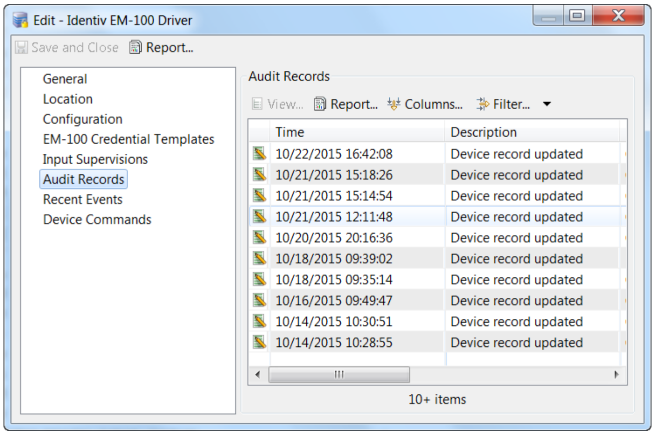


Compatibility	Name	Number	Inactive ...	Inactive ...	Active R...	Active R...
EM-100	Normally closed, n...	2	196	0	255	197
EM-100	Normally open, no ...	1	255	197	196	0
EM-100	Standard EOL, 1K n...	3	180	159	215	181
EM-100	Standard EOL, 2K n...	4	215	181	180	159
EM-100	Standard EOL, 2K n...	5	196	159	215	197
EM-100	Standard EOL, 4K n...	6	215	197	196	159
Unsupported	Normally closed, n...	8	128	0	255	129
Unsupported	Normally open, no ...	7	255	129	128	0
Unsupported	Standard EOL, 1K n...	9	89	80	133	120
Unsupported	Standard EOL, 2K n...	10	133	120	89	80
Unsupported	Standard EOL, 2K n...	11	131	118	172	155
Unsupported	Standard EOL, 4K n...	12	175	158	132	119

This table lists all input supervisions currently supported by this driver.

To add a new supervision, click **Add...** and make changes as required on the property sheet to define a new input supervision model. For more on this, refer to Device Configuration Properties, page 8-26.

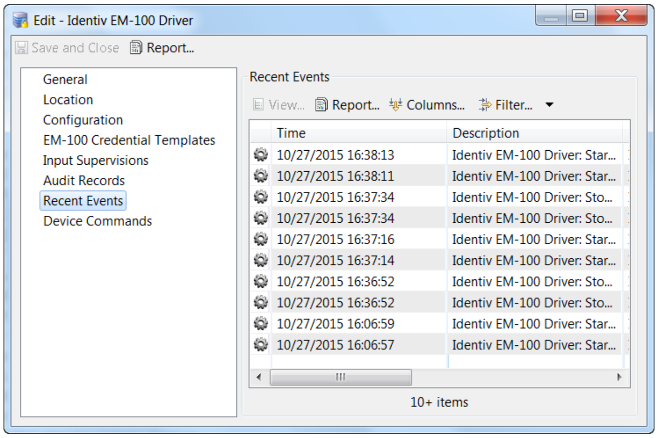
Driver Audit Records Page



Time	Description
10/22/2015 16:42:08	Device record updated
10/21/2015 15:18:26	Device record updated
10/21/2015 15:14:54	Device record updated
10/21/2015 12:11:48	Device record updated
10/20/2015 20:16:36	Device record updated
10/18/2015 09:39:02	Device record updated
10/18/2015 09:35:14	Device record updated
10/16/2015 09:49:47	Device record updated
10/14/2015 10:30:51	Device record updated
10/14/2015 10:28:55	Device record updated

This table displays a list of all audit records detected for this driver. For more on this, see Viewing Audit Records and Events for Personnel Records, page 9-9.

Driver Recent Events Page



Time	Description
10/27/2015 16:38:13	Identiv EM-100 Driver: Star...
10/27/2015 16:38:11	Identiv EM-100 Driver: Star...
10/27/2015 16:37:34	Identiv EM-100 Driver: Sto...
10/27/2015 16:37:34	Identiv EM-100 Driver: Sto...
10/27/2015 16:37:16	Identiv EM-100 Driver: Star...
10/27/2015 16:37:14	Identiv EM-100 Driver: Star...
10/27/2015 16:36:52	Identiv EM-100 Driver: Sto...
10/27/2015 16:36:52	Identiv EM-100 Driver: Sto...
10/27/2015 16:06:59	Identiv EM-100 Driver: Star...
10/27/2015 16:06:57	Identiv EM-100 Driver: Star...

10+ items

This table displays a list of all recent events recorded for this driver. See Viewing the Recent Events for a Device or Driver, page 5-15.

Controller and Driver Commands

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

- Access GW Driver Commands, page 6-46
- Gateway Controller Commands, page 6-47
- Physical Driver Commands, page 6-49
- Identiv EM-100 Driver Commands, page 6-49

Access GW Driver Commands

Table 6-1 Access GW Driver Commands

Command	Description
Apply Configuration Changes	Downloads configuration changes to all gateways. Changes made in ICPAM are inactive until applied with this command. See Applying Configuration Changes, page 6-30.
Apply Credential Changes	Downloads credential changes to all gateways. Credential changes made in ICPAM 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 Controllers, page 9-8.
Reset Gateway Password	Resets the password on all configured gateways. See Changing Gateway Passwords, page 6-35.
Bulk Image Upgrade	Downloads a firmware image to all gateways. See Upgrading Gateway Firmware Images Using ICPAM, page C-11.
Set NTP Server	Sets the Network Time Protocol (NTP) server for one or more gateways. See Changing the NTP Setting for Multiple Gateways, page C-6.
Run System Sanity Report	Creates a snapshot of potential inconsistencies in the system. See Generating a Gateway Driver System Sanity Report, page 5-16.
View Recent Events	View a list of recent events for all gateways. See Viewing the Recent Events for a Device or Driver, page 5-15.
New Gateway Controller	Creates a gateway configuration entry. See Creating Custom Gateway Configurations without Templates, page 6-2.
Edit	Opens the Edit window to revise the driver properties.
Disable	Disables all gateways, attached devices, and door configurations. See Disabling or Deleting a Door, page 7-15. Disabled Devices can be re-enabled.
Delete	Permanently removes the gateways and attached devices from the configuration. See Disabling or Deleting a Door, page 7-15.

Table 6-1 Access GW Driver Commands (continued)

Command	Description
View Device Status	Opens a new window containing the Status and Extended Status information. See Viewing Device and Door Status, page 5-10.
Show in Graphic Map Editor	Allows operators to add facility maps, and plot and organize devices for use in the Map viewer module. See Map Editor, page 12-50.

Gateway Controller Commands

Table 6-2 Gateway Controller Commands

Command	Description
Apply Configuration Changes	Downloads configuration changes to the specified controller. Changes made in ICPAM are inactive until applied with this command. **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 to Controllers, page 6-31.
Reload Gateway Configuration	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.
File Manager	Provides info of various files available on the gateway: • **Images**: Set of firmware images available on the gateway including status. See Upgrading Gateway Firmware Images Using ICPAM, page C-11 for more info. • **Core Files**: Core files for any core dumps that occurred on the Gateway. • **Log File**: List of debug log files. • **Technical Summary**: Technical data to assist in debugging issues. **Note** Each screen also provides options to download or upload the files.
Save As Gateway Template	Saves the gateway configuration as a template that can be used to configure additional devices. See Creating Custom Gateway Configurations without Templates, page 6-2 and Gateway Templates, page 5-23.
Clone Gateway	Creates an exact duplicate of a gateway configuration. See Cloning a Gateway Configuration, page 6-33.
Reset Gateway	Performs a soft reset of the gateway. See the *Cisco Physical Access Gateway User Guide* for more details.

Table 6-2 Gateway Controller Commands (continued)

Command	Description
Set Gateway Address	Replaces the gateway network configuration. **Note** The gateway network settings can also be configured using a direct connection to the Gateway. See the *Cisco Physical Access Gateway User Guide*. 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. To view the current settings, select the gateway in the Hardware Tree module. In the Extended Status screen (bottom right window), select the **Gateway Network Address** tab.
Format Gateway Flash	Erases and formats the gateway flash memory.
Replace Gateway	Replaces the current gateway with new gateway device. This command is active only when the device is disconnected from ICPAM (Unknown State). The command is used to replace a faulty device. See Replacing a Gateway, page 6-34.
Reset Gateway Password	Resets the password for the selected gateway device. You can also reset the passwords for multiple gateways. See Changing Gateway Passwords, page 6-35.
Download All Credentials	Downloads all credentials to the gateway to ensure all required data is correct. This command should be used only if a problem exists.
Credential Look up	Search for credentials on a gateway.
View Recent Events	View a list of recent events for the gateway. See Viewing the Recent Events for a Device or Driver, page 5-15.
New Module	Adds a new expansion module to the gateway configuration.
Edit	Opens the Edit window to revise the device properties.
Disable	Disables the device and all attached devices. Also disables any door configurations. See Disabling or Deleting a Door, page 7-15. Disabled devices can be re-enabled.
Delete	Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Door, page 7-15.
View Device Status	Opens a new window containing the Status and Extended Status information.
Show in Graphic Map Editor	Allows operators to add facility maps, and plot and organize devices for use in the Map Viewer module. See Map Editor, page 12-50.

Physical Driver Commands

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

Table 6-3 Physical Driver Commands

Command	Description
View Recent Events	View a list of recent events for the configured doors. See Viewing the Recent Events for a Device or Driver, page 5-15.
New Door	Creates a new door configuration. See Adding New Doors, page 7-2.
Edit	Opens the Edit window to revise the driver properties.
Disable	Disables the device and all attached devices. See Disabling or Deleting a Door, page 7-15. Disabled Devices can be re-enabled.
Delete	Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Door, page 7-15.
View Device Status	Opens a new window containing the Status and Extended Status information.
Show in Graphic Map Editor	Allows operators to add facility maps and plot and organize devices for use in the Map viewer module. See Map Editor, page 12-50.

Note If you run any gateway commands or door commands in the Door/Location-based Hardware module, all the related events are populated as Physical Driver commands.

Identiv EM-100 Driver Commands

To access the following commands, right-click on the Identiv EM-100 Driver icon in the Hardware Tree view.

Table 6-4 Identiv EM-100 Driver Commands

Command	Description
View Recent Events	View a list of recent events for the configured doors. See Viewing the Recent Events for a Device or Driver, page 5-15.
New Door	Creates a new door configuration. See Configuring Doors, page 7-1.
Edit	Opens the Edit window to revise the driver properties. The Identiv edit window includes the pages described in Identiv EM-100 Driver Property Sheets, page 6-40.
Disable	Disables the device and all attached devices. See Disabling or Deleting a Door, page 7-15. Disabled Devices can be re-enabled.
Delete	Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Door, page 7-15.

Table 6-4 Identiv EM-100 Driver Commands (continued)

Command	Description
View Device Status	Opens a new window containing the Status and Extended Status information.
Show in Graphic Map Editor	Allows operators to add facility maps and plot and organize devices for use in the Map viewer module. See Map Editor, page 12-50.

Note If you run any gateway commands or door commands in the Door/Location-based Hardware module, all the related events are populated as Physical Driver commands.

CHAPTER 7

Configuring Doors

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

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 Controller Configurations, page 5-1 for more information.

Contents

Adding New Doors

This section includes the following information.

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

Adding Custom Doors

Complete the following instructions to add a door.

Step 1 Verify that the gateway for the door configuration exists in the Hardware Tree module.

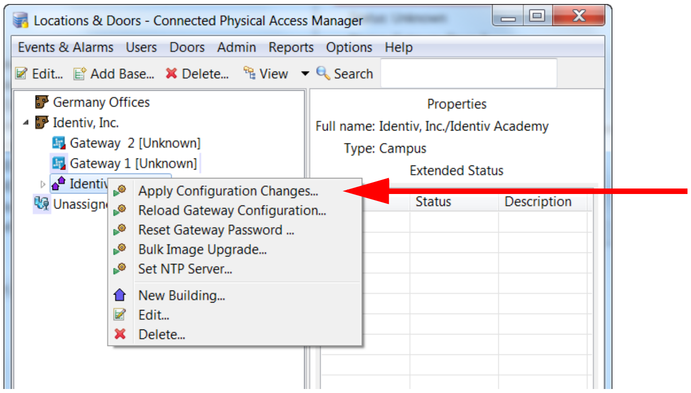
Step 2 Right click on the required driver.

Step 3 From the drop-down menu, select the **New Door...** option.

Step 4 Select a name and location for this new door.

Step 5 Apply the door configuration changes.

In the Door/Location-based Hardware module, right-click a location and select **Apply Configuration Changes**. Only gateways in the Up state are updated.



Full name: Identiv, Inc./Identiv Academy

Type: Campus

Step 6 Once the door appears, right click on it and select **Edit**.

The Door Edit property sheets appear as described in Door Property Sheets, page 7-26.

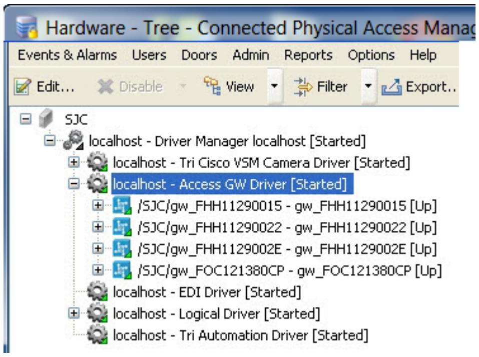
Step 7 Make changes to the properties on these pages as required.

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.

Note This procedure can only be used for adding doors to a gateway.

Step 1 Verify that the gateway for the door configuration exists in the Hardware Tree module.



SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [Started]
localhost - Access GW Driver [Started]
/SJC/gw_FHH11290015 - gw_FHH11290015 [Up]
/SJC/gw_FHH11290022 - gw_FHH11290022 [Up]
/SJC/gw_FHH1129002E - gw_FHH1129002E [Up]
/SJC/gw_FOC121380CP - gw_FOC121380CP [Up]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - Tri Automation Driver [Started]

If the gateway is not already configured, use one of the following methods:

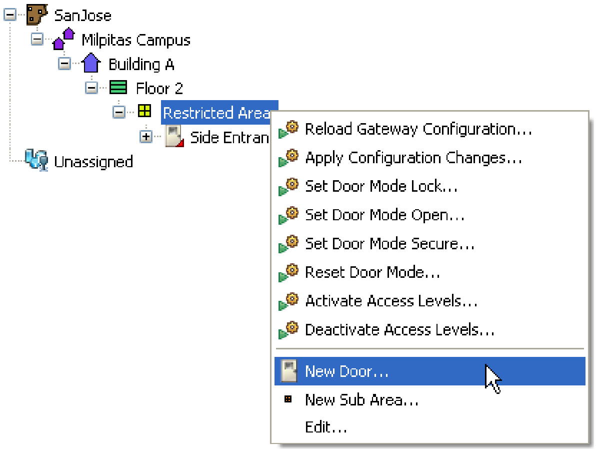
- Creating Custom Gateway Configurations without Templates, page 6-2
- Configuring Gateways Using Existing Templates, page 6-7

Note See also Provisioned (Pre-Populated) vs. Discovered Controller Configurations, page 5-1.

Step 2 Create a new door:

a. Select **Door/Location-based Hardware** from the Doors menu.

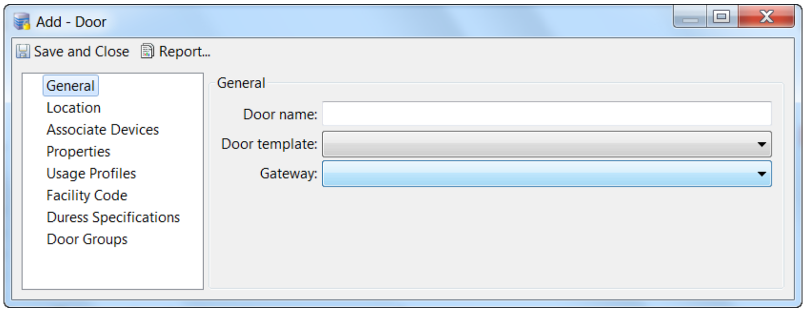
b. Right-click a location and select **New Door**.



Note If the location does not exist, refer to Creating the Location Map, page 5-8 for more information.

Tip You can also create a door in the Hardware Tree module. Right-click on the physical driver and select **New Door**.

Step 3 Enter the **General** settings:

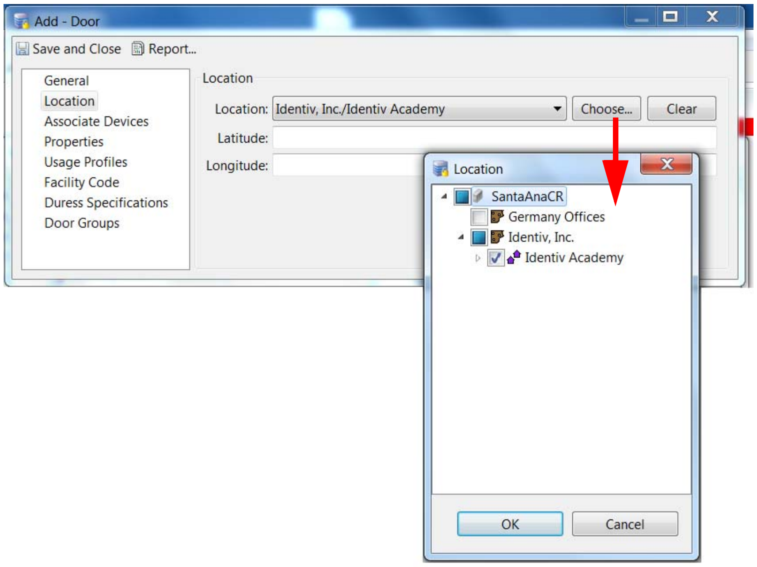


- **Door name**: enter a descriptive name for the door configuration.
- **Door Template**: select the door template that contains the correct set of door devices. See Configuring Door Templates, page 8-2 for more information.
- **Gateway**: select the gateway used for the door configuration. The devices in the door template are assigned to the gateway interfaces.

Step 4 Select a location for the door.

a. Select the **Location** submenu.

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



Location: Identiv, Inc./Identiv Academy

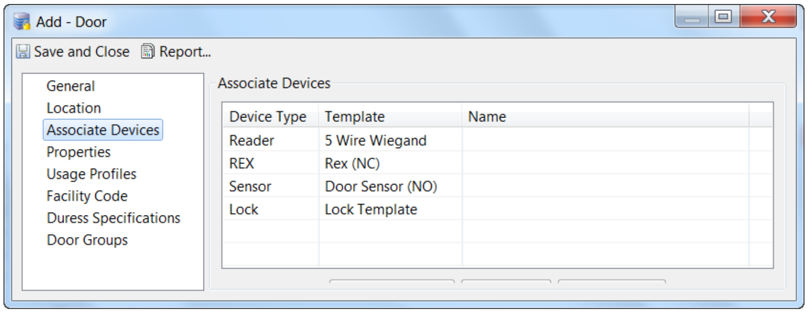
Note If you create a new door in a specific location in the Door/Location-based Hardware module, the door location takes the location of the hirerarchy as a default location.

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

c. 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 controller. If the gateway includes expansion modules, you can also choose an interface from a Reader, Input, or Output module.

a. Select the **Associate Devices** submenu.

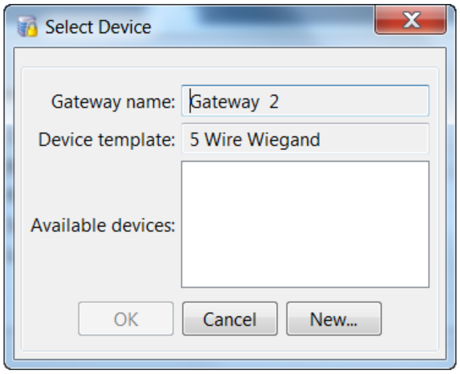


Associate Devices

Device Type	Template	Name
Reader	5 Wire Wiegand	
REX	Rex (NC)	
Sensor	Door Sensor (NO)	
Lock	Lock Template	

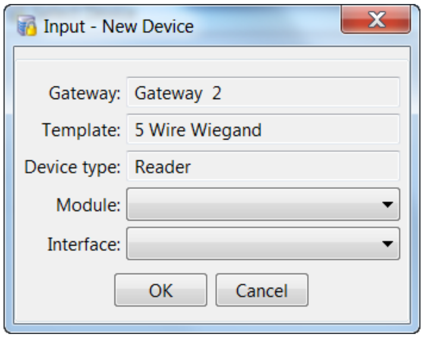
b. Highlight a device (such as a reader) and click the **Associate Device** button.

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



Gateway name: Gateway 2
Device template: 5 Wire Wiegand
Available devices:

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



Gateway: Gateway 2
Template: 5 Wire Wiegand
Device type: Reader
Module:
Interface:

Note 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.

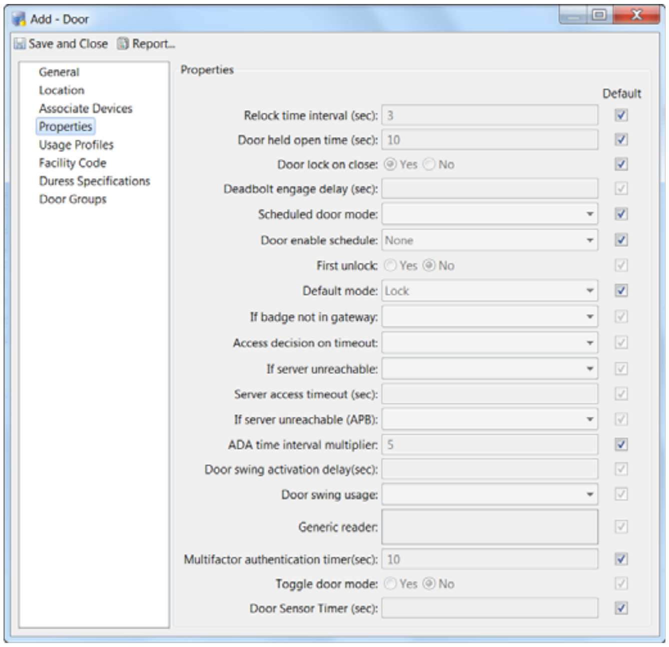
e. Click **OK**.

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** submenu.

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



Add - Door

Save and Close | Report...

General
Location
Associate Devices
Properties
Usage Profiles
Facility Code
Duress Specifications
Door Groups

Properties

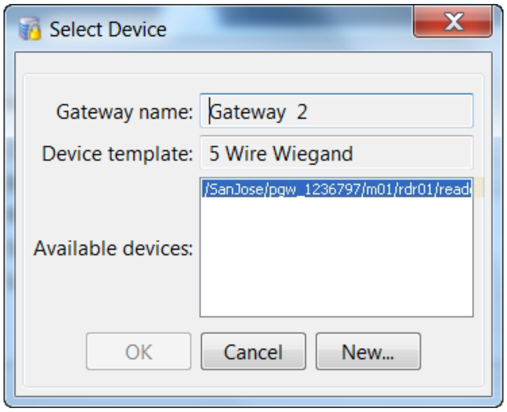
		Default
Relock time interval (sec):	3	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:		☑
Door enable schedule:	None	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:		☑
Access decision on timeout:		☑
If server unreachable:		☑
Server access timeout (sec):		☑
If server unreachable (APB):		☑
ADA time interval multiplier:	5	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

See Device Configuration Properties, page 8-26 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.



Select Device

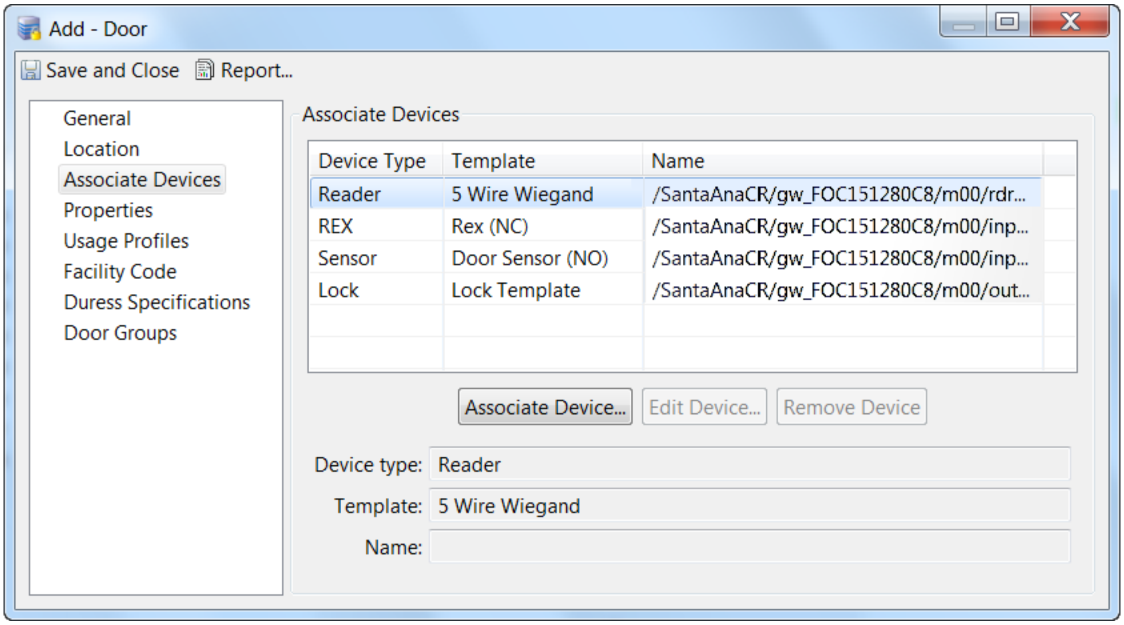
Gateway name: Gateway 2

Device template: 5 Wire Wiegand

Available devices: /SanJose/pgw_1236797/m01/rdr01/read

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

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



Add - Door

Save and Close | Report...

Associate Devices

Device Type	Template	Name
Reader	5 Wire Wiegand	/SantaAnaCR/gw_FOC151280C8/m00/rdr...
REX	Rex (NC)	/SantaAnaCR/gw_FOC151280C8/m00/inp...
Sensor	Door Sensor (NO)	/SantaAnaCR/gw_FOC151280C8/m00/inp...
Lock	Lock Template	/SantaAnaCR/gw_FOC151280C8/m00/out...

Device type: Reader

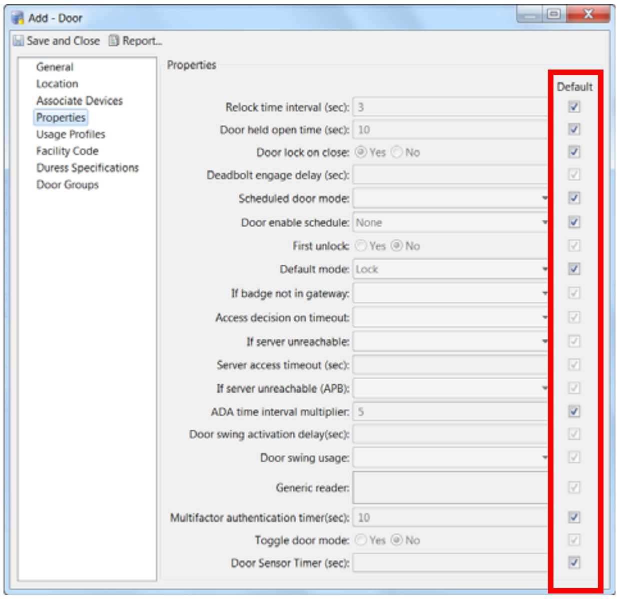
Template: 5 Wire Wiegand

Name:

Step 9 (Optional) Modify the Properties for the door.

a. Click the **Properties** submenu.

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



Add - Door

Save and Close | Report...

Properties

		Default
Relock time interval (sec):	3	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:		☑
Door enable schedule:	None	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:		☑
Access decision on timeout:		☑
If server unreachable:		☑
Server access timeout (sec):		☑
If server unreachable (APB):		☑
ADA time interval multiplier:	5	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

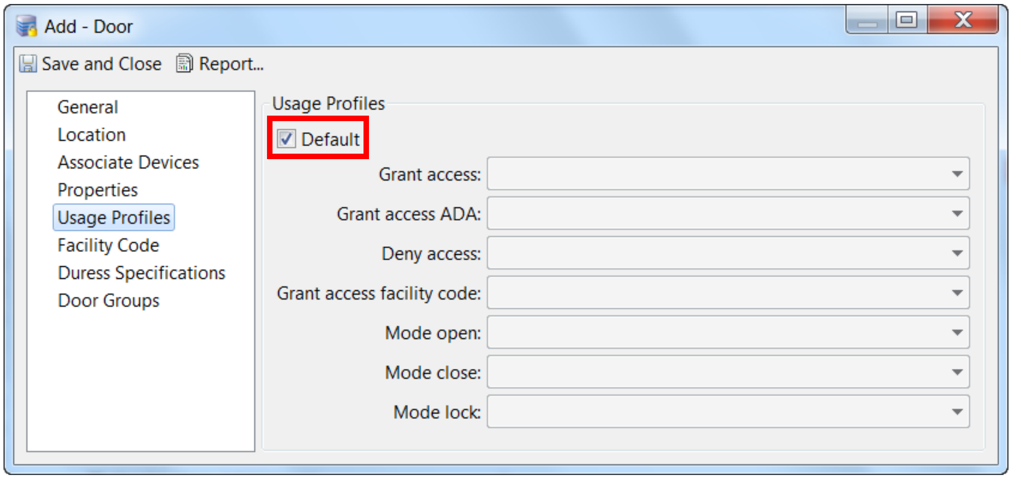
For more information see the following:

- Chapter 5, "Understanding Controller and Door Configurations"
- Door Configuration Properties, page 8-24

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

a. Click the **Usage Profiles** submenu.

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



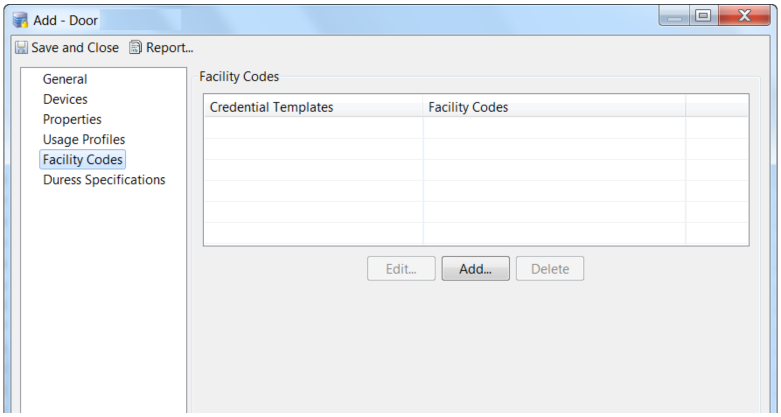
Note If there are two doors created from a gateway,the reader LED profile changes does not apply to the second door.

See Configuring Reader LED Profiles, page 8-21 for more information.

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

a. Click the **Facility Code Information** submenu.

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**.

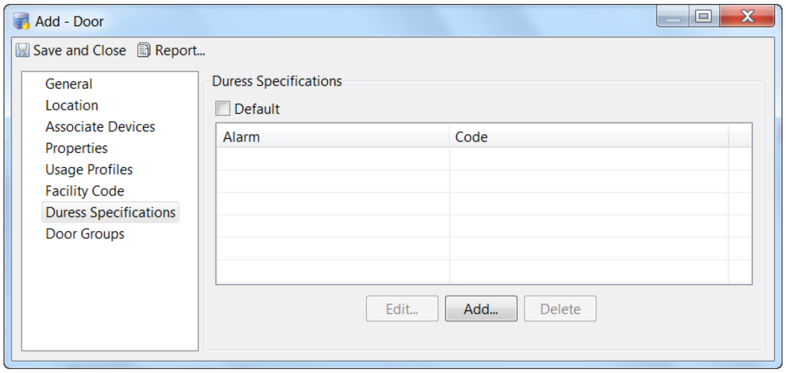
Note By default a door can have 26BitWeigandCT credential with 456,123 facility codes.

See Configuring Credential Templates, page 8-13 for more information.

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

a. Click the **Duress Specification** submenu.

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.

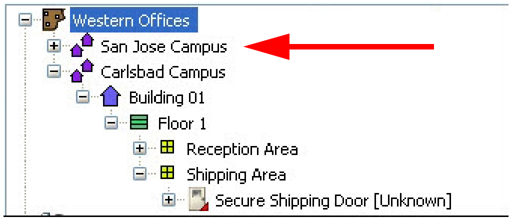
To Delete an alarm:

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.

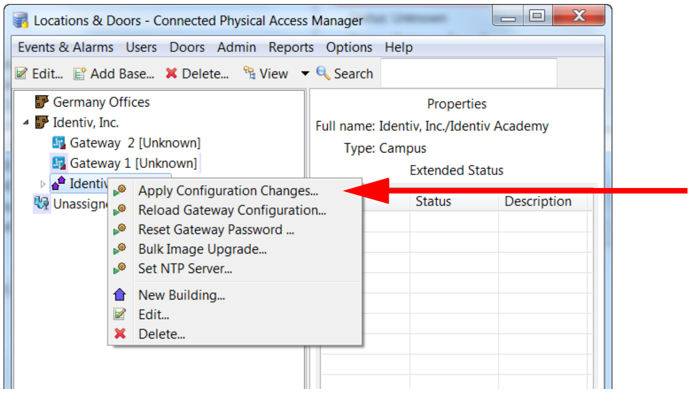
The door configuration is displayed as a child of the selected location.



Note The door is also listed under the Physical Driver in the Hardware Tree module.

Step 14 Apply the door configuration changes.

In the Door/Location-based Hardware module, right-click a location and select **Apply Configuration Changes**. Only gateways in the Up state are updated.



Full name: Identiv, Inc./Identiv Academy
Type: Campus

For more information, see TipThe names of all hardware elements are editable, including drivers, controllers, expansion modules, and door devices., page 7-12

Related Documentation

- Provisioned (Pre-Populated) vs. Discovered Controller Configurations, page 5-1
- Creating Custom Gateway Configurations without Templates, page 6-2
- Configuring Gateways Using Existing Templates, page 6-7

Modifying Door Configurations

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

- Modifying Doors and Devices in the Hardware Tree View, page 7-10
- Modifying Devices in the Door/Location-based Hardware Module, page 7-11

Modifying Doors and Devices in the Hardware Tree View

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

Step 1 Select **Hardware Tree** from the Doors menu.

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.

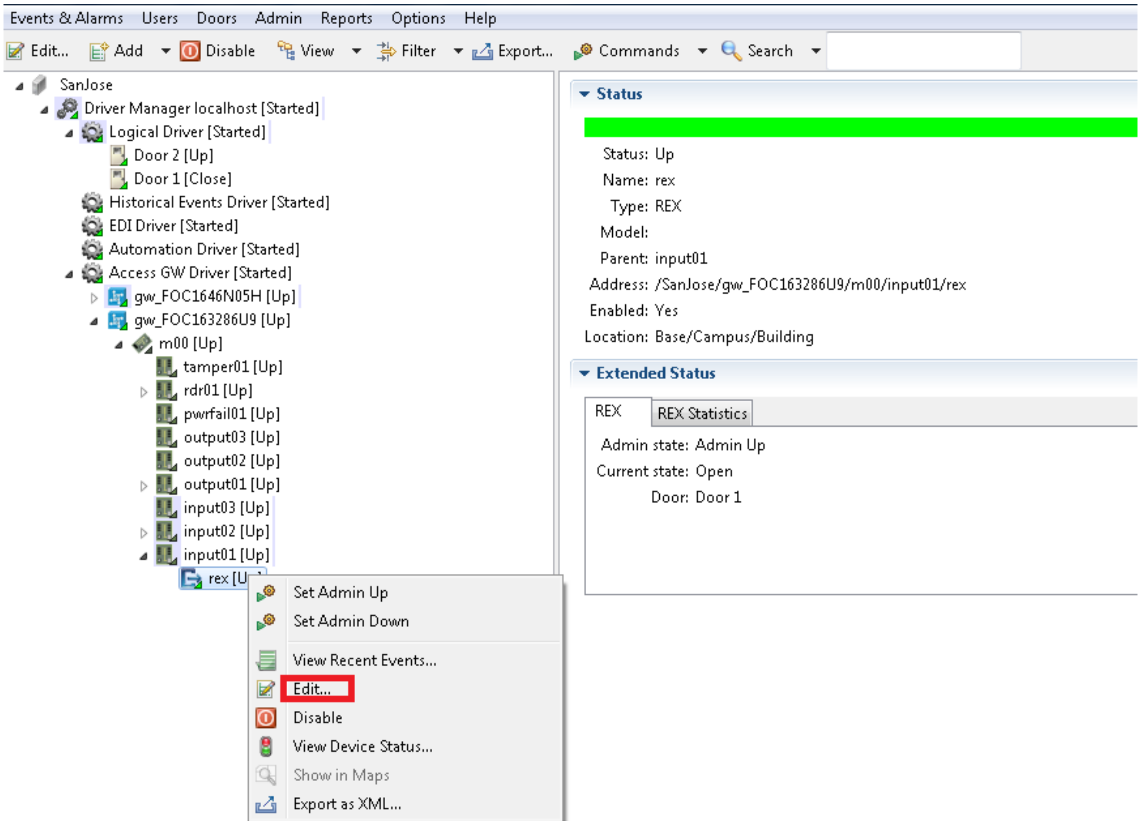
Step 3 Click **Properties** in the device window and edit the settings as necessary.

For more on the property sheets that are available for this operation, refer to Door Property Sheets, page 7-26.

Step 4 To override the template settings, deselect the **Default** check box to activate the field. For field descriptions, see Door Configuration Properties, page 8-24 and Device Configuration Properties, page 8-26.

Step 5 Download the configuration changes to the controller. Changes do not take effect until downloaded.

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



Status: Up
Name: rex
Type: REX
Model:
Parent: input01
Address: /SanJose/gw_FOC163286U9/m00/input01/rex
Enabled: Yes
Location: Base/Campus/Building

Admin state: Admin Up
Current state: Open
Door: Door 1

Modifying Devices in the Door/Location-based Hardware Module

In the Door/Location-based Hardware module, you can edit all attributes of a door configuration, including device properties and the location map.

For instructions to modify the location map, see Creating the Location Map, page 5-8.

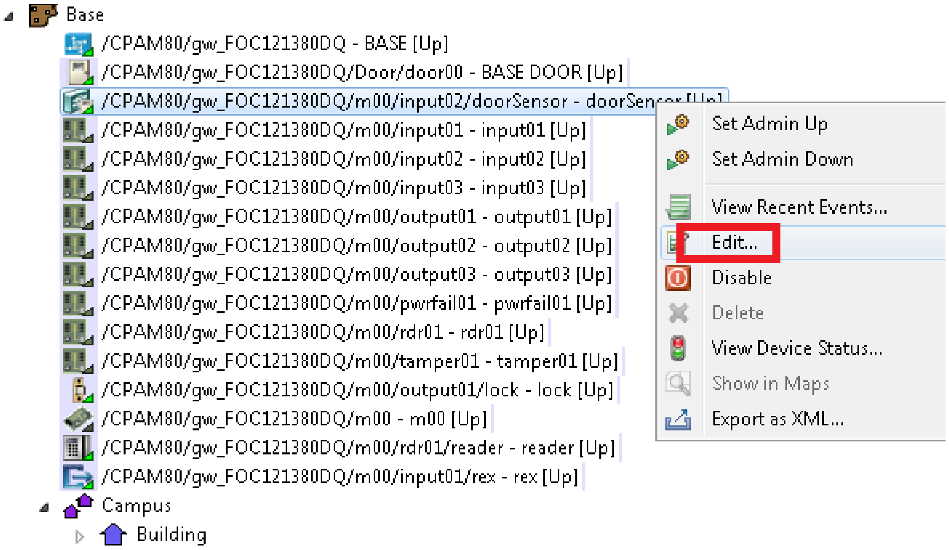
Step 1 In the Door/Location-based Hardware module, expand the location tree to display the door configuration or a specific device.

Step 2 Right-click on the door or device name and select **Edit**, as shown in Figure 7-2.

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

For more information on the pages in the Door Edit window, refer to Door Property Sheets, page 7-26.

Figure 7-2 Edit Menu for a Device in the Hardware Tree Location View


Base
/CPAM80/gw_FOC121380DQ - BASE [Up]
/CPAM80/gw_FOC121380DQ/Door/door00 - BASE DOOR [Up]
/CPAM80/gw_FOC121380DQ/m00/input02/doorSensor - doorSensor [Up]
/CPAM80/gw_FOC121380DQ/m00/input01 - input01 [Up]
/CPAM80/gw_FOC121380DQ/m00/input02 - input02 [Up]
/CPAM80/gw_FOC121380DQ/m00/input03 - input03 [Up]
/CPAM80/gw_FOC121380DQ/m00/output01 - output01 [Up]
/CPAM80/gw_FOC121380DQ/m00/output02 - output02 [Up]
/CPAM80/gw_FOC121380DQ/m00/output03 - output03 [Up]
/CPAM80/gw_FOC121380DQ/m00/pwrfail01 - pwrfail01 [Up]
/CPAM80/gw_FOC121380DQ/m00/rdr01 - rdr01 [Up]
/CPAM80/gw_FOC121380DQ/m00/tamper01 - tamper01 [Up]
/CPAM80/gw_FOC121380DQ/m00/output01/lock - lock [Up]
/CPAM80/gw_FOC121380DQ/m00 - m00 [Up]
/CPAM80/gw_FOC121380DQ/m00/rdr01/reader - reader [Up]
/CPAM80/gw_FOC121380DQ/m00/input01/rex - rex [Up]
Campus
Building
Set Admin Up
Set Admin Down
View Recent Events...
Edit...
Disable
Delete
View Device Status...
Show in Maps
Export as XML...

Step 3 Select a submenu and edit the settings as necessary. To override the template properties, deselect the Default check box to activate the field.

For more information on the pages in the Door Edit window, refer to Door Property Sheets, page 7-26.

Step 4 Download the configuration changes. For more on this process, see Applying Configuration Changes to Controllers, page 7-12.

Tip The names of all hardware elements are editable, including drivers, controllers, expansion modules, and door devices.

Applying Configuration Changes

Changes made to a door or device configuration in ICPAM are inactive until applied to the controller. You can apply the configuration changes to a specific controller, to all controllers, or to all controllers in a location. Applying a configuration downloads the revised configuration file to the controller.

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

This section includes the following information.

- Applying Configuration Changes to Controllers, page 7-12
- Configuration Management in Provisioned vs. Discovered Configurations, page 7-14

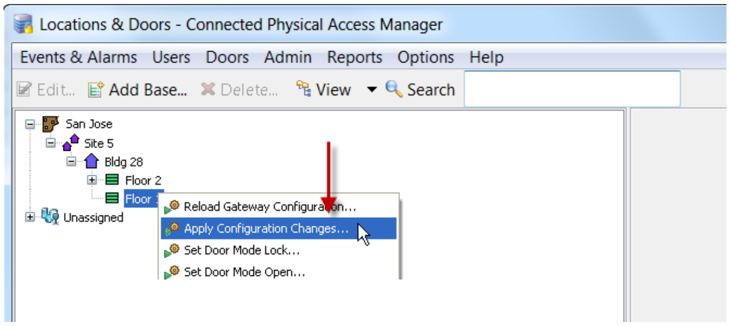
Applying Configuration Changes to Controllers

You can download the configuration to controllers using either the **Hardware Tree** or **Door/Location-based Hardware** modules.

Applying Configuration Changes in the Hardware Tree Module

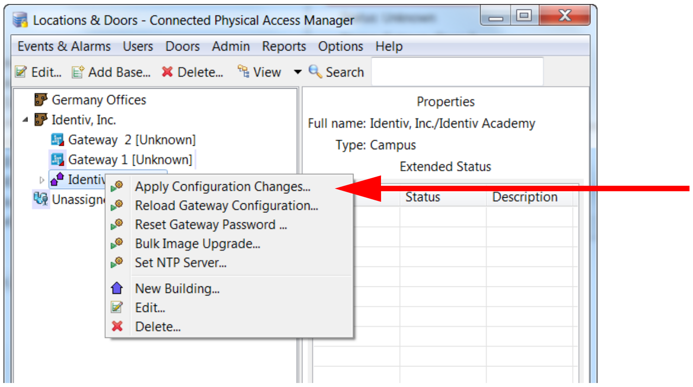
Select **Apply Configuration Changes** on the controller or GW Driver or on a specific controller.

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



or

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



Full name: Identiv, Inc./Identiv Academy

Type: Campus

Note Controllers must be in the Up state, signified by a green triangle in the icon. A dark green triangle means configuration changes that have not been applied. See Understanding Device Status Colors, page 5-13.

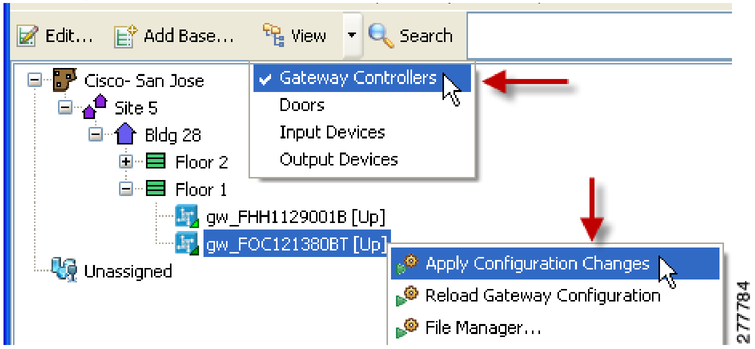
Applying Configuration Changes in the Door/Location-based Hardware Module

Select **Apply Configuration Changes** on the affected controller or on a location.

Specific Controller:

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.

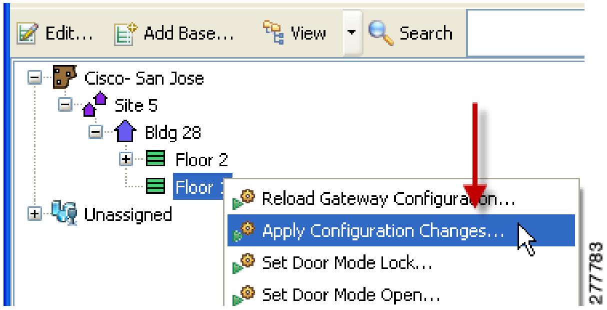


or

Multiple Controllers:

a. Right-click a location icon.

b. Select **Apply Configuration Changes**.



Note Controllers must be in the Up state, signified by a green triangle in the icon. A dark green triangle means configuration changes that have not been applied. See Understanding Device Status Colors, page 5-13.

Configuration Management in Provisioned vs. Discovered Configurations

- In a Provisioned configuration, the configuration is entered before the controller is brought online and the configuration is automatically downloaded when the controller 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 controller is added to the network before a configuration is created. ICPAM automatically creates a basic configuration containing the serial numbers of the controller and any expansion modules. Any subsequent configuration changes must be downloaded using one of the methods described in this section.
- If a controller 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 Controller Configurations, page 5-1 for more information.

Disabling or Deleting a Door

Disabling a device or door configuration deactivates the item, but does not remove it from the ICPAM 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 physical 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. Identiv 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 7-15
- Deleting Devices and Doors, page 7-16
- Enabling a Device or Door, page 7-18

Disabling a Device or Door

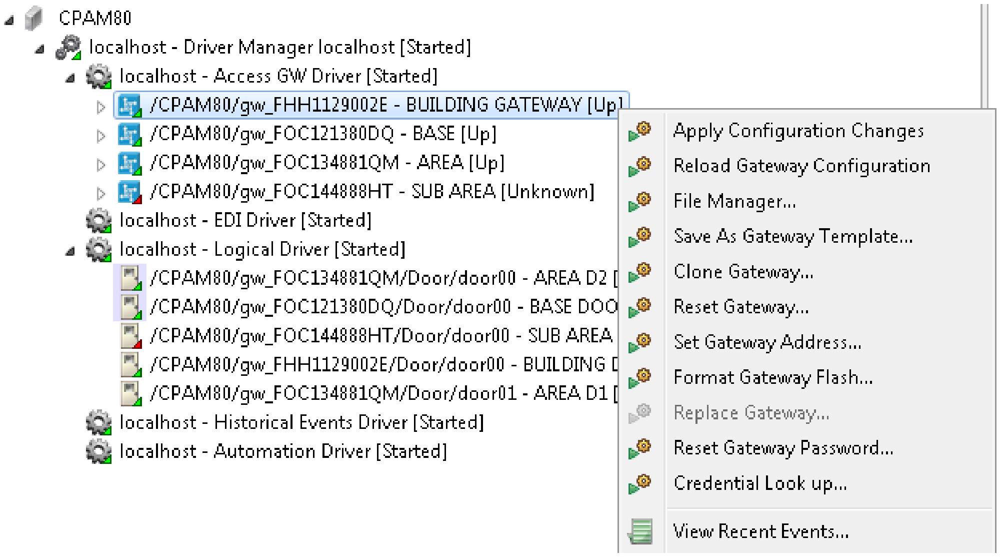
To disable a device or door, right-click the item and select **Disable** from the drop down menu.

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

Step 1 Select either **Hardware Tree** or **Door/Location-based Hardware** from the Doors menu.

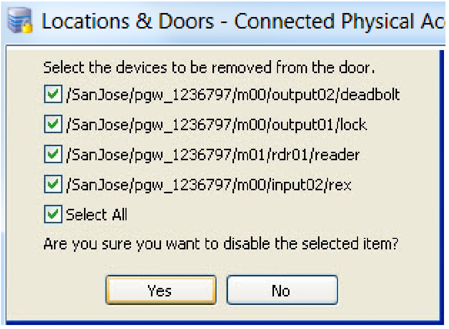
Step 2 Right-click a controller, door configuration, or other device, and select **Disable** (Figure 7-3).

Figure 7-3 Disabling a Device Using the Hardware Tree Module


CPAM80
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/CPAM80/gw_FHH1129002E - BUILDING GATEWAY [Up]
/CPAM80/gw_FOC121380DQ - BASE [Up]
/CPAM80/gw_FOC134881QM - AREA [Up]
/CPAM80/gw_FOC144888HT - SUB AREA [Unknown]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
/CPAM80/gw_FOC134881QM/Door/door00 - AREA D2 [
/CPAM80/gw_FOC121380DQ/Door/door00 - BASE DOO
/CPAM80/gw_FOC144888HT/Door/door00 - SUB AREA
/CPAM80/gw_FHH1129002E/Door/door00 - BUILDING [
/CPAM80/gw_FOC134881QM/Door/door01 - AREA D1 [
localhost - Historical Events Driver [Started]
localhost - Automation Driver [Started]
Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
Clone Gateway...
Reset Gateway...
Set Gateway Address...
Format Gateway Flash...
Replace Gateway...
Reset Gateway Password...
Credential Look up...
View Recent Events...

- **Disabling a device**: removes the controller 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 7-4. Select the devices to be disabled, or check the box for **Select All**, and then click **Yes**.

Figure 7-4 Confirmation Warning When Disabling a Door Configuration



Locations & Doors - Connected Physical Ac

Select the devices to be removed from the door.

☑ /SanJose/pgw_1236797/m00/output02/deadbolt
☑ /SanJose/pgw_1236797/m00/output01/lock
☑ /SanJose/pgw_1236797/m01/rdr01/reader
☑ /SanJose/pgw_1236797/m00/input02/rex
☑ Select All

Are you sure you want to disable the selected item?

Step 3 Download the configuration changes to the controller. Changes do not take effect until downloaded.

Step 4 (Optional) To delete a device, controller or door configuration, see Deleting Devices and Doors, page 7-16.

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 ICPAM 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 Identiv 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.

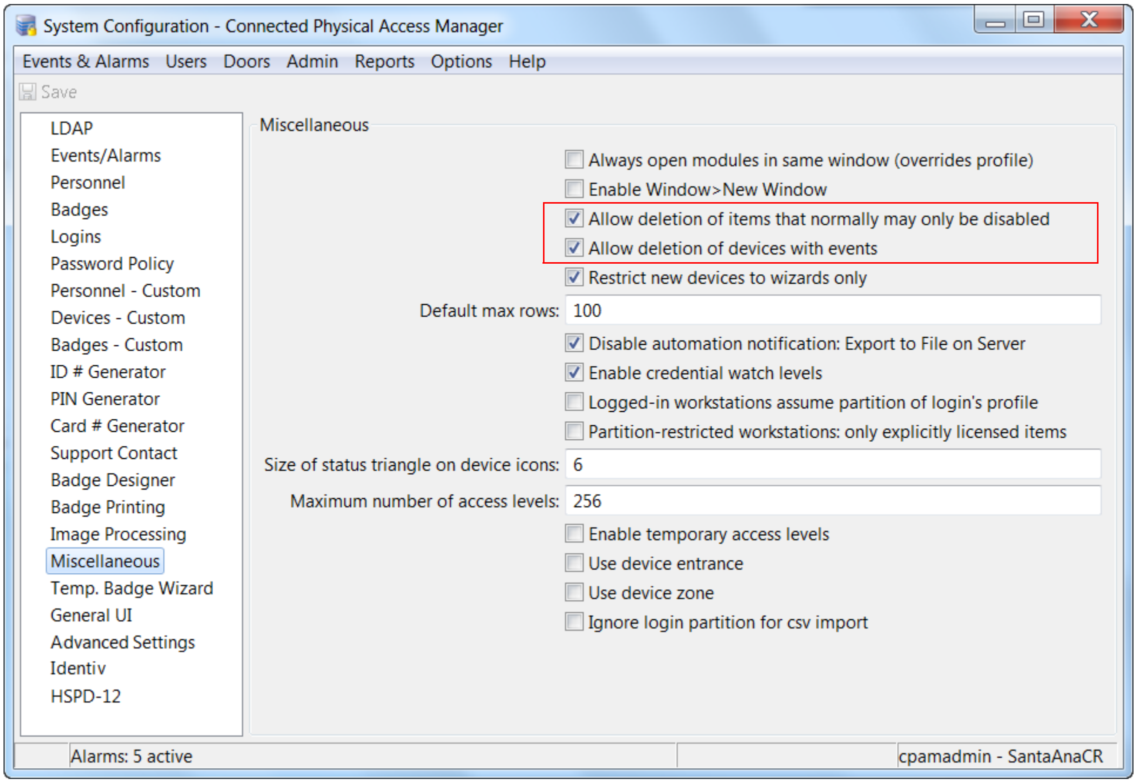
- Deleting a Controller, page 6-34
- Enabling the Delete Options, page 7-17
- Deleting a Device, page 7-18

Enabling the Delete Options

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

Step 2 Select the **Miscellaneous** submenu, as shown in Figure 7-5.

Figure 7-5 Device Delete Options in The Admin Module: System Configuration



System Configuration - Connected Physical Access Manager

Miscellaneous

□ Always open modules in same window (overrides profile)
□ Enable Window>New Window
☑ Allow deletion of items that normally may only be disabled
☑ Allow deletion of devices with events
☑ Restrict new devices to wizards only
Default max rows: 100
☑ Disable automation notification: Export to File on Server
☑ Enable credential watch levels
□ Logged-in workstations assume partition of login's profile
□ Partition-restricted workstations: only explicitly licensed items
Size of status triangle on device icons: 6
Maximum number of access levels: 256
□ Enable temporary access levels
□ Use device entrance
□ Use device zone
□ Ignore login partition for csv import

Alarms: 5 active
cpamadmin - SantaAnaCR

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 ICPAM application to enable the changes (select Logout from the Options menu). The Delete menu does not appear in ICPAM until you log out and log back in.

Deleting a Device

To delete a device, do the following:

Step 1 Enable the Delete functions, as described in Enabling the Delete Options, page 7-17.

Step 2 Disable the device, as described in Disabling a Device or Door, page 7-15.

Step 3 Select **All Devices** from the **Filter** menu to display one or more disabled devices.

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

Step 5 Select **Yes** to confirm.

Step 6 Download the changes to the controller, as described in For more on this process, see Applying Configuration Changes to Controllers, page 7-12.

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.

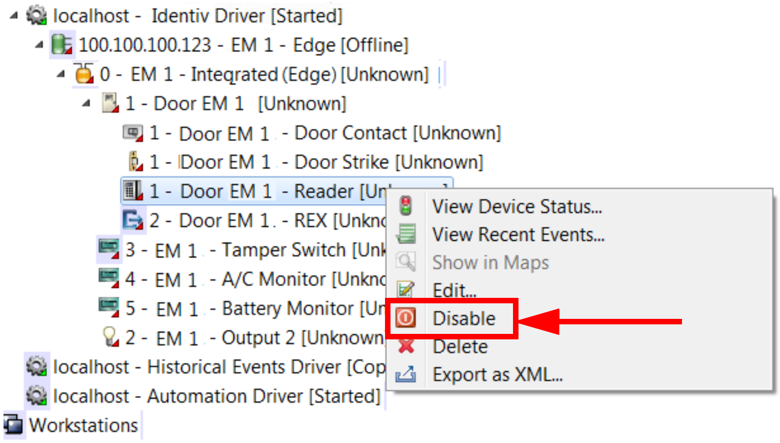
Disable and Enable a Device and Door: Example

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

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.


localhost - Identiv Driver [Started]
100.100.100.123 - EM 1 - Edge [Offline]
0 - EM 1 - Integrated (Edge) [Unknown]
1 - Door EM 1 [Unknown]
1 - Door EM 1 - Door Contact [Unknown]
1 - Door EM 1 - Door Strike [Unknown]
1 - Door EM 1 - Reader [Un
2 - Door EM 1 - REX [Unkno
3 - EM 1 - Tamper Switch [Unk
4 - EM 1 - A/C Monitor [Unkno
5 - EM 1 - Battery Monitor [Ur
2 - EM 1 - Output 2 [Unknown
localhost - Historical Events Driver [Cop
localhost - Automation Driver [Started]
Workstations
View Device Status...
View Recent Events...
Show in Maps
Edit...
Disable
Delete
Export as XML...

Step 2 Accept or modify the device settings.

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

Step 3 Re-enable the door.

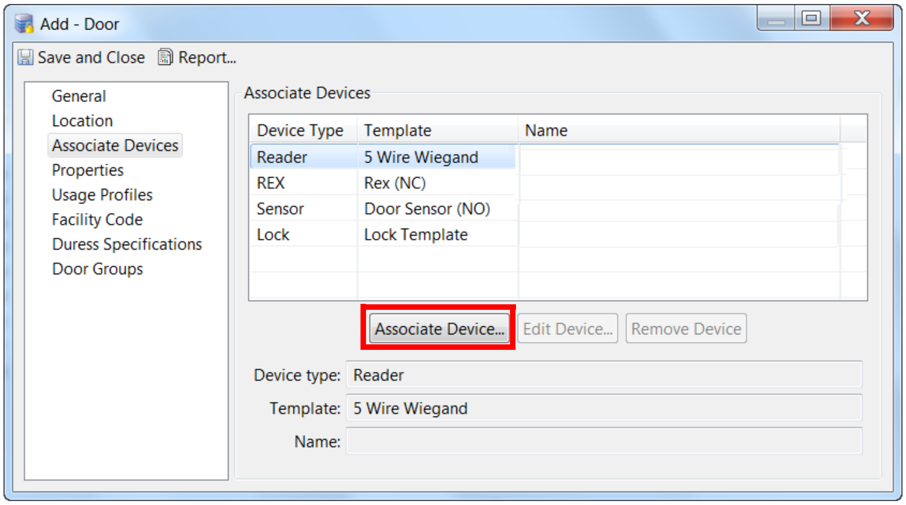
Note To re-enable a door, you must reassociate the device with the door.

a. Select **All Devices** from the Filter menu to display one or more disabled devices.

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

c. Select the **Associate Devices** submenu, as shown in the example to the right.

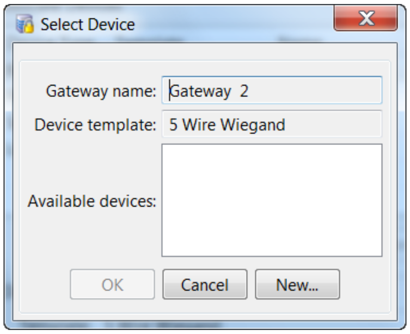
d. Highlight a device (such as reader) and click **Associate Device**.



Device Type	Template	Name
Reader	5 Wire Wiegand	
REX	Rex (NC)	
Sensor	Door Sensor (NO)	
Lock	Lock Template	

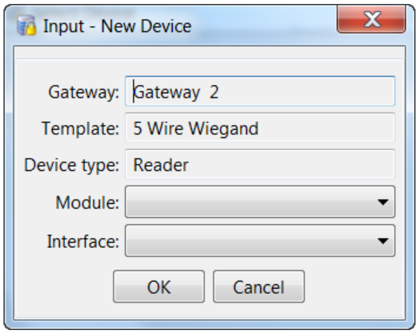
Device type: Reader
Template: 5 Wire Wiegand
Name:

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



Gateway name: Gateway 2
Device template: 5 Wire Wiegand
Available devices:

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



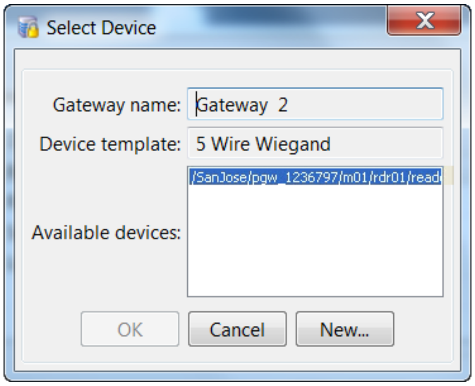
Gateway: Gateway 2
Template: 5 Wire Wiegand
Device type: Reader
Module:
Interface:

g. Click **OK**.

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

a. Highlight the interface from the list in the **Available Device** field. This list includes the available unused ports from the controller and any expansion modules attached to the controller.

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



Gateway name: Gateway 2

Device template: 5 Wire Wiegand

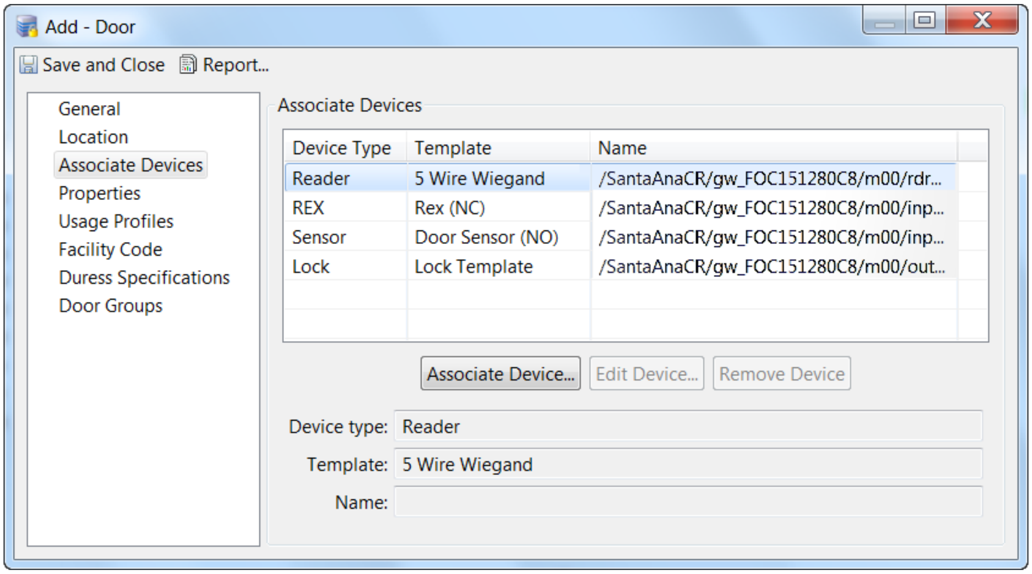
Available devices: /SanJose/pgw_1236797/m01/rdr01/read

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.



Device Type	Template	Name
Reader	5 Wire Wiegand	/SantaAnaCR/gw_FOC151280C8/m00/rdr...
REX	Rex (NC)	/SantaAnaCR/gw_FOC151280C8/m00/inp...
Sensor	Door Sensor (NO)	/SantaAnaCR/gw_FOC151280C8/m00/inp...
Lock	Lock Template	/SantaAnaCR/gw_FOC151280C8/m00/out...

Device type: Reader

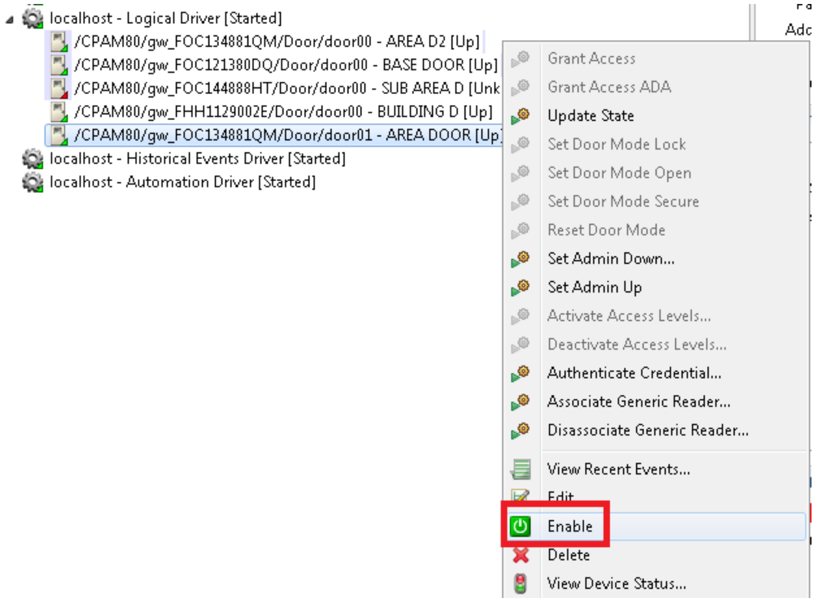
Template: 5 Wire Wiegand

Name:

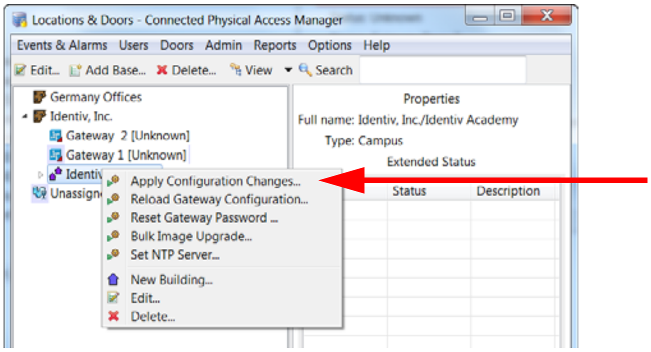
Step 6 Re-enable the door.

Note The device should appear again under the door.

Step 7 Right-click the door name and select **Enable**.


localhost - Logical Driver [Started]
/CPAM80/gw_FOC134881QM/Door/door00 - AREA D2 [Up]
/CPAM80/gw_FOC121380DQ/Door/door00 - BASE DOOR [Up]
/CPAM80/gw_FOC144888HT/Door/door00 - SUB AREA D [Unk
/CPAM80/gw_FHH1129002E/Door/door00 - BUILDING D [Up]
/CPAM80/gw_FOC134881QM/Door/door01 - AREA DOOR [Up]
localhost - Historical Events Driver [Started]
localhost - Automation Driver [Started]
Adc
Grant Access
Grant Access ADA
Update State
Set Door Mode Lock
Set Door Mode Open
Set Door Mode Secure
Reset Door Mode
Set Admin Down...
Set Admin Up
Activate Access Levels...
Deactivate Access Levels...
Authenticate Credential...
Associate Generic Reader...
Disassociate Generic Reader...
View Recent Events...
Edit
Enable
Delete
View Device Status...

Step 8 To apply the door configuration changes, right-click a location or controller and select **Apply Configuration Changes**. Only controllers in the Up state are updated.


Locations & Doors - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
Germany Offices
Identiv, Inc.
Gateway 2 [Unknown]
Gateway 1 [Unknown]
Identiv
Unassign
Properties
Full name: Identiv, Inc./Identiv Academy
Type: Campus
Extended Status
Status
Description
Apply Configuration Changes...
Reload Gateway Configuration...
Reset Gateway Password ...
Bulk Image Upgrade...
Set NTP Server...
New Building...
Edit...
Delete...

For more information, see Applying Configuration Changes to Controllers, page 7-12.

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 12-34), Global I/O, Quick Launch, Map and Access Policies (Configuring Access Policies, page 11-2).

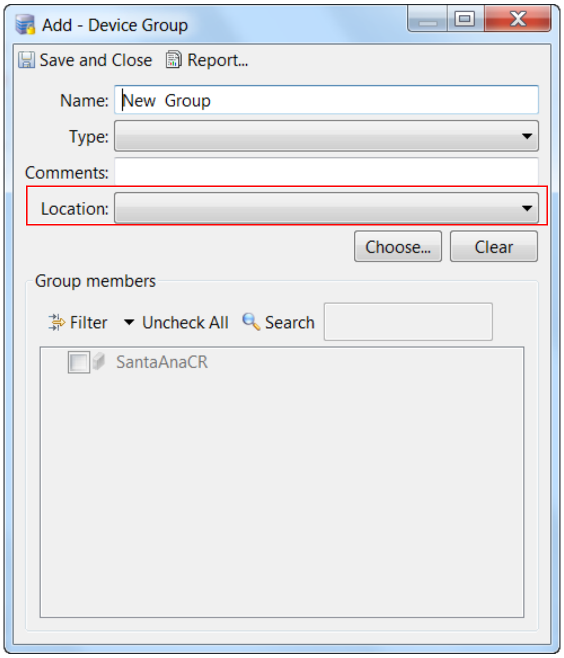
For example, a device group for all lobby doors can be created, and then specified in an access policy. Users assigned to that access policy will only have access to doors in that device group.

Device Groups in ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (see Logins Settings, page 17-10), 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 7-6).

Figure 7-6 Device Groups based on hierarchical Location



Name: New Group
Type:
Comments:
Location:

□ SantaAnaCR

- 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.

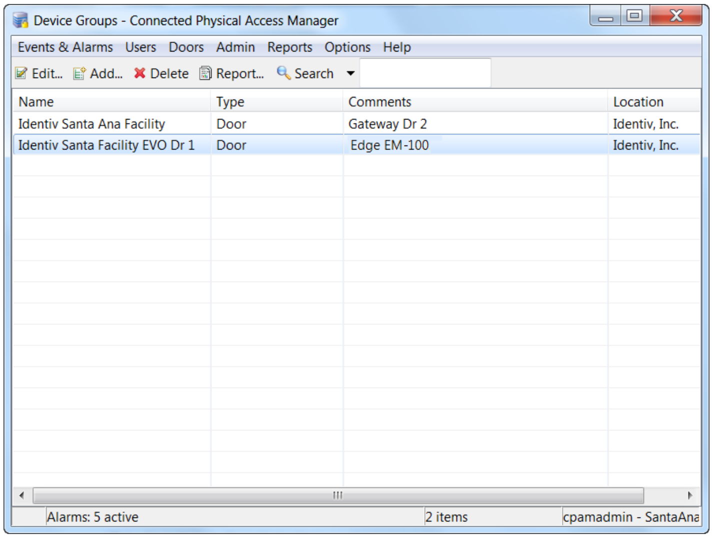
Note These points are applicable only when the profile enhancement feature is set in the System Configuration of ICPAM. Otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

To configure device groups, do the following:

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

The Device Groups - Physical Access Manager window opens, as shown in Figure 7-7.

Figure 7-7 Device Groups Window



Name	Type	Comments	Location
Identiv Santa Ana Facility	Door	Gateway Dr 2	Identiv, Inc.
Identiv Santa Facility EVO Dr 1	Door	Edge EM-100	Identiv, Inc.

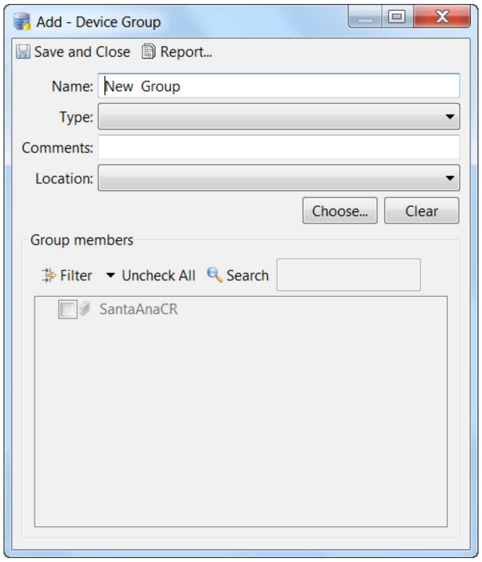
Step 2 Add or edit a device group.

- 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 resulting window (Figure 7-8), enter a **Name** for the device group.

Figure 7-8 Add Device Group Window



Name: New Group

Step 4 From the **Type** drop-down list select any one of the following devices types:

- Door
- Controller
- Module
- Reader

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

Step 5 Select the 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 7-7).

Adding an Expansion Module in an Existing Setup

An expansion module can be added in one of the following modes:

- Auto-discover
- Provision

Auto-Discover

To add an expansion module, connect the module with the controller using a CAN bus. The gateway automatically recognizes the new module, and enables the device in the Hardware Tree module under the controller. It is necessary to provide external power to power up the expansion module (12 V DC or 24 V DC).

Provision Mode

To add an expansion module in the provision mode, follow the below steps:

Step 1 Right click the controller and select **New Module** from the menu.

Step 2 Select one of the modules (Input/Output/Reader) from the drop-down list.

Step 3 If you select the reader module, select the reader connection mode (either one or two readers).

Step 4 Enter a valid serial number and then click Finish. This physically connects the module with gateway using a CAN bus. It is necessary to provide an external power source to power up the expansion module.

Step 5 Execute apply configuration changes command to make module active.

Replacing an Expansion Module

To replace an expansion module in an existing setup, follow the below steps:

Step 1 Remove the module that is to be replaced and disable it.

Step 2 Execute the replace module command with a valid serial number, and enable it.

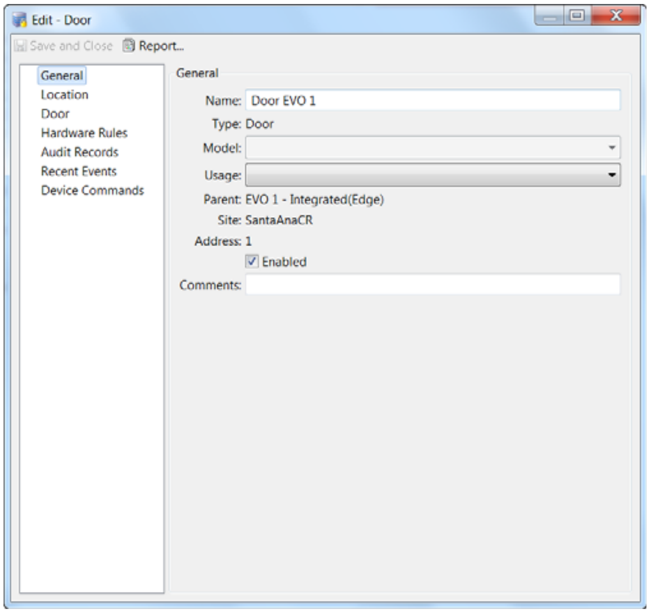
Step 3 Execute the **Reload Gateway Configuration** command to update the correct serial number.

Door Property Sheets

When you edit a door's properties, either through Modifying Doors and Devices in the Hardware Tree View, page 7-10 or Modifying Devices in the Door/Location-based Hardware Module, page 7-11, a window resembling Figure 7-9 on page 7-26 or Figure 7-10 on page 7-27 appears, depending on which controller you are using, EM-100 or Cisco Gateway.

There are seven pages in this window, each of which is detailed in this section.

Figure 7-9 EM-100 Edit Door Property Sheet

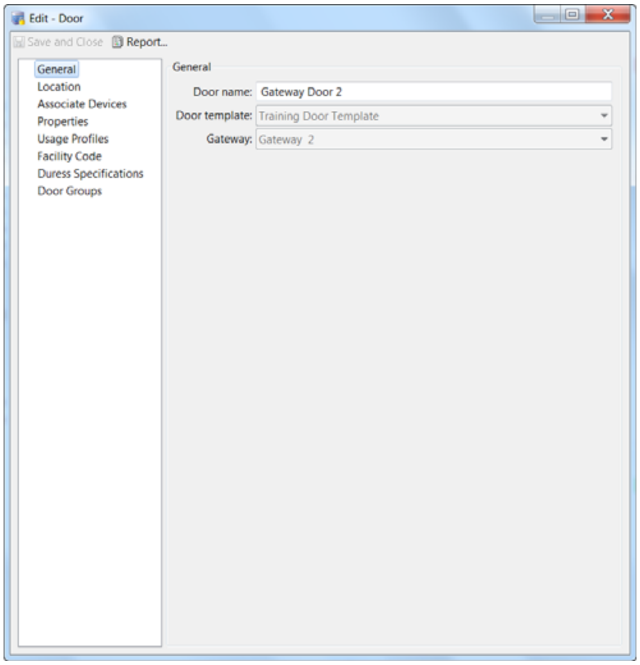


Name: Door EVO 1
Type: Door
Model:
Usage:
Parent: EVO 1 - Integrated(Edge)
Site: SantaAnaCR
Address: 1
☑ Enabled
Comments:

If the door is attached to an EM-100 controller these property sheets will appear:

- Door Edit General Property Sheet
- Door Edit Location Property Sheet
- Door Edit Door Property Sheet
- Door Edit Hardware Rules Property Sheet
- Door Edit Audit Records Property Sheet
- Door Edit Recent Events Property Sheet
- Door Edit Device Commands Property Sheet

Figure 7-10 Gateway Edit Door Property Sheets



Door name: Gateway Door 2

Door template: Training Door Template

Gateway: Gateway 2

If the door is attached to the Cisco gateway, these property sheets will appear:

- Door Edit General Property Sheet
- Door Edit Location Property Sheet
- Door Edit Associate Devices Property Sheet
- Door Edit Properties Property Sheet
- Door Edit Usage Profiles Property Sheet
- Door Edit Facility Code Property Sheet
- Door Edit Duress Specifications Property Sheet
- Door Edit Door Groups Property Sheet

General Door Property Sheet

When you select the **General** tab, a page like Figure 7-9 or Figure 7-10 appears.

Depending on which controller you are using, this page includes the following fields:

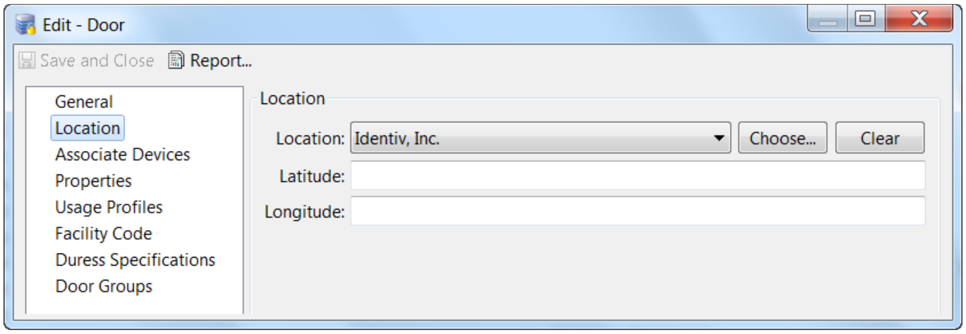
Table 7-1 Gateway Door General Page

Field	Description
Door	Enter a name for this door.
Door template	This field indicates the door template selected for this door. For more on door templates, refer to Configuring Door Templates, page 8-2.
Gateway	This read-only field indicates the gateway to which to door is attached.

Field	Description
Door	Enter a name for this door.
Type	This read-only field indicates the type of device described by this property sheet. This is normally a door.
Model	This read-only field indicates the model of EM-100 this door is.
Usage	From the drop-down list, select the option that describes the usage for this door. The options are: • **Door** (default) • **Elevator** • **Portal** • **Turnstile** • **Vehicle Gate**
Parent	This read-only field indicates this door's place in the system's hierarchy.
Site	This read-only field indicates the site where this door resides.
Address	This read-only field indicates the door's address.
Enabled	Check this box to indicate that this door is active and ready to communicate with the host.
Comments	If required, enter information about this door.

Location Door Property Sheet

When you select the **Location** tab from the Gateway door property sheet, a page like this appears:



Location: Identiv, Inc.

Latitude:

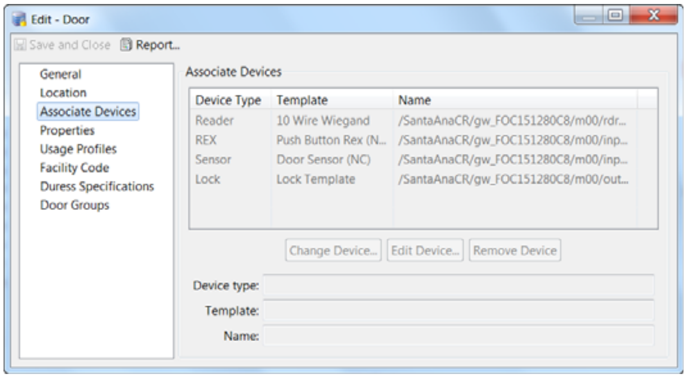
Longitude:

This page includes the following fields:

Field	Description
Location	Select the location (area) where this door is located. If needed, click **Choose...** and navigate to the correct location. Only those locations previously defined for this system appear in this option list. For more on creating location, refer to Creating the Location Map, page 5-8.
Latitude	If needed, enter the latitude of this door.
Longitude	If needed, enter the longitude of this door.

Associate Devices Door Property Sheet

When you select the **Associate Devices** tab from the Gateway door property sheet, a page like this appears:



Associate Devices

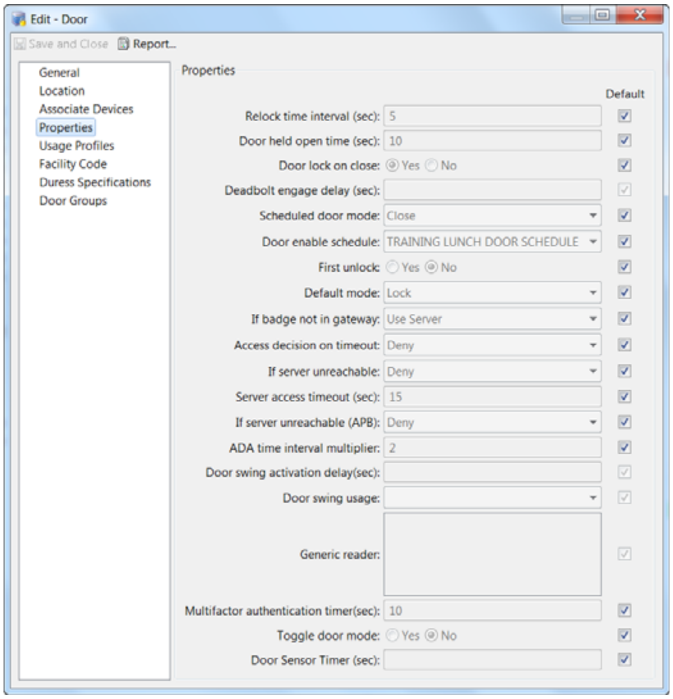
Device Type	Template	Name
Reader	10 Wire Wiegand	/SantaAnaCR/gw_FOC151280C8/m00/rdr...
REX	Push Button Rex (N...	/SantaAnaCR/gw_FOC151280C8/m00/inp...
Sensor	Door Sensor (NC)	/SantaAnaCR/gw_FOC151280C8/m00/inp...
Lock	Lock Template	/SantaAnaCR/gw_FOC151280C8/m00/out...

Device type:
Template:
Name:

This page includes a table of all devices currently associated with this door. For instructions on how to associate new devices with this door, refer to Configuring Doors, page 7-1.

Properties Door Property Sheet

When you select the **Properties** tab from the Gateway door property sheet, a page like this appears:



Properties

		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

The fields appearing on this property sheet include:

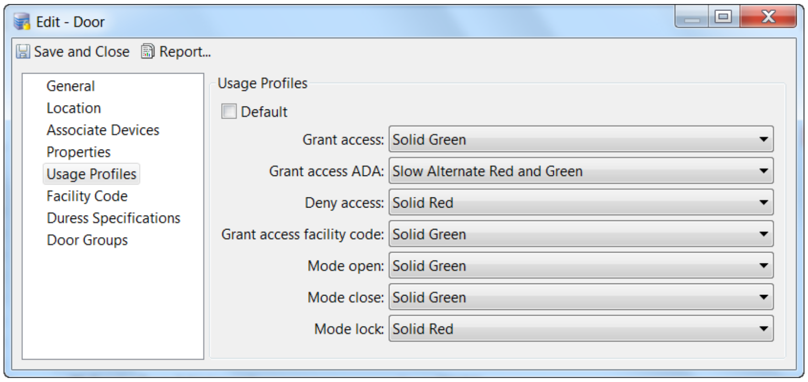
Field	Description
Default	Check the box to the left of each value to assume the default for that door property. Uncheck the box to specify a custom value for this door property.
Relock interval time (sec)	The number of seconds to keep the door open after an access request is granted (grant access).
Door held open time (sec)	The number of seconds before the Door Help Open alarm is generated.
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.
Deadbolt engage delay (sec)	The delay (in seconds) after a door closes until the deadbolt is applied.
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.

Field	Description
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 to add or modify the available door schedules.
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.
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.
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 ICPAM. See Using Local (Controller) Credentials if Network Communication is Lost, 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 from one of these options: • **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.

Field	Description
Toggle door mode	Click the **Yes** radio button to enable toggle door mode. Click **No** to disable toggling.
Door sensor timer	Specify in seconds the time the door sensor is enabled.

Usage Profiles Door Property Sheet

For Gateway doors, click the **Usage Profiles** tab to display the usage profiles door property sheet.



Edit - Door

Save and Close Report...

- General
- Location
- Associate Devices
- Properties
- Usage Profiles
- Facility Code
- Duress Specifications
- Door Groups

Usage Profiles

□ Default

Grant access: Solid Green

Grant access ADA: Slow Alternate Red and Green

Deny access: Solid Red

Grant access facility code: Solid Green

Mode open: Solid Green

Mode close: Solid Green

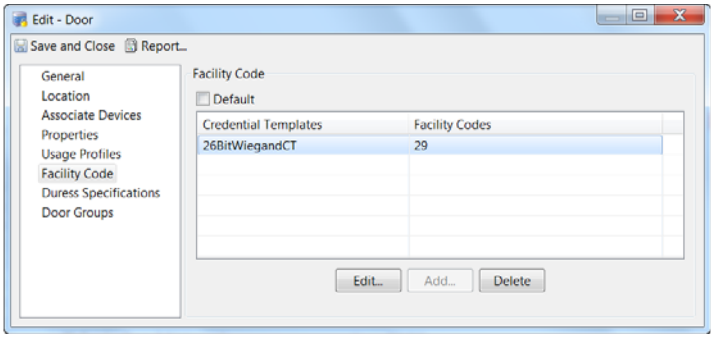
Mode lock: Solid Red

The fields on this property sheet include:

Field	Description
Default	Check the box to the left of each value to assume the default for that door property. Uncheck the box to specify a custom value for this door property.
Grant access	Select a color and pattern for the grant access state applicable to this door.
Grant access ADA	Select a color and pattern for the grant access ADA state applicable to this door.
Deny access	Select a color and pattern for the deny access state applicable to this door.
Grant access facility code	Select a color and pattern for the grant access facility code applicable to this door.
Mode open	Select a color and pattern for the mode open state applicable to this door.
Mode close	Select a color and pattern for the mode closed state applicable to this door.
Mode lock	Select a color and pattern for the mode lock state applicable to this door.

Facility Code Door Property Sheet

When you select the **Facility Code** tab on a Cisco Gateway door property sheet, a page like this appears:



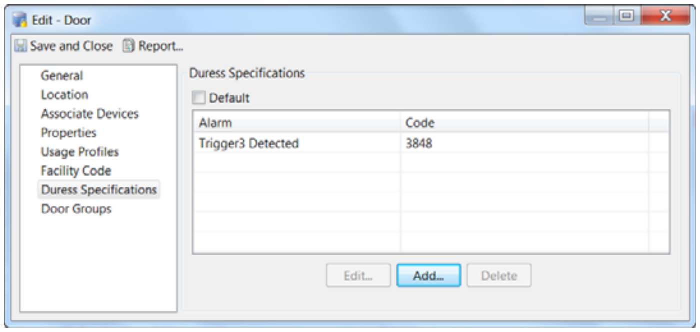
☐ Default

Credential Templates	Facility Codes
26BitWiegandCT	29

Field	Description
Default	Check this box to indicate that this door always uses the default facility code. By default a door can have 26BitWeigandCT credential with 456,123 facility codes.
Table	This table indicates the facility codes and their associated credential templates already assigned to this door.
Edit...	Click to highlight an existing entry in the table then click this button to edit an existing entry.
Add...	When active, click this button to create a new facility code.
Delete	Select an entry from the table, then click this button to delete the entry from the table.

Duress Specifications Door Property Sheet

If you select the **Duress Specification** tab from the Gateway door property sheet, a page like this appears:



☐ Default

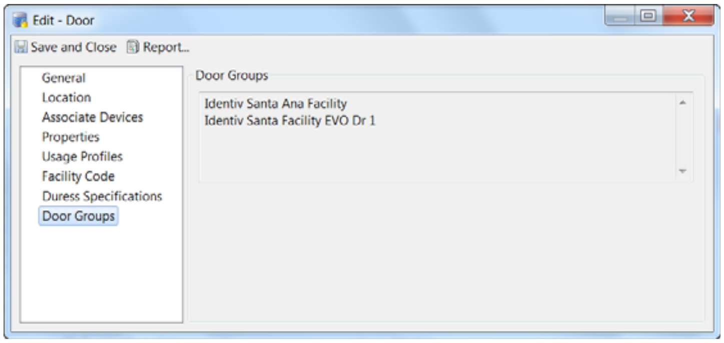
Alarm	Code
Trigger3 Detected	3848

Field	Description
Default	Check this box to indicate that the default duress code is the only one acceptable.
Window	Displays a list of the currently accepted and defined duress specifications.

Field	Description
Edit...	Click to highlight a listed duress specification then click this button. The edit duress specification dialog box appears.
Add...	Click to display a duress specification dialog box and enter a duress code.
Delete	Click to highlight a listed duress specification then click this button to delete the specification.

Door Groups Door Property Sheet

When you select the **Door Groups** tab from the Gateway door property sheet, a page like this appears:



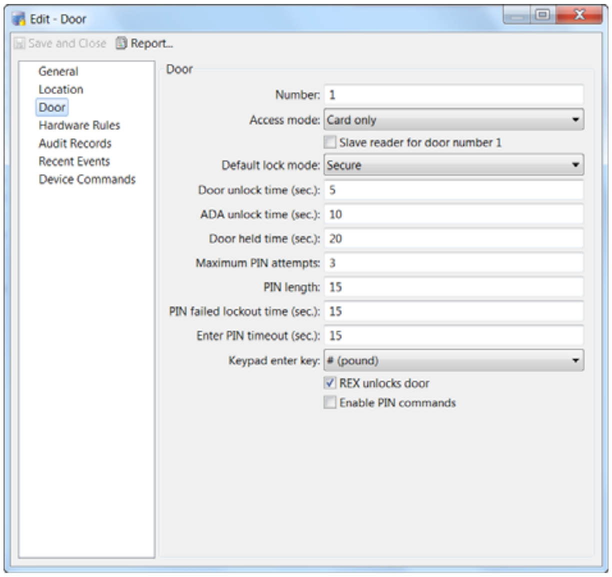
Door Groups

Identiv Santa Ana Facility
Identiv Santa Facility EVO Dr 1

This property sheet lists the door groups in which this door is currently enrolled.

Door Door Property Sheet

When you select the **Door** tab on an EM-100 door property sheet, a page like this appears:



Door

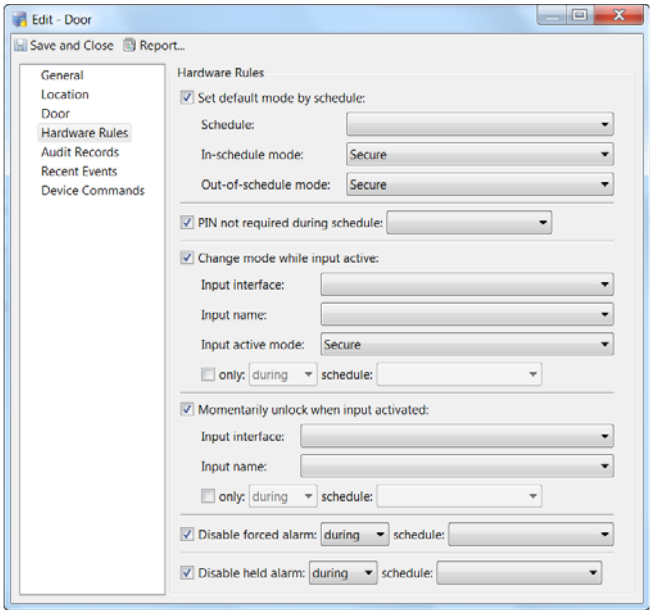
Number: 1
Access mode: Card only
□ Slave reader for door number 1
Default lock mode: Secure
Door unlock time (sec.): 5
ADA unlock time (sec.): 10
Door held time (sec.): 20
Maximum PIN attempts: 3
PIN length: 15
PIN failed lockout time (sec.): 15
Enter PIN timeout (sec.): 15
Keypad enter key: # (pound)
☑ REX unlocks door
□ Enable PIN commands

The fields on this page include:

Field	Description
Access mode	Select the option indicating the type of access to this door. Available options are: • **Card only** • **Code only** • **Card and Code**
Slave reader for door number 1	Check this box to indicate that this reader is slaved to another reader, as with readers positioned inside and outside the same door.
Default lock mode	Select the default lock mode: secure and unlocked.
Door unlock time (sec.)	Specify the number of seconds this door can remain unlocked.
ADA unlock time (sec.)	Specify the number of seconds beyond the door unlock time that the lock can remain open for ADA users.
Door held time (sec.)	Specify the number of seconds that a door can be held open before an alarm is issued.
Maximum PIN attempts	Specify the maximum number of times a PIN can be entered incorrectly before an alarm is issued and the door is locked.
PIN length	Specify the length of the PIN in digits.
PIN failed lockout time (sec.)	Specify the number of seconds the door remains locked after the maximum number of attempts has occurred.
Enter PIN timeout (sec.)	Specify the number of seconds between PIN attempts.
Keypad enter key	Specify the character used to request entry after the PIN has been entered. # (pound) is the default.
REX unlocks door	Check this box to indicate that the door can be unlocked by a REX.
Enable PIN commands	Check this box to indicate that the user may enter PIN commands through the keypad.

Hardware Rules Door Property Sheet

When you select the **Hardware Rules** tab from the EM-100 door property sheet, a page like this appears:



Hardware Rules

☑ Set default mode by schedule:

Schedule:

In-schedule mode: Secure

Out-of-schedule mode: Secure

☑ PIN not required during schedule:

☑ Change mode while input active:

Input interface:

Input name:

Input active mode: Secure

□ only: during schedule:

☑ Momentarily unlock when input activated:

Input interface:

Input name:

□ only: during schedule:

☑ Disable forced alarm: during schedule:

☑ Disable held alarm: during schedule:

The fields on this page include:

Table 7-2 Hardware Rules Door Property Sheet

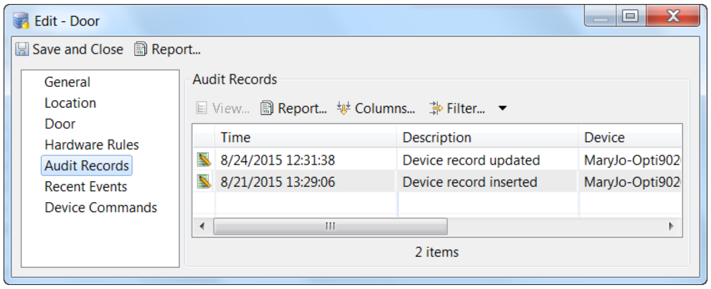
Field	Description
Set default mode by schedule	Check this box to indicate that this door is set to its default values at a specific time and indicates the disposition of the door outside of that schedule.
Schedule	From the drop-down list, indicate the time during which default mode is in effect for this door.
In-schedule mode	From the drop-down list, indicate the state for this door during the time indicated by the schedule.
Out-of-schedule mode	From the drop-down list, indicate the state for this door outside of the time indicated by the schedule.
PIN not required during schedule	Check this box to indicate that a PIN is NOT required during the specified schedule.
Schedule	From the drop-down list, indicate the time or schedule during which the PIN is not required for this door.
Change mode while input active	Check this box to indicate that the door can change mode while a specified input is active.
Input interface	From the drop-down list, select the interface that, when active, changes the mode of this door.
Input name	From the drop-down list, select the name of the input that changes the door mode when it goes active.
Input active mode	From the drop-down list, select the mode indicating the input is active.

Table 7-2 Hardware Rules Door Property Sheet (continued)

Field	Description
only: / schedule:	Check only and indicate the schedule and condition if the mode change can occur only during specified times.
Momentarily unlock when input activated:	Check this box to indicate that the door should be momentarily unlocked when the input specified below is activated.
Input interface	From the drop-down list, select the interface that, when active, causes this door to momentarily unlock.
Input name	From the drop-down list, select the name of the input that causes this door to momentarily unlock.
only: / schedule:	Check and indicate the schedule and condition if the door can momentarily unlock only during certain times.
Disable forced alarm	Check this box then specify a time interval during which a forced alarm is disabled for this door.
Disable held alarm	Check this box then specify a time interval during which a held alarm is disabled for this door.

Audit Records Door Property Sheet

When you select the Audit Records tab from an EM-100 door, a page like this appears:



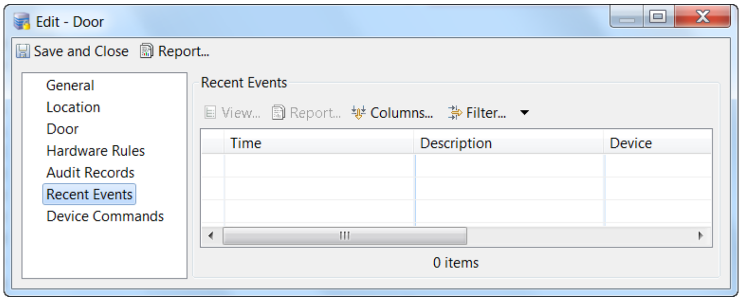
Time	Description	Device
8/24/2015 12:31:38	Device record updated	MaryJo-Opti902
8/21/2015 13:29:06	Device record inserted	MaryJo-Opti902

2 items

The columns on this page display the following information:

Recent Events Door Property Sheet

When you select the **Recent Events** tab from the EM-100 door property sheet, a page like this appears:



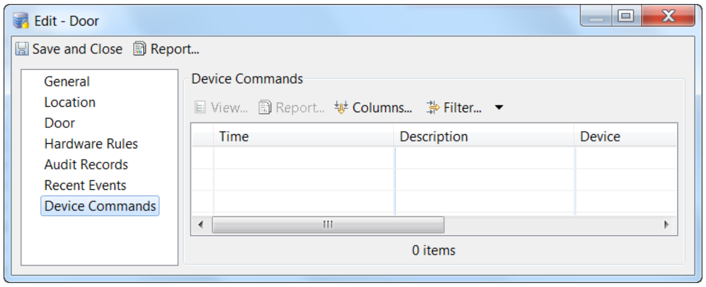
Time	Description	Device

0 items

Field	Description
View	When available, select a recent from the table then click this button to review a full explanation of the event for that device. You can also double-click the event in the table.
Report	Select a recent event from the table then click this button to generate a report.
Columns	Click this link and add or modify existing columns in the table. For more on this, refer to Revising the Column Display.
Filter	Click this link to filter the events and display a subset of records. To change the number of viewable events, select Max rows. See Using Filters.
Table	This table displays a list of all recent events currently available for this door.

Device Commands Door Property Sheet

When you select the **Device Commands** tab on the EM-100 door property sheet, a page like this appears:



Field	Description
View	When available, select a device command from the table then click this button to review a full explanation of the event for that device. You can also double-click the event in the table.
Report	Select a command from the table then click this button to generate a report.
Columns	Click this link and add or modify existing columns in the table. For more on this, refer to Revising the Column Display.
Filter	Click this link to filter the events and display a subset of records. To change the number of viewable events, select Max rows. See Using Filters.
Table	This table displays a list of all commands currently available for this door.

Device Commands

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

- Reader Module Commands, page 7-39
- Input and Output Module Commands, page 7-40

Reader Module Commands

Table 7-3 Reader Module (Module 00) Commands

Command	Description
Reset Module	Resets the device.
Squelch	Suppresses any events from this module. Events are not reported or saved.
Unsquelch	Undo squelch. Events are reported and saved.
View Recent Events	View a list of recent events for the module. See Viewing the Recent Events for a Device or Driver, page 5-15.
Replace Module	Replaces the current module with new device. This command is active only when the device is disconnected from ICPAM (Unknown State). See Replacing a Gateway, page 6-34.
Edit	Opens the Edit window to revise the device properties.
Edit Reader Connection Mode	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.
Disable	Disables the device and all attached devices. Also disables referenced door configurations. See Disabling or Deleting a Door, page 7-15. Disabled Devices can be re-enabled.
Delete	Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Door, page 7-15.
View Device Status	Opens a new window containing the Status and Extended Status information.
Show in Graphic Map Editor	Allows operators to add facility maps, and plot and organize devices for use in the Map viewer module. See Map Editor, page 12-50.

Input and Output Module Commands

Table 7-4 Input and Output Module Commands

Command	Description
Reset Module	Resets the device.
Squelch	Suppresses any events from this module. Events are not reported or saved.
Unsquelch	Undo squelch. Events are reported and saved.
Replace Module	Replaces the current device with new device. This command is active only when the device is disconnected from ICPAM (Unknown State). The command is used to replace a faulty device. See Replacing a Gateway, page 6-34.
View Recent Events	View a list of recent events for the module. See Viewing the Recent Events for a Device or Driver, page 5-15.
Edit	Opens the Edit window to revise the device properties.
Disable	Disables the device and all attached devices. Also disables referenced door configurations. See Disabling or Deleting a Door, page 7-15. Disabled Devices can be re-enabled.
Delete	Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Door, page 7-15.
View Device Status	Opens a new window containing the Status and Extended Status information.
Show in Graphic Map Editor	The Graphic Map Editor module allows operators to add facility maps, and plot and organize devices for use in the Map viewer module. See Map Editor, page 12-50.

Door Modes and Commands

Door Modes

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

- **Open**: The door is physically held open. The lock is in Unlocked state, the door sensor is dis-engaged. When door is in Open mode, and a badge is presented to a reader, the badge data is read but may not be validated.
- **Close**: The door is physically closed. The lock is in Unlocked state and the door sensor is engaged, indicating door is closed. When the door is in Close mode, and a badge is presented, the badge data is read but may not be validated.
- **Lock**: The door is physically closed and the lock is in Locked state. The Door Sensor is engaged. When the door is in Lock mode, and a badge is presented, the badge data is read and validated: if access is granted the lock is opened, access is denied if the badge is invalid.

- **Secure**: The door is locked and the deadbolt is applied. The deadbolt remains in place until issue a command to change the door mode (such as **Reset Door Mode**). See Door Commands, page 7-41 for more information.

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

Door Commands

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

Table 7-5 Door Commands in Locations View

Command	Description
Grant Access	Grants access to the door.
Grant Access ADA	Grants access to a door, and applies the ADA settings, such as the amount of time the door is held open, or use of a mechanical swing device. See Door Configuration Properties, page 8-24 for more information.
Update State	Updates the door state displayed in the hardware tree.
Set Door Mode Lock	Overrides the current door mode and locks the mechanism. The door mode remains set to Lock until you do one of the following: • Select the command **Reset Door Mode** to return the door to the configured mode (such as the default mode or scheduled mode). • Select a different **Set Door Mode** command. • Reset the Gateway using the **Reset Gateway** command. You can also reboot the Gateway. • Successfully execute the **Reload Gateway Configuration** command. • Invoke the **Apply Configuration Changes** command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies). **Note** Badge access is still allowed, or you can manually grant access with the **Grant Access** command.

Table 7-5 Door Commands in Locations View (continued)

Command	Description
Set Door Mode Open	Overrides the current door mode and unlocks the mechanism. The door mode remains set to Unlock until you do one of the following: • Select the command **Reset Door Mode** to return the door to the configured mode (such as the default mode or scheduled mode). • Select a different **Set Door Mode** command. • Reset the Gateway using the **Reset Gateway** command. You can also reboot the Gateway. • Successfully execute the **Reload Gateway Configuration** command. • Invoke the **Apply Configuration Changes** command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies). **Note** Badge access is still allowed, or you can manually grant access with the **Grant Access** command.
Set Door Mode Secure	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: • Select the command **Reset Door Mode** to return the door to the configured mode (such as the default mode or scheduled mode). • Select a different **Set Door Mode** command. • Reset the Gateway using the **Reset Gateway** command. You can also reboot the Gateway. • Successfully execute the **Reload Gateway Configuration** command. • Successfully execute the **Apply Configuration Changes** command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies). **Note** Badge access is still allowed, or you can manually grant access with the **Grant Access** command.
Reset Door Mode	Resets the door to the configured default mode.
Set Admin Down	Places the door in the Down state.
Set Admin Up	Places the door in the Up state.

Table 7-5 Door Commands in Locations View (continued)

Command	Description
Activate Access Policies	Manually activates the access policies for one or more doors. Use this command if the access policies were deactivated.
Deactivate Access Policies	Manually deactivates all access policies for one or more doors. All access is denied. Activate/deactivate access policies for multiple doors: • Select **Door/Location-based Hardware** from the Doors menu, right click a location and select **Deactivate Access Policies**. All doors in that location are affected. Activate/deactivate access policies for a single door: • Right-click a door icon in the **Door/Location-based Hardware** module and select the command. • In the **Hardware Tree** module, expand the Physical Driver device tree, right-click a door and select the command. To reactive the access policies, select **Activate Access Policies**.

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.

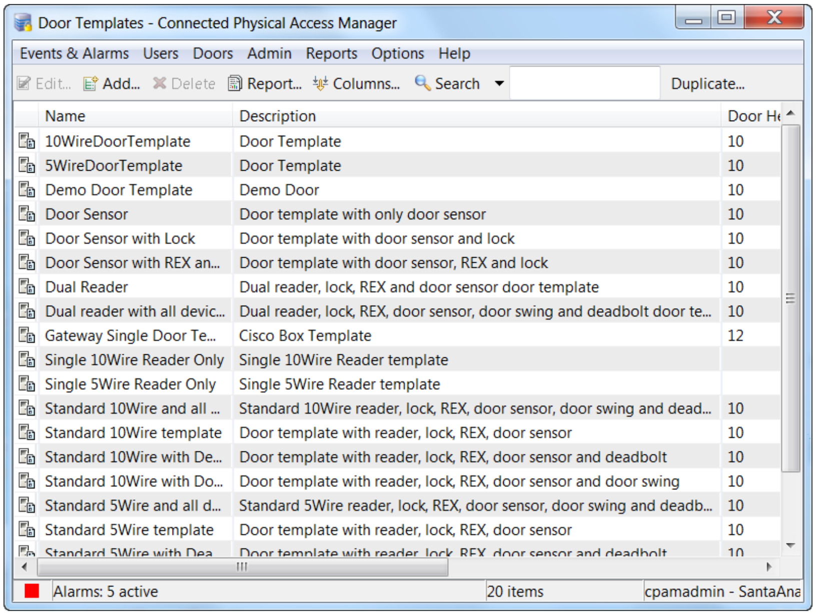
See Chapter 5, "Understanding Controller and Door Configurations" for more information.

Contents

Configuring Door Templates

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

Figure 8-1 Door Templates Main Window



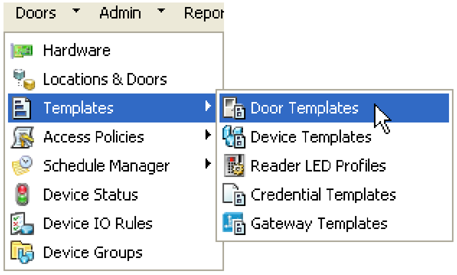
Name	Description	Door He
10WireDoorTemplate	Door Template	10
5WireDoorTemplate	Door Template	10
Demo Door Template	Demo Door	10
Door Sensor	Door template with only door sensor	10
Door Sensor with Lock	Door template with door sensor and lock	10
Door Sensor with REX an...	Door template with door sensor, REX and lock	10
Dual Reader	Dual reader, lock, REX and door sensor door template	10
Dual reader with all devic...	Dual reader, lock, REX, door sensor, door swing and deadbolt door te...	10
Gateway Single Door Te...	Cisco Box Template	12
Single 10Wire Reader Only	Single 10Wire Reader template	
Single 5Wire Reader Only	Single 5Wire Reader template	
Standard 10Wire and all ...	Standard 10Wire reader, lock, REX, door sensor, door swing and dead...	10
Standard 10Wire template	Door template with reader, lock, REX, door sensor	10
Standard 10Wire with De...	Door template with reader, lock, REX, door sensor and deadbolt	10
Standard 10Wire with Do...	Door template with reader, lock, REX, door sensor and door swing	10
Standard 5Wire and all d...	Standard 5Wire reader, lock, REX, door sensor, door swing and deadb...	10
Standard 5Wire template	Door template with reader, lock, REX, door sensor	10
Standard 5Wire with Dea	Door template with reader, lock, REX, door sensor and deadbolt	10

Alarms: 5 active | 20 items | cpamadmin - SantaAna

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

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

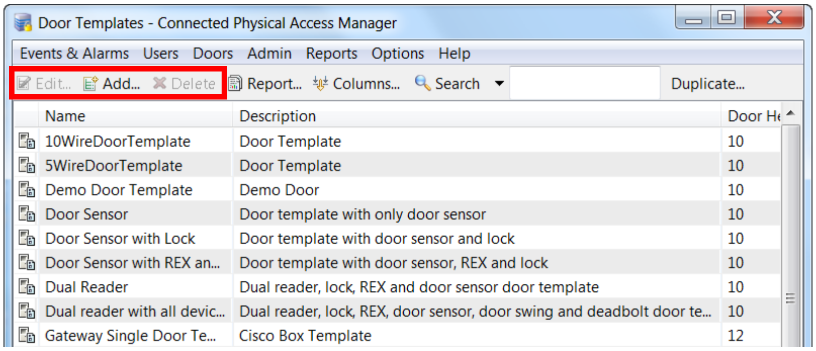
Step 1 Select **Door Templates** from the **Doors** menu in the **Templates** submenu.



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

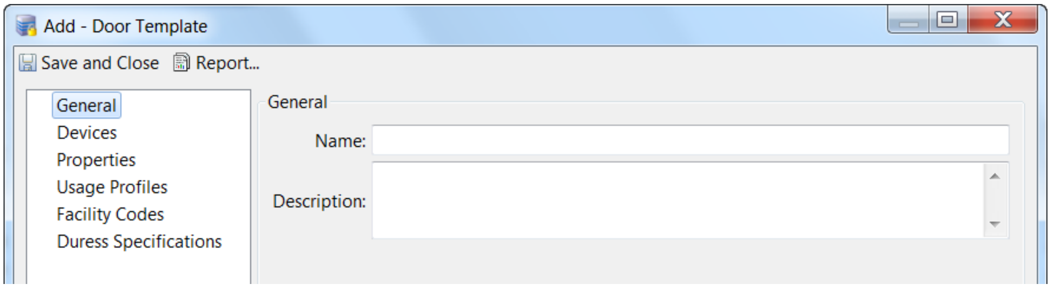
- You can also right-click an entry and select **Add**, **Edit**, or **Delete**.
- To duplicate an existing template:
  - Select the template and click the **Duplicate** button in the upper right.
  - Enter a **New Name** for the template and click **OK**.

- In the main window, select the duplicate template name and click **Edit**.
- Revise the template settings as described in the following steps.


Door Templates - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Delete Report... Columns... Search Duplicate...

Name	Description	Door He
10WireDoorTemplate	Door Template	10
5WireDoorTemplate	Door Template	10
Demo Door Template	Demo Door	10
Door Sensor	Door template with only door sensor	10
Door Sensor with Lock	Door template with door sensor and lock	10
Door Sensor with REX an...	Door template with door sensor, REX and lock	10
Dual Reader	Dual reader, lock, REX and door sensor door template	10
Dual reader with all devic...	Dual reader, lock, REX, door sensor, door swing and deadbolt door te...	10
Gateway Single Door Te...	Cisco Box Template	12

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



Step 4 Select the devices for in the door template:

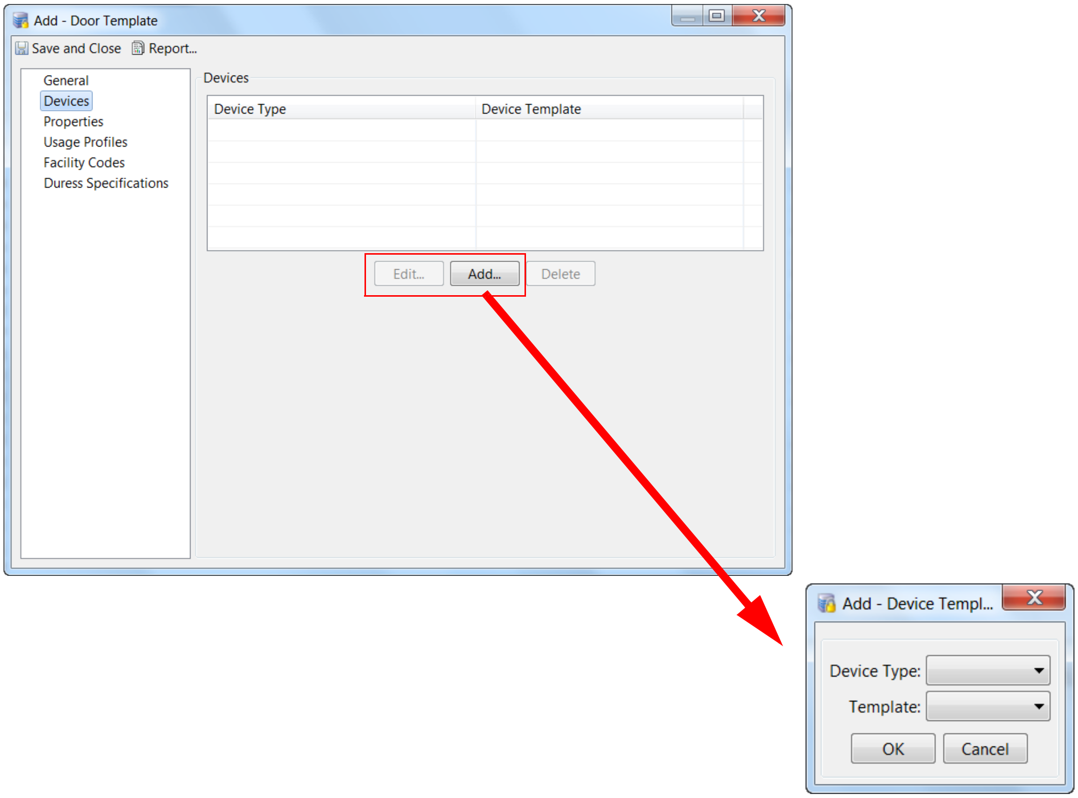
a. Select the **Devices** tab.

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

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

d. Select the **Template**. Only the templates for the device type are displayed. For example, if the device type is Reader, then only reader templates are displayed. See Configuring Device Templates, page 8-10 for instructions to create and modify the available templates.

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



f. Click **Next** to continue.

Step 5 Define the door lock properties.

a. Select the **Properties** tab.

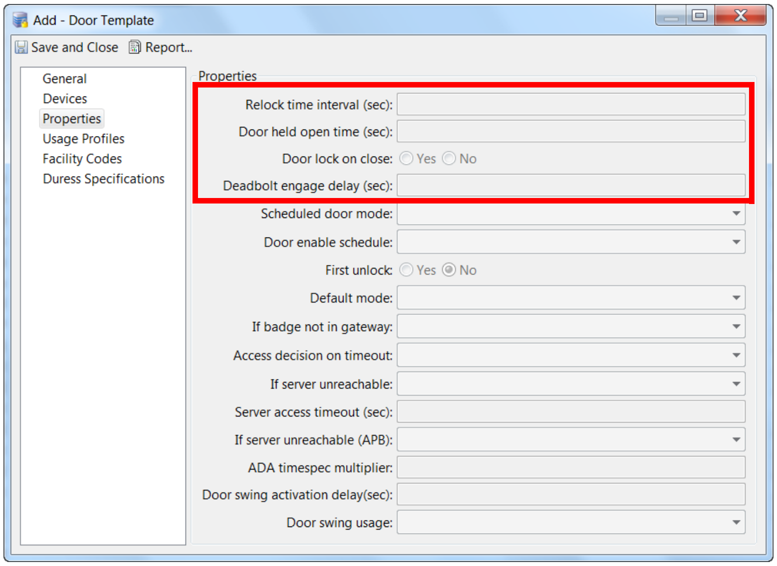
b. **Relock interval time (sec)**: the number of seconds to keep the door open after an access request is granted (grant access).

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.



Relock time interval (sec):
Door held open time (sec):
Door lock on close: ○ Yes ○ No
Deadbolt engage delay (sec):
Scheduled door mode:
Door enable schedule:
First unlock: ○ Yes ● No
Default mode:
If badge not in gateway:
Access decision on timeout:
If server unreachable:
Server access timeout (sec):
If server unreachable (APB):
ADA timespec multiplier:
Door swing activation delay(sec):
Door swing usage:

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**.

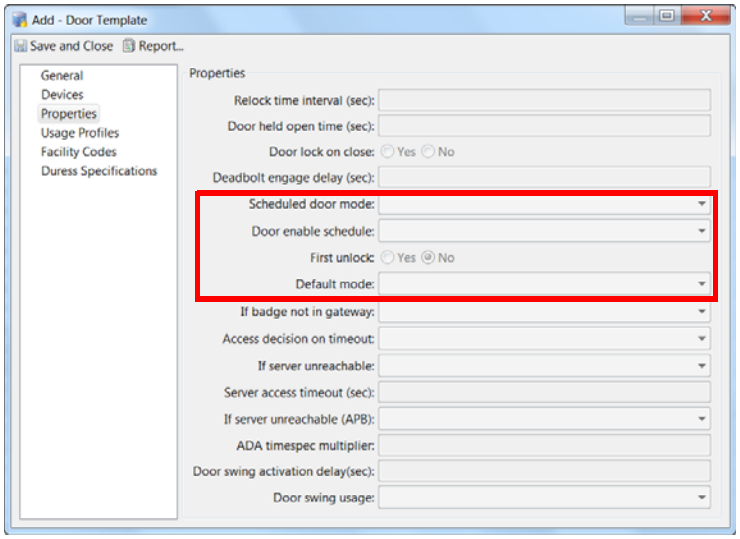
Step 6 Define the door mode and schedule:

a. Select the **Properties** tab.

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

- *Open*: the door is held open and the lock is in unlocked state.
- *Close*: the door is physically closed and the lock is in unlocked state.
- *Lock*: the door is physically closed and the lock is in Locked state.

– *Secure*: the door is locked and the deadbolt is applied.



See Door Modes, page 7-40 for more information.

c. **Door enable schedule**: (optional) select a door schedule. If you select **None**, then the door will remain in the **Default** mode at all times. If you select a schedule, the schedule will override the default mode for the times and days defined in the schedule. See Using the Schedule Manager, page 11-9 to add or modify the available door schedules.

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

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

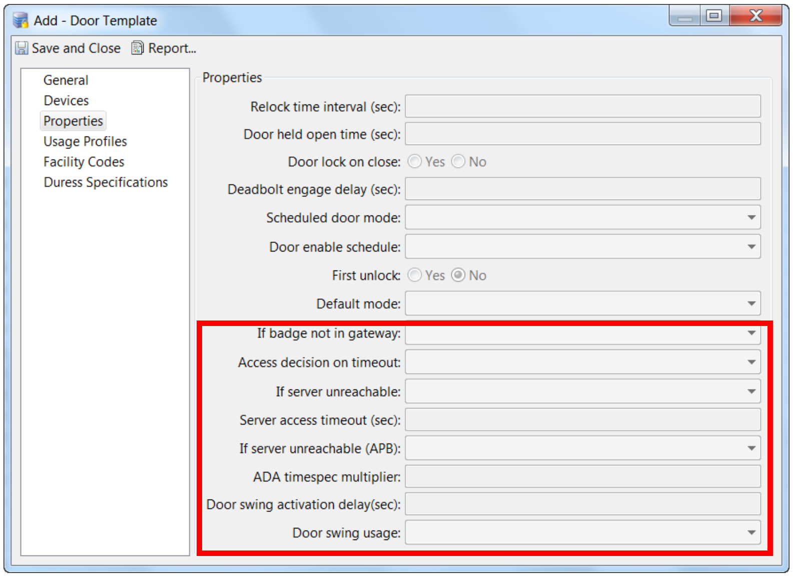
e. **First Unlock**: select **First Unlock** to activate the door schedule only on the first successful badge swipe. The door remains in default mode until a badge is used to access the door, even after the beginning time for the schedule. This is useful in situations such as snow days to ensure the door is not opened until a badge holder is physically present.

Tip See Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 5-25 for more information.

Step 7 Enter the additional door **Properties**:

- **Relock interval time (sec)**: see Step f.
- **Door held open time (sec)**: see Step f.
- **Door lock on close**: see Step f.
- **Deadbolt engage delay (sec)**: see Step f.
- **Scheduled Door Mode**: see Step 4.
- **Door enable schedule**: see Step 4.
- **First Unlock**: see Step 4.

- **Default Mode**: see 4..



Add - Door Template

Save and Close Report...

General
Devices
Properties
Usage Profiles
Facility Codes
Duress Specifications

Properties

Relock time interval (sec):
Door held open time (sec):
Door lock on close: ○ Yes ○ No
Deadbolt engage delay (sec):
Scheduled door mode:
Door enable schedule:
First unlock: ○ Yes ● No
Default mode:
If badge not in gateway:
Access decision on timeout:
If server unreachable:
Server access timeout (sec):
If server unreachable (APB):
ADA timespec multiplier:
Door swing activation delay(sec):
Door swing usage:

- **If badge not in gateway**: the action taken by the gateway if the badge is not in the gateway database.

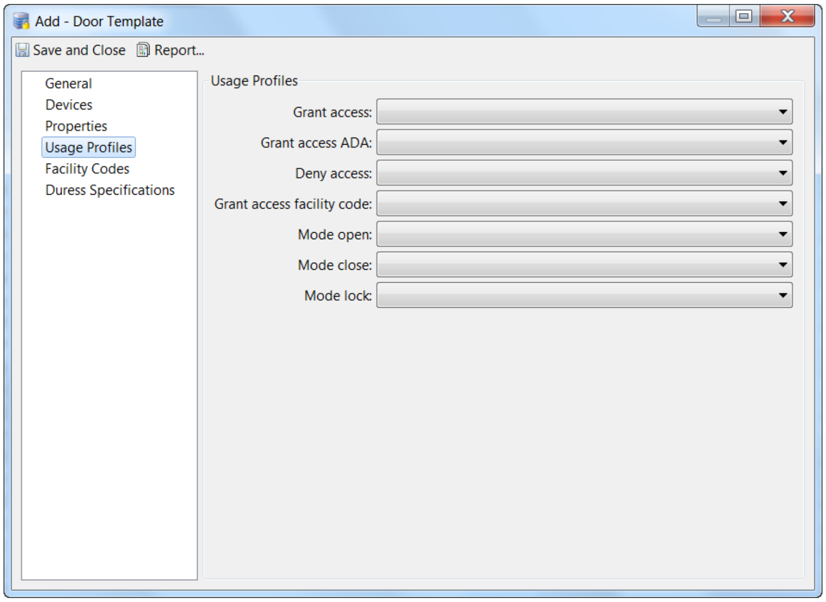
Note In ICPAM 2.1, **If the badge not in gateway** property is set to **Use Server** by default. This enables the badge to be authenticated if the badge is present in ICPAM even if it does not exist in the gateway. This option is enabled by default for new installations. Customers upgrading from previous versions need to change the options in the door properties if desired.

- **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 ICPAM. See the "Using Local (Controller) 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.

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.

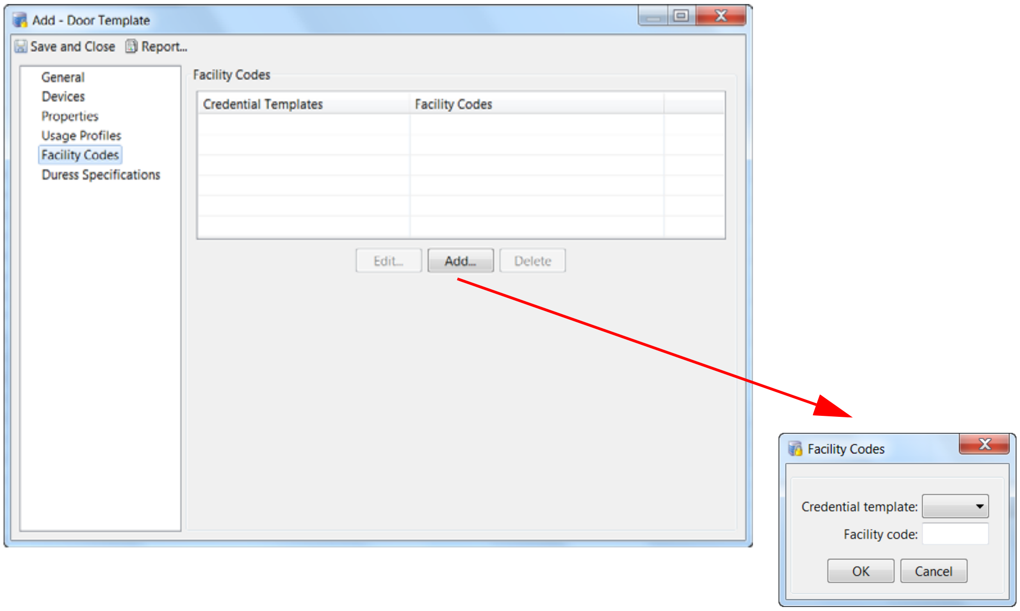
- **Grant facility code**: the LED display when access is granted based on a Facility Code.
- **Mode open**: the LED display when the door mode is *Open*.
- **Mode close**: the LED display when the door mode is *Close*.
- **Mode lock**: the LED display when the door mode is *Lock*.



Tip See Configuring Reader LED and Buzzer Profiles, page 8-21 for more information

Step 9 Enter the **Facility Code Info**:

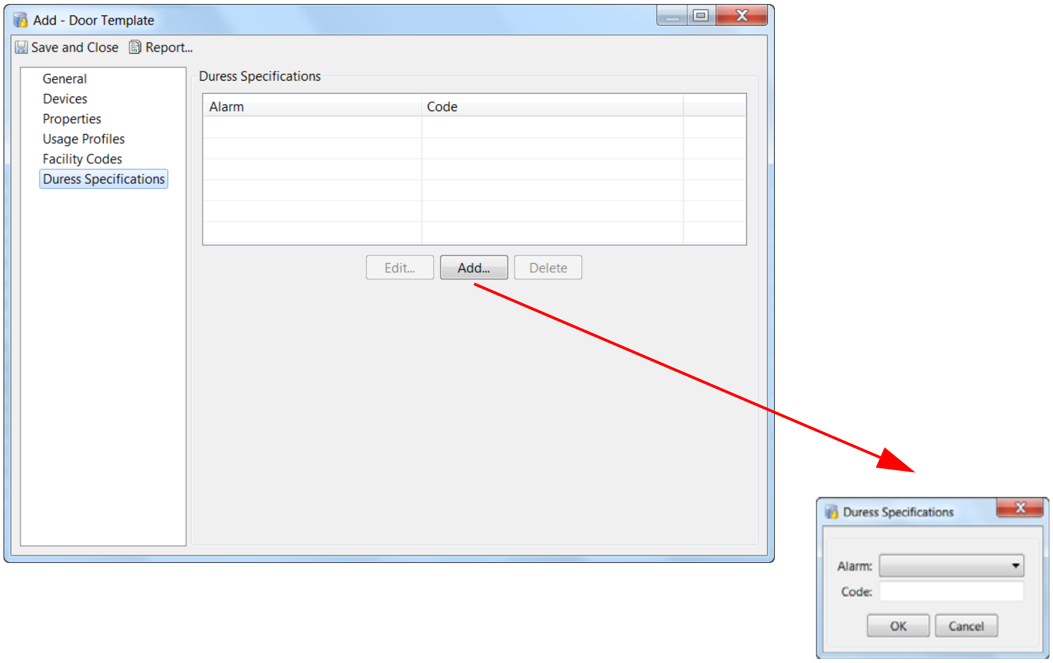
Click **Add** to add a credential template and facility code.



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.

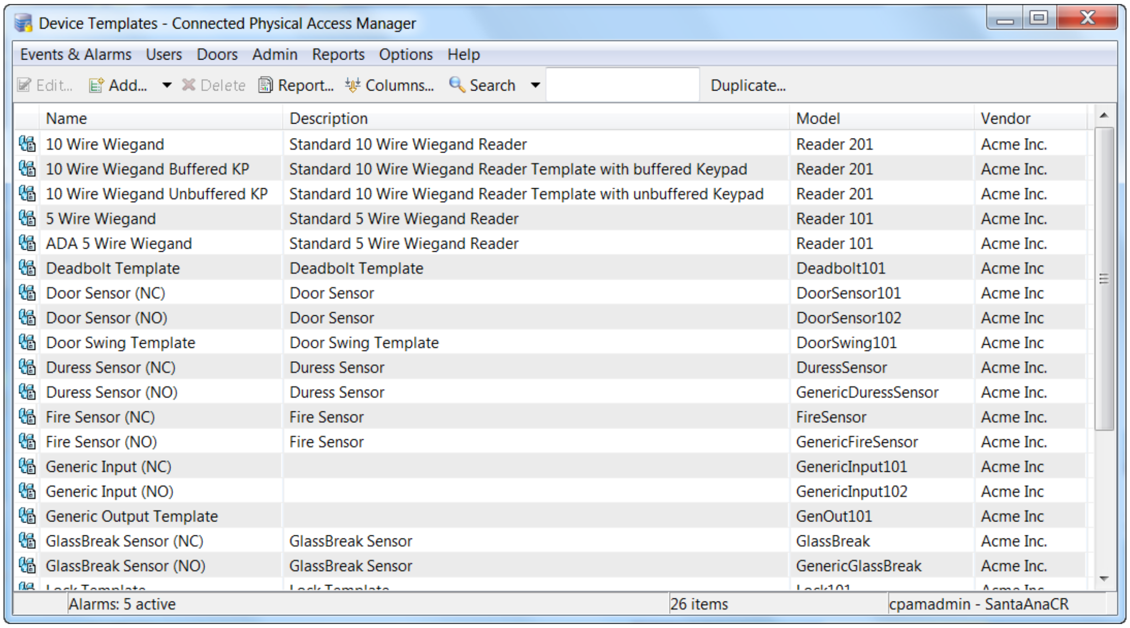
Configuring Device Templates

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

This section includes instructions on how to create device templates.

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

Figure 8-2 Device Templates Main Window



Name	Description	Model	Vendor
10 Wire Wiegand	Standard 10 Wire Wiegand Reader	Reader 201	Acme Inc.
10 Wire Wiegand Buffered KP	Standard 10 Wire Wiegand Reader Template with buffered Keypad	Reader 201	Acme Inc.
10 Wire Wiegand Unbuffered KP	Standard 10 Wire Wiegand Reader Template with unbuffered Keypad	Reader 201	Acme Inc.
5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
ADA 5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
Deadbolt Template	Deadbolt Template	Deadbolt101	Acme Inc
Door Sensor (NC)	Door Sensor	DoorSensor101	Acme Inc
Door Sensor (NO)	Door Sensor	DoorSensor102	Acme Inc
Door Swing Template	Door Swing Template	DoorSwing101	Acme Inc
Duress Sensor (NC)	Duress Sensor	DuressSensor	Acme Inc.
Duress Sensor (NO)	Duress Sensor	GenericDuressSensor	Acme Inc.
Fire Sensor (NC)	Fire Sensor	FireSensor	Acme Inc.
Fire Sensor (NO)	Fire Sensor	GenericFireSensor	Acme Inc.
Generic Input (NC)		GenericInput101	Acme Inc
Generic Input (NO)		GenericInput102	Acme Inc
Generic Output Template		GenOut101	Acme Inc
GlassBreak Sensor (NC)	GlassBreak Sensor	GlassBreak	Acme Inc.
GlassBreak Sensor (NO)	GlassBreak Sensor	GenericGlassBreak	Acme Inc.
Lock Template	Lock Template	Lock101	Acme Inc

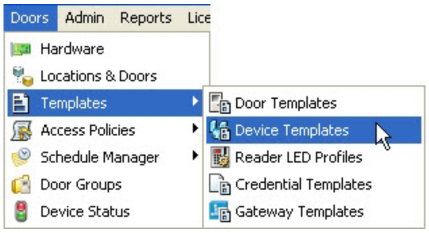
Alarms: 5 active 26 items cpamadmin - SantaAnaCR

For more information, see Chapter 5, "Understanding Controller and Door Configurations" and Chapter 7, "Configuring Doors".

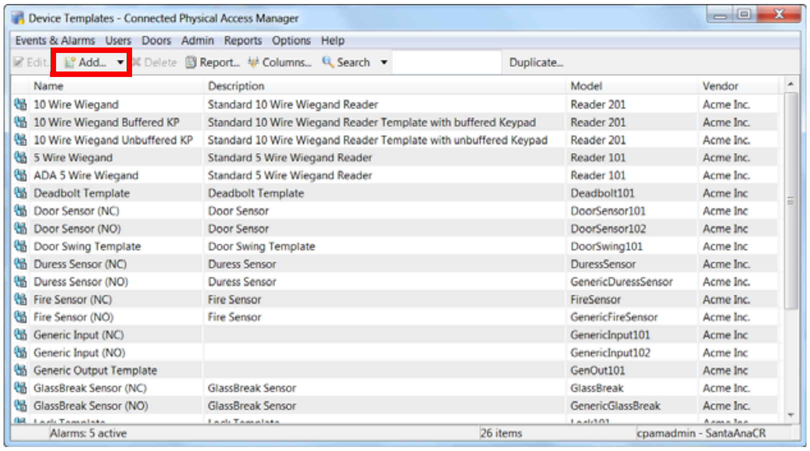
Creating a Device Template

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

Step 1 Select **Device Templates** from the **Doors** menu, in the **Templates** submenu.



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



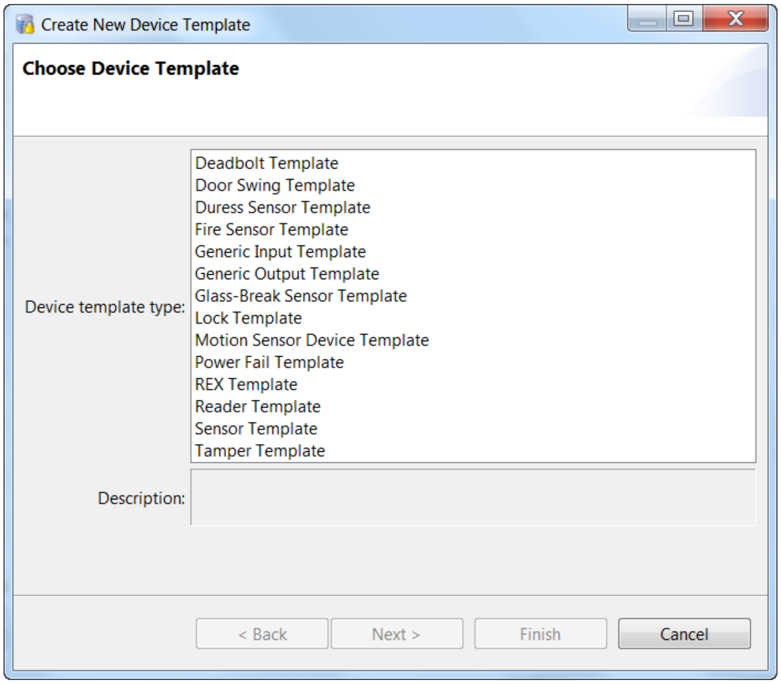
Name	Description	Model	Vendor
10 Wire Wiegand	Standard 10 Wire Wiegand Reader	Reader 201	Acme Inc.
10 Wire Wiegand Buffered KP	Standard 10 Wire Wiegand Reader Template with buffered Keypad	Reader 201	Acme Inc.
10 Wire Wiegand Unbuffered KP	Standard 10 Wire Wiegand Reader Template with unbuffered Keypad	Reader 201	Acme Inc.
5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
ADA 5 Wire Wiegand	Standard 5 Wire Wiegand Reader	Reader 101	Acme Inc.
Deadbolt Template	Deadbolt Template	Deadbolt101	Acme Inc
Door Sensor (NC)	Door Sensor	DoorSensor101	Acme Inc
Door Sensor (NO)	Door Sensor	DoorSensor102	Acme Inc
Door Swing Template	Door Swing Template	DoorSwing101	Acme Inc
Duress Sensor (NC)	Duress Sensor	DuressSensor	Acme Inc.
Duress Sensor (NO)	Duress Sensor	GenericDuressSensor	Acme Inc.
Fire Sensor (NC)	Fire Sensor	FireSensor	Acme Inc.
Fire Sensor (NO)	Fire Sensor	GenericFireSensor	Acme Inc.
Generic Input (NC)		GenericInput101	Acme Inc
Generic Input (NO)		GenericInput102	Acme Inc
Generic Output Template		GenOut101	Acme Inc
GlassBreak Sensor (NC)	GlassBreak Sensor	GlassBreak	Acme Inc.
GlassBreak Sensor (NO)	GlassBreak Sensor	GenericGlassBreak	Acme Inc.
Lock Template	Lock Template	Lock101	Acme Inc.

Alarms: 5 active 26 items cpamadmin - SantaAnaCR

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.

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



Device template type:

Deadbolt Template
Door Swing Template
Duress Sensor Template
Fire Sensor Template
Generic Input Template
Generic Output Template
Glass-Break Sensor Template
Lock Template
Motion Sensor Device Template
Power Fail Template
REX Template
Reader Template
Sensor Template
Tamper Template

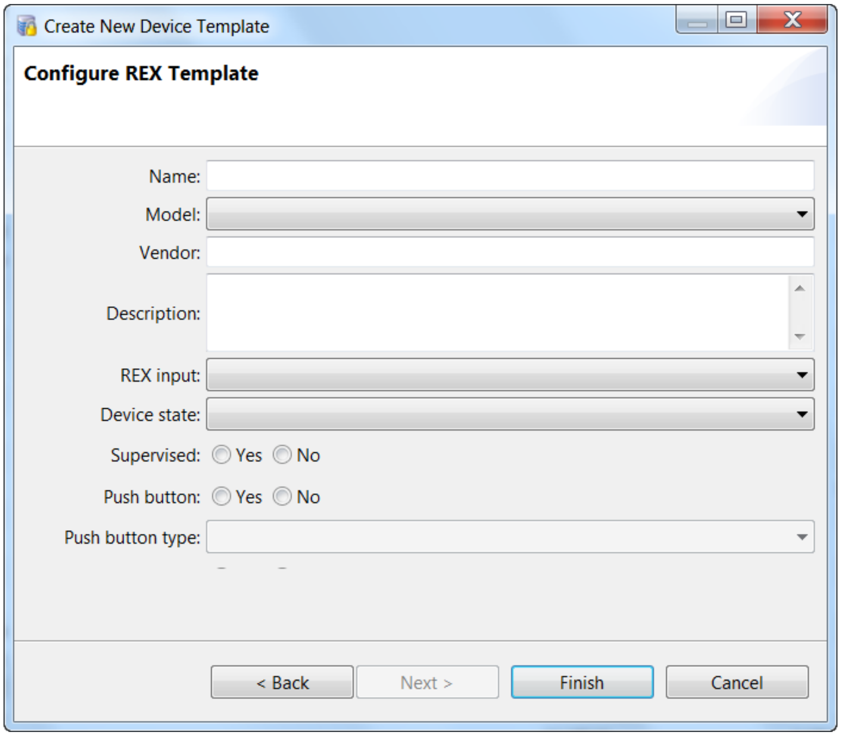
Description:

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 8-26 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.



Create New Device Template

Configure REX Template

Name:

Model:

Vendor:

Description:

REX input:

Device state:

Supervised: ○ Yes ○ No

Push button: ○ Yes ○ No

Push button type:

Configuring Credential Templates

Credential 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 8-13
- Credential Templates Settings Summary, page 8-15
- Creating a Gateway Credential Template, page 8-15
- Creating a Virtual Credential Template, page 8-17

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.

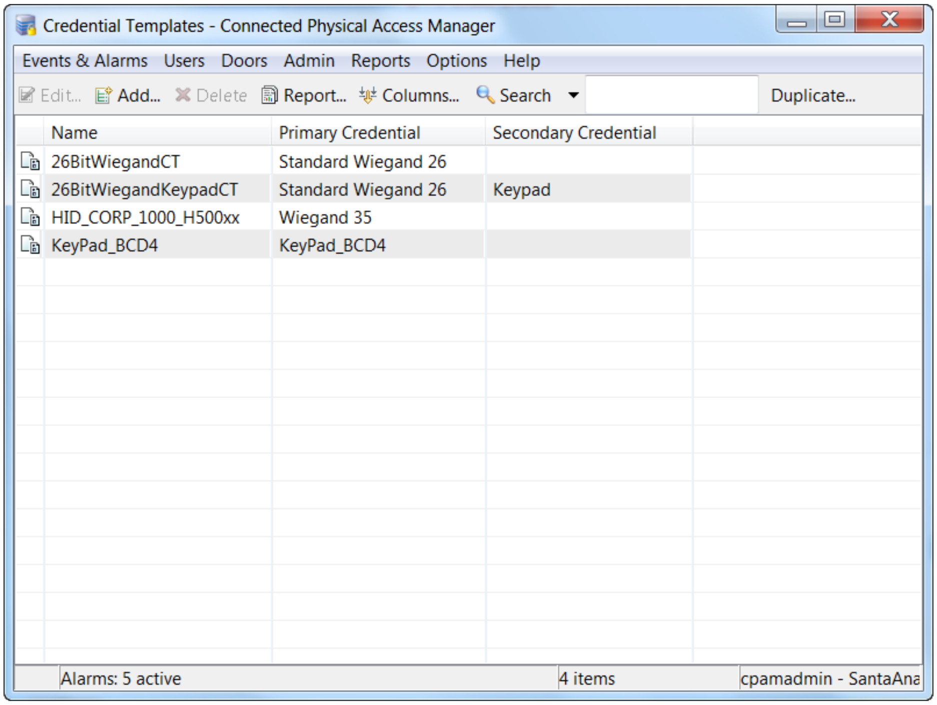
The data specification include the following:

- 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 8-15 for a configuration overview.

Existing templates cannot be modified. See Creating a Gateway Credential Template, page 8-15 for instructions to create a new template.

Figure 8-3 Credential Templates Main Window



Name	Primary Credential	Secondary Credential
26BitWiegandCT	Standard Wiegand 26	
26BitWiegandKeypadCT	Standard Wiegand 26	Keypad
HID_CORP_1000_H500xx	Wiegand 35	
KeyPad_BCD4	KeyPad_BCD4	

Alarms: 5 active
4 items
cpamadmin - SantaAna

Credential Templates Settings Summary

ICPAM 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, Location, and Other. Parity and sentinel are 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.

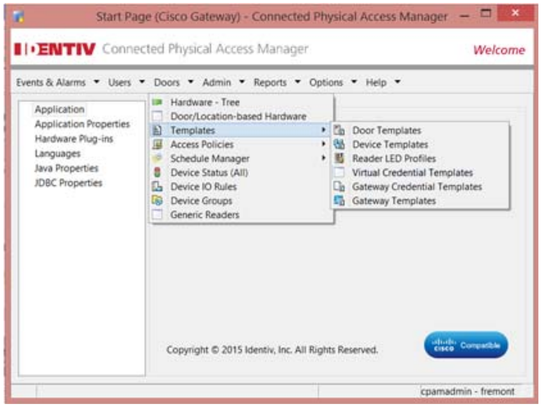
For example, the `KeyPad_BCD4`.

Creating a Gateway Credential Template

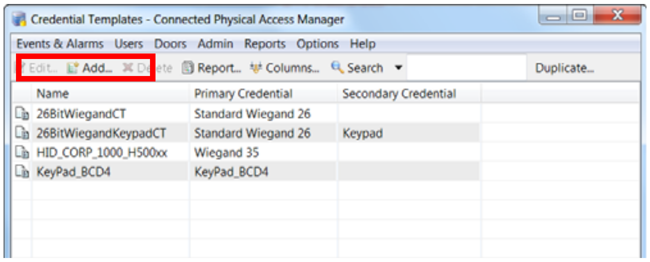
Complete the following instructions to create, edit, or duplicate a credential template for Cisco gateway credentials.

Step 1 Select **Templates** from the **Doors** menu.

Step 2 From the Templates submenu, select the **Gateway Credential Templates** option.



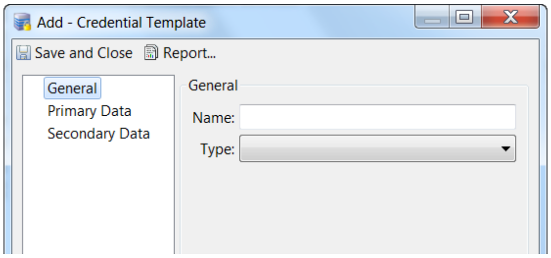
Step 3 Click **Add**, or select an existing template from the list and click **Edit**.



Name	Primary Credential	Secondary Credential
26BitWiegandCT	Standard Wiegand 26	
26BitWiegandKeypadCT	Standard Wiegand 26	Keypad
HID_CORP_1000_H500xx	Wiegand 35	
KeyPad_BCD4	KeyPad_BCD4	

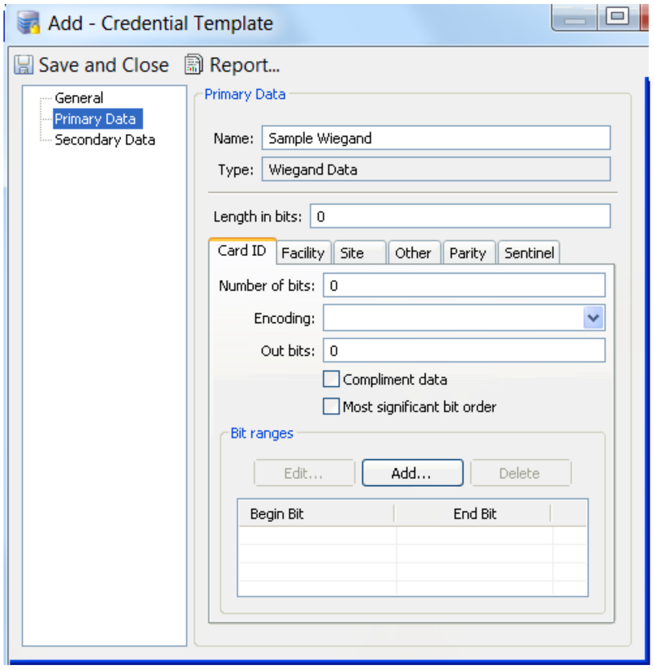
- You can also select an existing device from the list and click **Edit** or **Duplicate**. To duplicate an existing template:
  - Select the template and click the **Duplicate** button in the upper right.
  - Enter a **New Name** for the template and click **OK**.
  - In the main window, select the 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 4 Select the **General** tab, enter the **Name** and **Description** of the template.



Step 5 Enter the **Primary Data** and **Secondary Data** settings for the template.

See Credential Templates Settings Summary, page 8-15 for more information.



Primary Data

Name: Sample Wiegand

Type: Wiegand Data

Length in bits: 0

Number of bits: 0

Encoding:

Out bits: 0

□ Compliment data

□ Most significant bit order

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. The value for the field **length in bits** should be a number between 1 and 2147483647.

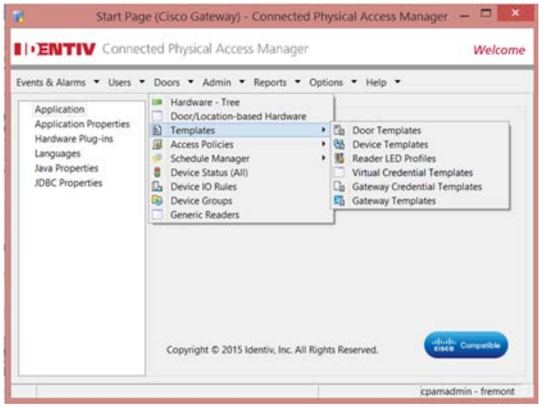
Step 6 Click **Save and Close** to save the template and close the window.

Creating a Virtual Credential Template

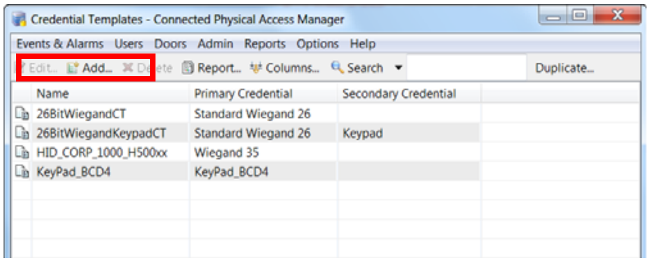
Complete the following instructions to create, edit, or duplicate a virtual credential template. This template is used to populate credentials for Identiv EM-100 drivers.

Step 1 Select **Templates** from the **Doors** menu.

Step 2 From the Templates submenu, select the **Virtual Credential Templates** option.



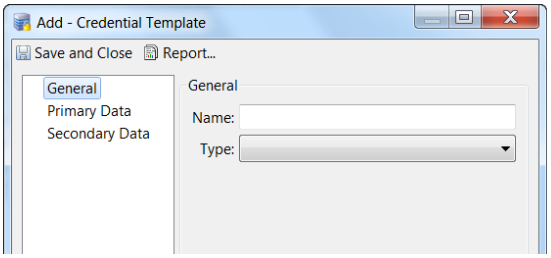
Step 3 Click **Add**, or select an existing template from the list and click **Edit**.



Name	Primary Credential	Secondary Credential
26BitWiegandCT	Standard Wiegand 26	
26BitWiegandKeypadCT	Standard Wiegand 26	Keypad
HID_CORP_1000_H500xx	Wiegand 35	
KeyPad_BCD4	KeyPad_BCD4	

- 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 4 Select the **General** tab, enter the **Name** and **Description** of the template.

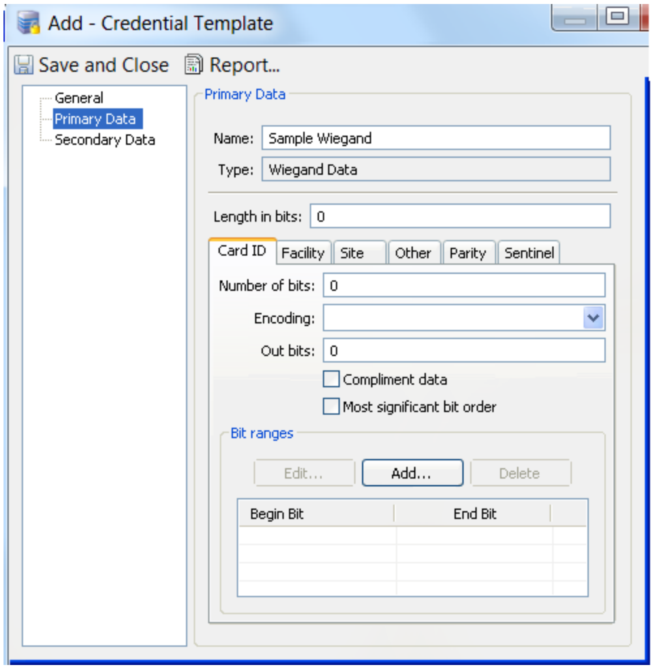


Name:

Type:

Step 5 Enter the **Primary Data** and **Secondary Data** settings for the template.

See Credential Templates Settings Summary, page 8-15 for more information.



Name: Sample Wiegand

Type: Wiegand Data

Length in bits: 0

Number of bits: 0

Encoding:

Out bits: 0

□ Compliment data

□ Most significant bit order

Begin Bit	End Bit

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. The value for the field **length in bits** should be a number between 1 and 2147483647.

Step 6 Click **Save and Close** to save the template and close the window.

For more on this, refer to Importing New Credential Templates from VFF Files, page 8-19.

Importing New Credential Templates from VFF Files

Identiv supplies a variety of VFF files that can be used creating dozens of credential types.

To import credential templates from VFFs:

Step 1 Download one or more VFFs from the Identiv website at this address:

http://www.identiv.com/icpam-credential-templates

Step 2 At the hardware tree, right-click on the EM-100 Driver and select **Edit**.

The EM-100 driver property sheets appear (Identiv EM-100 Driver Property Sheets, page 6-40).

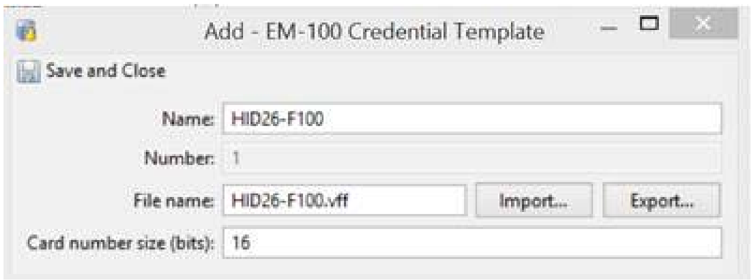
Step 3 Click to select the EM-100 Credential Template property sheet (Driver EM-100 Credential Templates Page, page 6-43).

Step 4 Click **Add**.

Step 5 Select **Wiegand** as the type and click **OK**.

The Add EM-100 Credential Template screen appears

.



Name: HID26-F100

Number: 1

File name: HID26-F100.vff

Card number size (bits): 16

Step 6 In the ‘Name’ field, enter an appropriate name for this credential template.

Step 7 Click **Import...**

Step 8 Browse to the VFF file you downloaded from the Identiv site.

Step 9 In the ‘Card number size (bits)’ field, enter the number of bits required for this card number format.

The value should be a number between 1 and 2147483647.

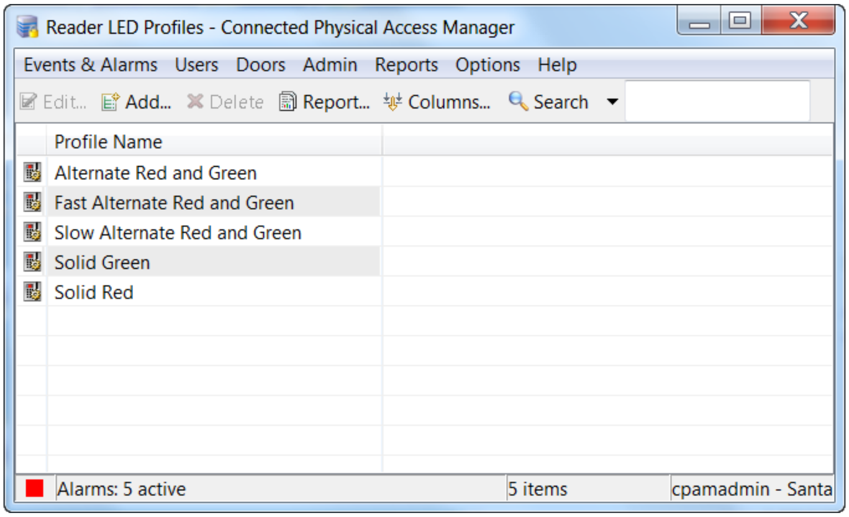
Step 10 Click **Save** and **Close**.

The new credential template now appears in the credential template 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 Tree module.

Figure 8-4 Reader UI Profile Main Window



Profile Name
Alternate Red and Green
Fast Alternate Red and Green
Slow Alternate Red and Green
Solid Green
Solid Red

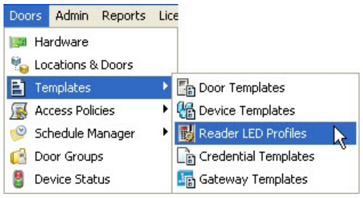
Alarms: 5 active | 5 items | cpamadmin - Santa

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.

Step 1 Select **Reader LED Profiles** from the Doors menu, in the **Templates** submenu.



Step 2 Create or edit the profile:

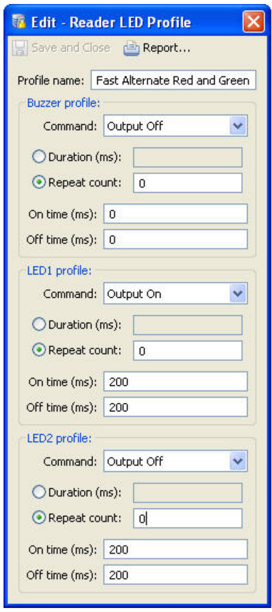
a. Click **Add**, or select an existing profile and click **Edit**.

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 O**n 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.



Edit - Reader LED Profile

Profile name: Fast Alternate Red and Green

Buzzer profile:

Command: Output Off

○ Duration (ms):

● Repeat count: 0

On time (ms): 0

Off time (ms): 0

LED1 profile:

Command: Output On

○ Duration (ms):

● Repeat count: 0

On time (ms): 200

Off time (ms): 200

LED2 profile:

Command: Output Off

○ Duration (ms):

● Repeat count: 0

On time (ms): 200

Off time (ms): 200

188729

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

Duplicating Templates

- Duplicating Door, Device, and Credential Templates, page 8-22
- Duplicating Gateway Templates, page 8-23

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.

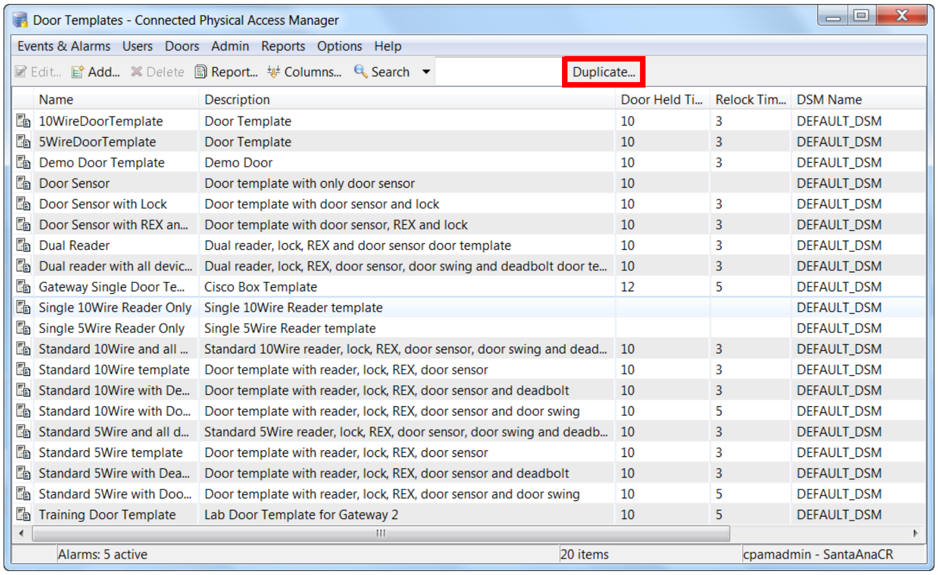
To create exact duplicates of door, device, and credential templates, do the following:

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 8-5.

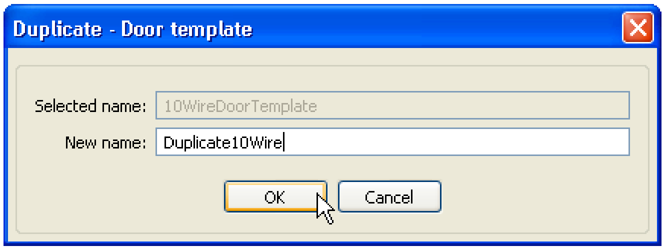
Figure 8-5 Duplicate Button in Door Template Window



Name	Description	Door Held Ti...	Relock Tim...	DSM Name
10WireDoorTemplate	Door Template	10	3	DEFAULT_DSM
5WireDoorTemplate	Door Template	10	3	DEFAULT_DSM
Demo Door Template	Demo Door	10	3	DEFAULT_DSM
Door Sensor	Door template with only door sensor	10		DEFAULT_DSM
Door Sensor with Lock	Door template with door sensor and lock	10	3	DEFAULT_DSM
Door Sensor with REX an...	Door template with door sensor, REX and lock	10	3	DEFAULT_DSM
Dual Reader	Dual reader, lock, REX and door sensor door template	10	3	DEFAULT_DSM
Dual reader with all devic...	Dual reader, lock, REX, door sensor, door swing and deadbolt door te...	10	3	DEFAULT_DSM
Gateway Single Door Te...	Cisco Box Template	12	5	DEFAULT_DSM
Single 10Wire Reader Only	Single 10Wire Reader template			DEFAULT_DSM
Single 5Wire Reader Only	Single 5Wire Reader template			DEFAULT_DSM
Standard 10Wire and all ...	Standard 10Wire reader, lock, REX, door sensor, door swing and dead...	10	3	DEFAULT_DSM
Standard 10Wire template	Door template with reader, lock, REX, door sensor	10	3	DEFAULT_DSM
Standard 10Wire with De...	Door template with reader, lock, REX, door sensor and deadbolt	10	3	DEFAULT_DSM
Standard 10Wire with Do...	Door template with reader, lock, REX, door sensor and door swing	10	5	DEFAULT_DSM
Standard 5Wire and all d...	Standard 5Wire reader, lock, REX, door sensor, door swing and deadb...	10	3	DEFAULT_DSM
Standard 5Wire template	Door template with reader, lock, REX, door sensor	10	3	DEFAULT_DSM
Standard 5Wire with Dea...	Door template with reader, lock, REX, door sensor and deadbolt	10	3	DEFAULT_DSM
Standard 5Wire with Doo...	Door template with reader, lock, REX, door sensor and door swing	10	5	DEFAULT_DSM
Training Door Template	Lab Door Template for Gateway 2	10	5	DEFAULT_DSM

Step 4 Enter a **New Name** for the template and click **OK**, as shown in Figure 8-6.

Figure 8-6 Duplicate Name



Selected name: 10WireDoorTemplate

New name: Duplicate10Wire

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 8-2
- Configuring Device Templates, page 8-10
- Configuring Credential Templates, page 8-13

Duplicating Gateway Templates

- To create a template from a gateway configuration, see Creating Custom Gateway Configurations without Templates, page 6-2.
- To create a clone of a gateway configuration for one-time use, see Cloning a Gateway Configuration, page 6-33. A gateway clone is an independent copy, and is used to configure one other controller.

Door Configuration Properties

The following properties are configured for a door template and configuration.

See the "Configuring Door Templates" section on page 8-2 for more information.

:

Table 8-1 Door Properties

Field	Description
Relock interval time (sec)	the number of seconds to keep the door open after an access request is granted (grant access).
Door held open time (sec)	The number of seconds before DoorHelpOpen alarm is generated.
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.
Deadbolt engage delay (sec)	The amount of time to wait (in seconds) after the door closes to engage the deadbolt.
Scheduled door mode	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 the "Understanding Door Modes, Door Schedules, and the First Unlock Feature" section on page 5-25.
Door enable schedule	The schedule to be used by Door. If you select **None**, 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 11-9 to add or modify the available door schedules. See also the "Understanding Door Modes, Door Schedules, and the First Unlock Feature" section on page 5-25.
First unlock	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. See the "Understanding Door Modes, Door Schedules, and the First Unlock Feature" section on page 5-25, for more information.

Table 8-1 Door Properties

Field	Description
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 the "Understanding Door Modes, Door Schedules, and the First Unlock Feature" section on page 5-25, 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 ICPAM. See the "Using Local (Controller) 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.

Note In ICPAM 2.1, the badge that is not in gateway property is set to **Use Server** by default. This enables the badge to be authenticated if the badge is present in ICPAM even if it does not exist in the gateway. This option is only enabled by default for new installations and customers upgrading from previous versions need to change the options in the door properties if desired.

Device Configuration Properties

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

- Understanding Normally Open vs. Normally Closed Devices, page 8-26
- Understanding Supervised vs. Unsupervised Input Devices, page 8-26
- Device Configuration Properties Summary, page 8-27

Understanding Normally Open vs. Normally Closed Devices

- Normally open (N.O.) contacts connect the circuit when the relay is activated; the circuit is disconnected when the relay is inactive.
- Normally closed (N.C.) 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.

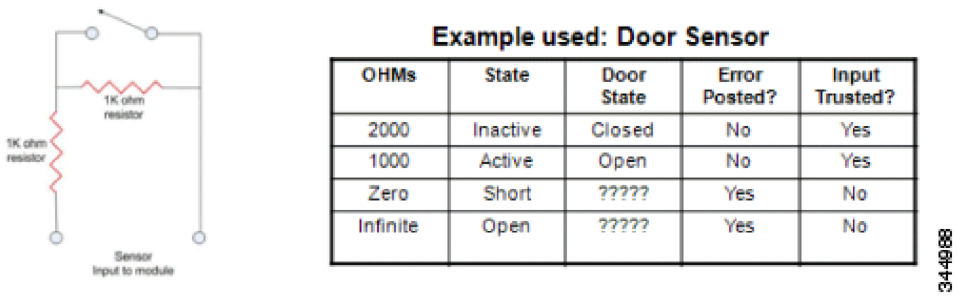
Unsupervised inputs have limited functionality. If a wire is cut or shorted between the input module and a normally open device. The server cannot determine the change and the device would remains in inactive state even when the switch is closed.

To make the input device supervised, use two 1K resistors in the circuit (Figure 8-7).

- 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, ICPAM can determine if a wire is cut or shorted.

Figure 8-7 Example of a Supervised Door Sensor



Example used: Door Sensor

OHMs	State	Door State	Error Posted?	Input Trusted?
2000	Inactive	Closed	No	Yes
1000	Active	Open	No	Yes
Zero	Short	?????	Yes	No
Infinite	Open	?????	Yes	No

Device Configuration Properties Summary

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

Table 8-2 Device Configuration Properties

Device	Properties
Deadbolt	• **Name**: The template name. • **Model**: The device model. • **Vendor**: The device vendor or manufacturer. • **Description**: A text description of the device.
Door Swing	• **Name**: The template name. • **Model**: The device model. • **Vendor**: The device vendor or manufacturer. • **Description**: A text description of the device. • **Trigger Time (sec)**: The number of seconds that power is applied to operate the door swing.
Door Sensor	• **Sensor 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. • **Device state**: The default state of the device.
Duress Sensor	• **Sensor 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. • **Sensor state**: The default state of the device.
Fire Sensor	• **Sensor 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. • **Device state**: The default state of the device.
Generic Input Device	• **Normal state**: The type of device contact: – **Normally Open**: the device is normally open. – **Normally Closed**: the device is normally closed. • **Supervised**: Defines if the device is supervised or unsupervised. • **Device state**: The default state of the device.

Table 8-2 Device Configuration Properties (continued)

Device	Properties
Generic Output Device	• **Name**: The template name. • **Model**: The device model. • **Vendor**: The device vendor or manufacturer. • **Description**: A text description of the device. • **Activation Time (ms)**: When the command **Timed Activate Relay** is invoked, this property defines the number of milliseconds the generic output is activated. **Note** In ICPAM 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 *normally open* or *normally closed.* In ICPAM Release 1.0.3 or earlier, this setting could also be made in software. If you are upgrading from ICPAM Release 1.0.3 or earlier, verify that devices are correctly wired to the module as *normally open* or *normally closed*. See *Cisco Physical Access Gateway User Guide* for more information.
Glass-Break	• **Sensor 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. • **Sensor state**: The default state of the device.
Lock	• **Name**: The template name. • **Model**: The device model. • **Vendor**: The device vendor or manufacturer. • **Description**: A text description of the device. **Note** In ICPAM 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 *normally open* or *normally closed.* In ICPAM Release 1.0.3 or earlier, this setting could also be made in software. If you are upgrading from ICPAM Release 1.0.3 or earlier, verify that devices are correctly wired to the module as *normally open* or *normally closed*. See *Cisco Physical Access Gateway User Guide* for more information.
Motion Sensor	• **Name**: The template name. • **Model**: The device model. • **Vendor**: The device vendor or manufacturer. • **Description**: A text description of the device. • **Normal state**: The type of device contact: – **Normally Open**: the device is normally open. – **Normally Closed**: the device is normally closed. • **Supervised**: Defines if the device is supervised or unsupervised. • **Device state**: The default state of the device.

Table 8-2 Device Configuration Properties (continued)

Device	Properties
Power Fail	• **Normal state**: The type of device contact: – **Normally Open**: the device is normally open. – **Normally Closed**: the device is normally closed. • **Supervised**: Defines if the device is supervised or unsupervised. • **Power fail state**: The default state of the device.
REX	**Note** 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. • **Rex input**: The type of device contact: – **Normally Open**: the device is normally open. – **Normally Closed**: the device is normally closed. • **Device state**: The default state of the device. • **Supervised**: Defines if the device is supervised or unsupervised. • **Push button**: Indicates a push button type of REX. • **Push button type**: Indicates the kind of push button REX. • **ADA enabled**: Indicates if ADA is enabled or not. If ADA is enabled, *ADA timespec multiplier* property is applied on the door when REX is activated.

Table 8-2   Device Configuration Properties (continued)

Device	Properties
Reader	• **Reader type**: – **Card Reader** – **Card and Keypad Reader** – **Keypad Reader** **Note** The device does not support a reader device template with the type 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. **Note** While configuring the reader type as Card and Keypad, the user should declare a PIN for the badge that will be associated with this template. If not, any PIN entered by the user will grant access to the door associated with the template. • **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.

Table 8-2 Device Configuration Properties (continued)

Device	Properties
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 to small movements of the door but the door does not open.
- 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 ICPAM server, so there is no way of validating the debounce timer using Events Monitoring from the ICPAM server. Debounce timer validations can only be performed using the debugging logs on the controller 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.

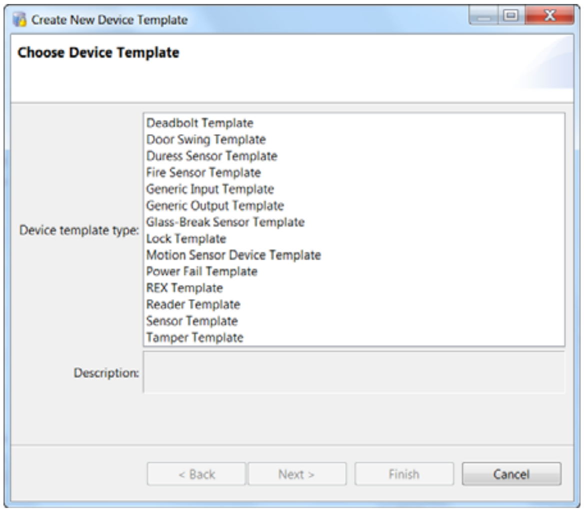
Procedure

To configure the debounce timer, do the following:

Step 1 Create a new input device template.

a. Select **Doors** > **Templates** > **Device Templates**. The Device Templates screen appears.

b. From the Device Templates screen, click the **Add...** button. The Create New Device Template Wizard appears like this example:



c. Click to highlight a door sensor or a duress sensor.

d. Click **Next**. A screen with the debounce timer field on it.

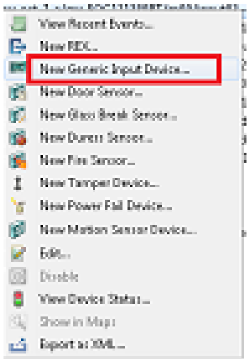
e. Specify the debounce timer value in the **Debounce Timer (ms)** field.

Step 2 Create a new input device for the gateway.

a. Go to **Doors** -> **Hardware Tree**.

b. Create a new input device for the gateway.

Figure 8-8 New Input Device

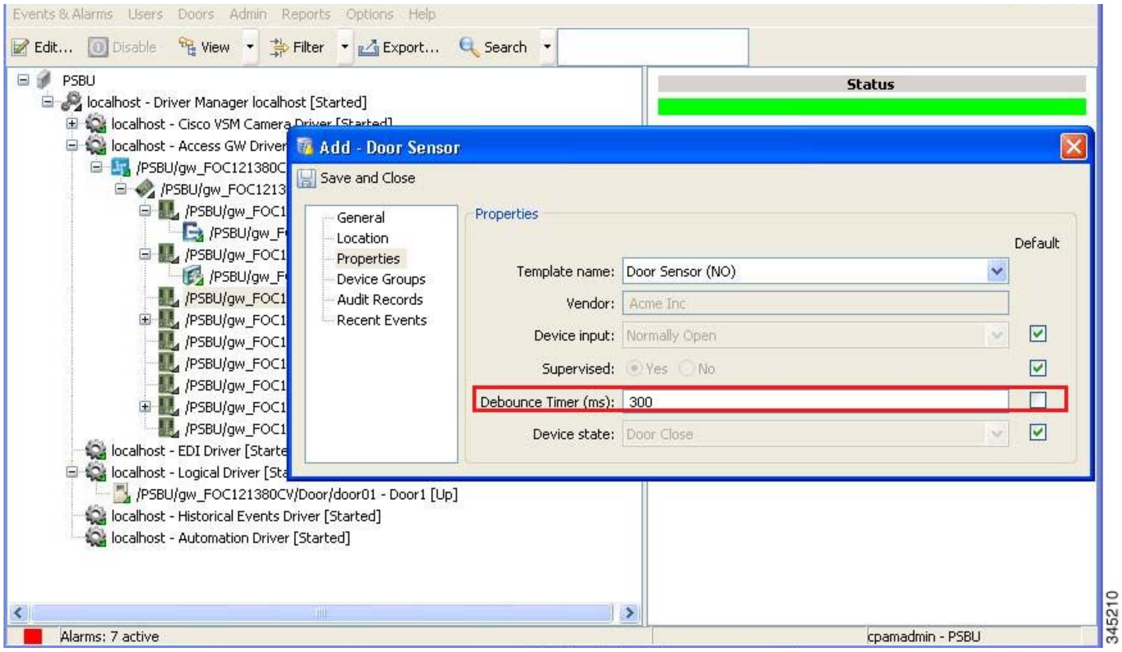


c. Select the **Properties** tab.

d. Choose the corresponding device template.

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

Figure 8-9 Enter Debounce timer value


Events & Alarms Users Doors Admin Reports Options Help
Edit... Disable View Filter Export... Search
PSBU
localhost - Driver Manager localhost [Started]
localhost - Cisco VSM Camera Driver [Started]
localhost - Access GW Driver
/PSBU/gw_FOC121380C
/PSBU/gw_FOC1213
/PSBU/gw_FOC1
/PSBU/gw_F
/PSBU/gw_FOC1
/PSBU/gw_F
/PSBU/gw_FOC1
/PSBU/gw_FOC1
/PSBU/gw_FOC1
/PSBU/gw_FOC1
/PSBU/gw_FOC1
/PSBU/gw_FOC1
/PSBU/gw_FOC1
localhost - EDI Driver [Starte
localhost - Logical Driver [Sta
/PSBU/gw_FOC121380CV/Door/door01 - Door1 [Up]
localhost - Historical Events Driver [Started]
localhost - Automation Driver [Started]
Status
Alarms: 7 active
cpamadmin - PSBU
Add - Door Sensor
Save and Close
General
Location
Properties
Device Groups
Audit Records
Recent Events
Properties
345210

		Default
Template name:	Door Sensor (NO)	
Vendor:	Acme Inc	
Device input:	Normally Open	☑
Supervised:	● Yes ○ No	☑
Debounce Timer (ms):	300	□
Device state:	Door Close	☑

Tip If the input device is already associated with the gateway, right-click the interface, select **Edit** and enter the debounce timer value. After setting the debounce timer the configuration must be applied on the associated gateway.

Note The default value for debounce timer is 0.

CHAPTER 9

Configuring Personnel and Badges

This chapter describes how to create the personnel records and badges used to access doors in the ICPAM system.

Note For instructions to synchronize ICPAM with personnel records from another database, see Chapter 14, “System Integration”.

Contents

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 Personnel ID of the record. If a record is imported with the same ID number, then the current record is updated with the new data.

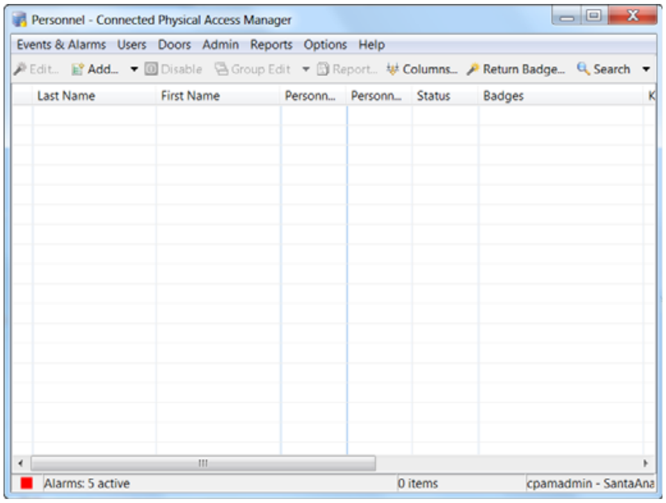
This section describes how to manage personnel, including adding an image, a badge, and an associated access policies.

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 3-14 for more information.
- To disable a record, select the entry and choose **Disable**. This is equivalent to setting the **Status** to **Inactive**.

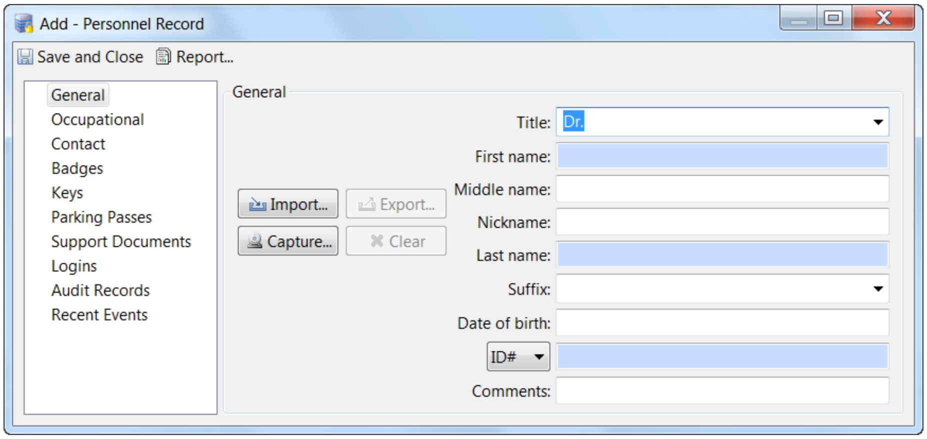
Figure 9-1 Personnel Module: Main Window



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 9-16.

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.

Figure 9-2 General



Title: Dr.

Table 9-1 Personnel Module: General Tab

Field	Description
Title	(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.
First name	(Required) The person's given name.
Middle name	(Optional) The person's middle name.
Last name	(Required) The person's surname (family name).
Suffix	(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.
Date of birth	(Optional) The person's birth date.
SSN/ID#/FIN	(Required) Select the type of ID number used from the drop-down menu, and enter the actual number in the field to the right. **Note** Personnel records are unique based on the ID number of the record. If a record is imported with the same ID number, then the current record is updated with the new data.
Comments	(Optional) Any additional comments or notes about the personnel record.
Site	(Optional) The site associated with the personnel record.
Import...	(Optional) Click **Import...** to add an image to the record (select a JPEG image from a local drive and click **OK**).

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

a. Click the **Capture...** button to open an image capture device interface.

- If a picture has already been taken, click the **Import...** button and browse to the desired JPEG image for the person's picture and click the **OK** button and skip to step 8.
- If the **Capture...** button is grayed out, enable the capture device in the properties section (see Enabling Image Capture Devices, page 9-54).

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.

In case a non-TWAIN device (like a webcam) is used, click the “capture image” button to take a snapshot of the feed from the webcam. The wizard allows the user to select a maximum 4 captures from a feed (numbered 1-4).

Double click the appropriate image from the captured images to proceed to the next step. Using the mouse move the highlighted box to the appropriate location. The area within the highlighted box will be saved within the personnel record.

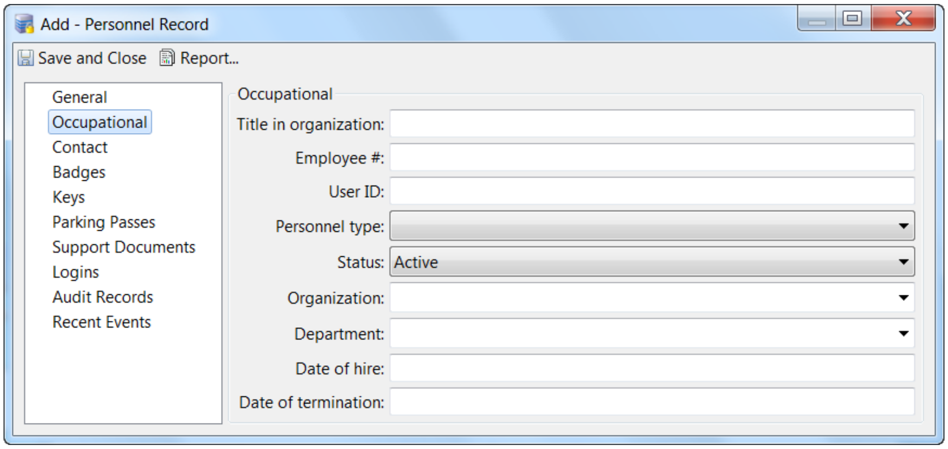
b. Click the **Save** button to save the picture or the **Capture** button to take another picture. Once the **Save** button is selected the **Capture Image** wizard will open. Using the mouse move the highlighted box to the appropriate location. The area within the highlighted box will be saved within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

c. 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, page 9-55, 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



Status: Active

Table 9-2 Personnel Module: Occupational Information Fields

Field	Description
Title in organization	The person’s title within the organization. For example, Director of Engineering.
Employee number	The employee number, if applicable. Generally, but not required to be, unique.
Personnel Type	The type of employee. Options include the following: • **Contractor** • **Employee - Full Time** • **Employee - Part Time** • **Other** • **Visitor**

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

Field	Description
Status	The status of the employee. Options include the following: • **Active** • **Inactive** • **On Leave** • **Retired** • **Terminated**
Organization	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 9-10.
Department	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 9-10.
Date of hire	The date the employee was hired.

Step 7 Enter the **Contact** for the personnel record, as shown in Figure 9-4. See Table 9-3 for field descriptions.

Figure 9-4 Contact Information

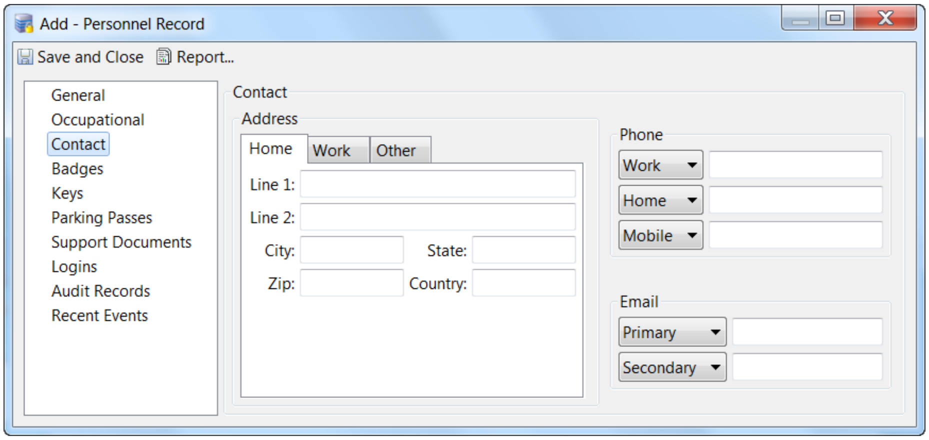


Table 9-3 Personnel Module: Contact Information Fields

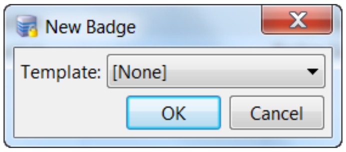
Field	Description
Address	The physical and/or mailing address(es) of the person. Each record can contain up to three different addresses: • **Work** • **Home** • **Other**
Phone numbers	The telephone number(s) for the person. Each record can contain up to five different phone numbers: • **Work** • **Home**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

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**.



Template: [None]

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

See Configuring Badge Templates, page 9-22 to create or modify the templates.

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 9-23.

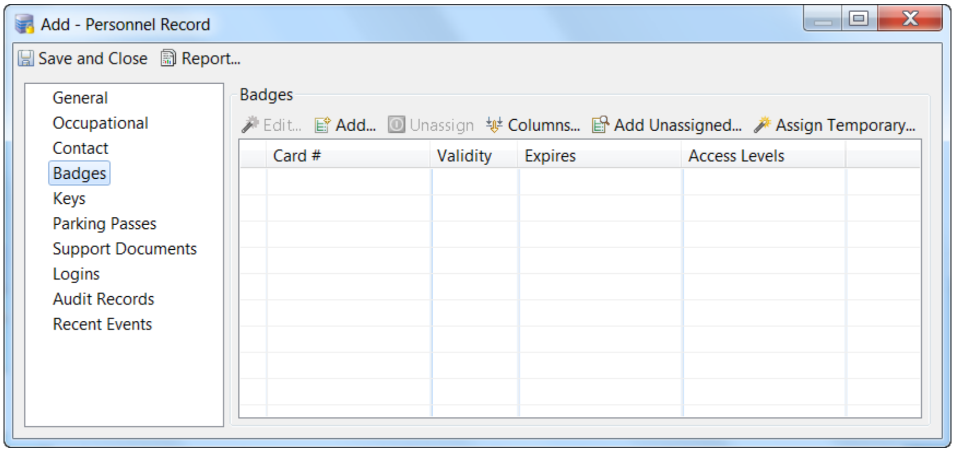
f. Click **Save and Close** to save the badge settings.

g. (Optional) Activate the changes. Changes to credentials (badges) are downloaded to the controllers 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 Tree** 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 **ICPAM Settings**. In the field **Credential download frequency (mins)**, enter the number of minutes between downloads. To activate changes to the ICPAM Settings, you must restart the ICPAM appliance. See Advanced Settings, page 17-29 for more information.

Figure 9-5 Personnel Record: Badges Window

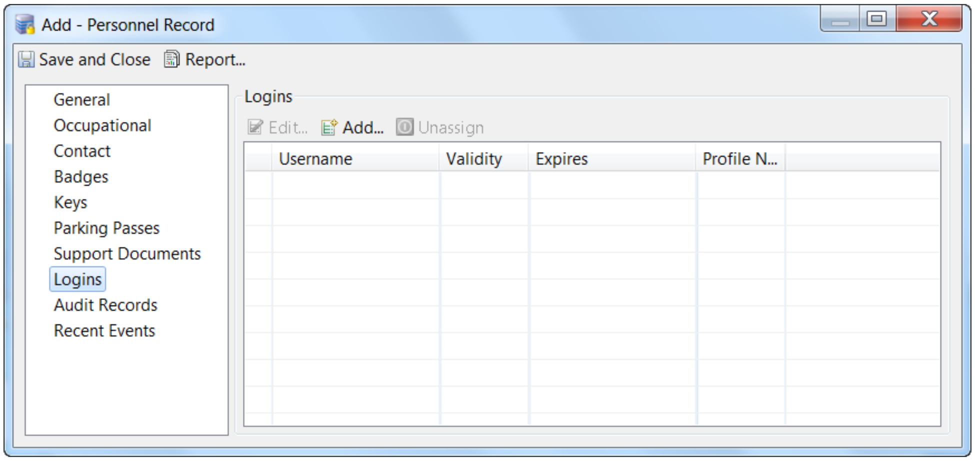


Step 9 Click the **Logins** tab to edit the logins and profiles assigned to the person. Multiple login usernames can be associated with a personnel record.

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.

Figure 9-6 Personnel Record: Logins Window



c. Complete the General settings. For field descriptions, see Creating User Login Accounts and Assigning Profiles, page 4-8.

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

e. Click **Save and Close**.

Step 10 If required, you can also specify these attributes:

- To designate one or more keys assigned to this employee, click the **Keys** tab and specify keys issued to this person.
- To specify one or more parking passes for the employee, click the **Parking Passes** tab and specify parking passes for this person.
- To include support documents required for this person, click the **Support Documents** tab and indicate those documents.

Step 11 When finished, click **Save and Close** in the **Personnel Record** window to make the changes permanent.

Downloading Credential Changes to the Controllers

By default, any changes to user credentials are automatically downloaded (applied) to the controllers 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 Tree** from the Doors menu.

Step 2 View the **Credential Download Status**.

a. Select the **Access GW Driver**.

b. Click the **Credential Download Status** tab in the Extended Status field.

c. Click the box next to the controller name to show or hide additional information, including the following:

- **Gateway Name**: the name of the controller.
- **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`.

Step 3 (Optional) To immediately download any outstanding credential changes for all controllers, right-click the **Access GW Driver**, and select the **Apply Credential Changes** command.

Otherwise, credential changes are automatically applied to all controllers every 60 minutes.

Tip To reapply the complete credential configuration for a specific controller, right-click the controller icon and select the **Download All Credentials** command. This command ensure the data is correct and should be used only if a problem exists

Viewing Audit Records and Events for Personnel Records

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

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

This section includes the following information:

- Viewing Audit Records, page 9-9
- Viewing Recent Events, page 9-10

Viewing Audit Records

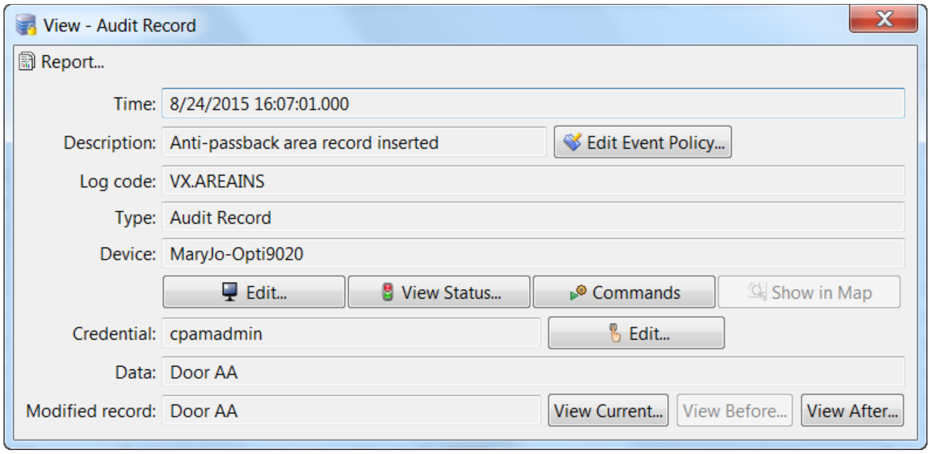
Step 1 Select **Personnel** from the **User** menu.

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

Step 3 Select **Audit Records**.

Step 4 Double-click an entry to view details for the item. Figure 9-7 describes the audit record fields.

Figure 9-7 Personnel Audit Records Window



View - Audit Record

Report...

Time: 8/24/2015 16:07:01.000

Description: Anti-passback area record inserted

Log code: VX.AREAINS

Type: Audit Record

Device: MaryJo-Opti9020

Credential: cpamadmin

Data: Door AA

Modified record: Door AA

Table 9-4 View Audit Record Screen

Field	Description
Time	The time and date when the modification occurred.
Type	The type of change.
Description	A description of the change.
Device	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.
Credential	The username used when the modification occurred. Click **View** to display and revise details for the username.
Data	Additional information about the modification.

Table 9-4 View Audit Record Screen

Field	Description
View Current...	Opens a new window displaying the current settings.
View Before...	Opens a new window displaying the settings before the change was made.
View After...	Opens a new window displaying the settings after the change was made.

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 9-5 Personnel Module: Recent Events Fields

Field	Description
Time	The time and date when the event occurred.
Description	A description of the event.
Device	The device associated with the event.
Address	The address of the device.
Personnel Record	The personnel record associated with the event.
Data	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.
Credential	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.
Site	The site where the event occurred.

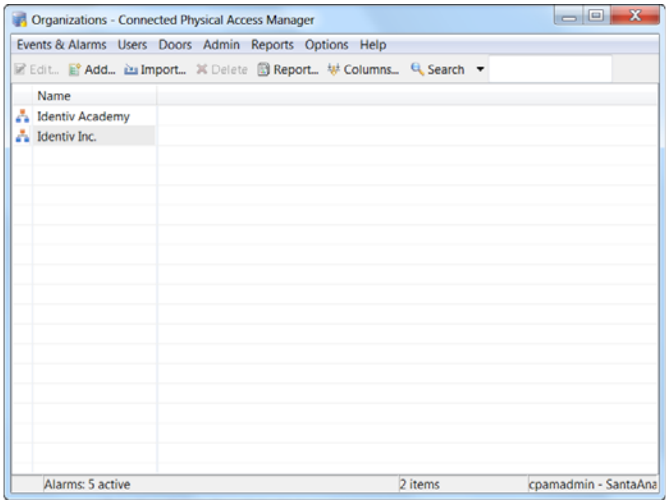
Editing Organization and Department Lists

Personnel records include an organization and department for the user (see the Occupational section of Personnel configuration, as described in Configuring Personnel, page 9-1, Step 6).

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

Step 1 Select **Organization** from the Users menu, as shown in Figure 9-8.

Figure 9-8 Organizations: Main Window



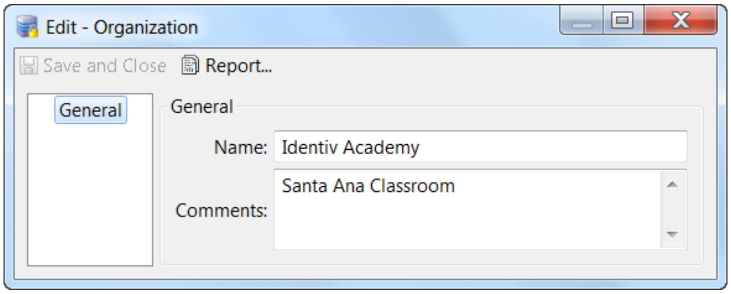
Name
Identiv Academy
Identiv Inc.

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 9-9.

Figure 9-9 Organizations: General Settings



Name: Identiv Academy

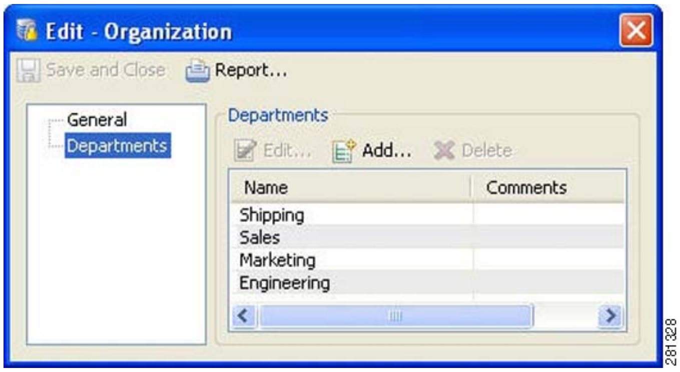
Comments: Santa Ana Classroom

Step 4 Enter the name of the organization and optional comments to describe the entry.

Step 5 Click the **Department** tab to edit the list of departments for the organization (Figure 9-10).

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**.

Figure 9-10   Organizations: Departments Window



Name	Comments
Shipping	
Sales	
Marketing	
Engineering	

Step 7 Click **Save and Close** to return to the main window.

Step 8 Click **Save and Close** again to save the organization and department changes and close the main window.

Importing Personnel Records Using a Comma Separated Value (CSV) File

Large amounts of personnel records can be added to ICPAM 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 ICPAM.

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 ICPAM configuration. Add the Organization values by manually creating them or through a data import. See Editing Organization and Department Lists, page 9-10 for more information.

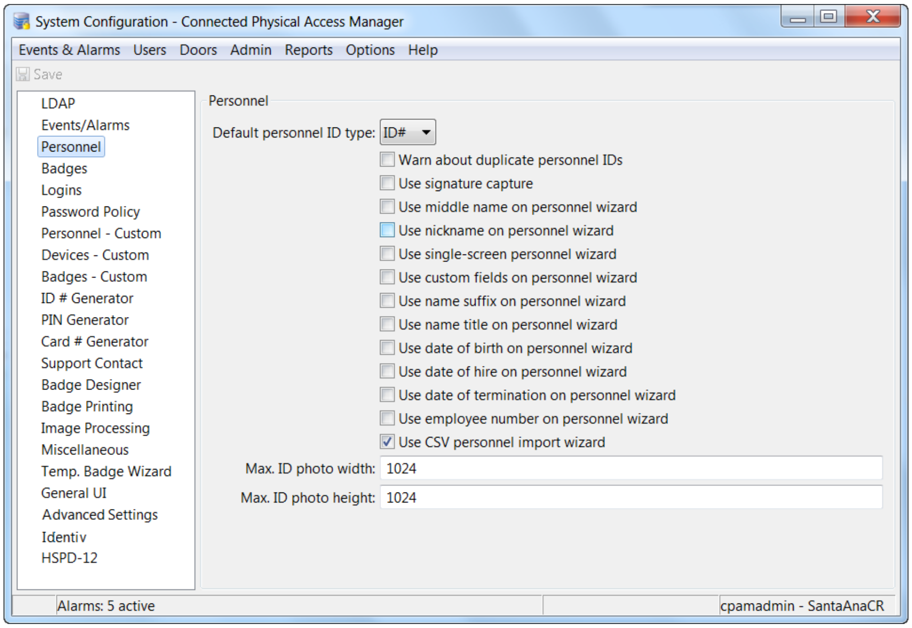
Once a personnel CSV file is extracted from a database it can be added to ICPAM using the following process:

Step 1 Enable the CSV personnel import wizard.

a. Select **System Configuration** in the **Admin** menu.

b. Select the **Personnel** tab (Figure 9-11).

Figure 9-11 System Configuration Personnel tab



Personnel

Default personnel ID type: ID#

□ Warn about duplicate personnel IDs
□ Use signature capture
□ Use middle name on personnel wizard
□ Use nickname on personnel wizard
□ Use single-screen personnel wizard
□ Use custom fields on personnel wizard
□ Use name suffix on personnel wizard
□ Use name title on personnel wizard
□ Use date of birth on personnel wizard
□ Use date of hire on personnel wizard
□ Use date of termination on personnel wizard
□ Use employee number on personnel wizard
☑ Use CSV personnel import wizard

Max. ID photo width: 1024

Max. ID photo height: 1024

Alarms: 5 active cpamadmin - SantaAnaCR

c. Select the check box for **Use CVS personnel import wizard**.

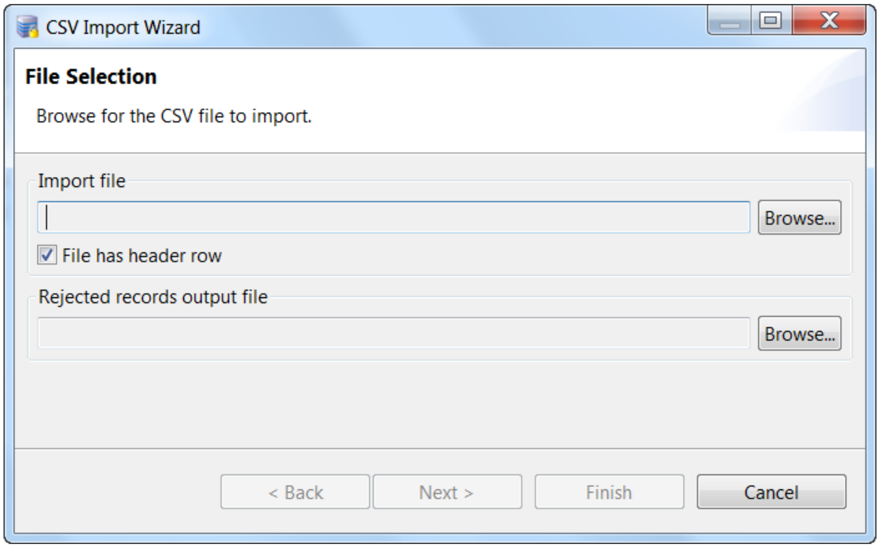
d. Click **Save**.

e. Log out and log back in to the ICPAM 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 9-12 CSV File Selection



CSV Import Wizard

File Selection

Browse for the CSV file to import.

Import file

Browse...

☑ File has header row

Rejected records output file

Browse...

Step 4 In the File Selection window, select the file to import into ICPAM, as shown in Figure 9-12.

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

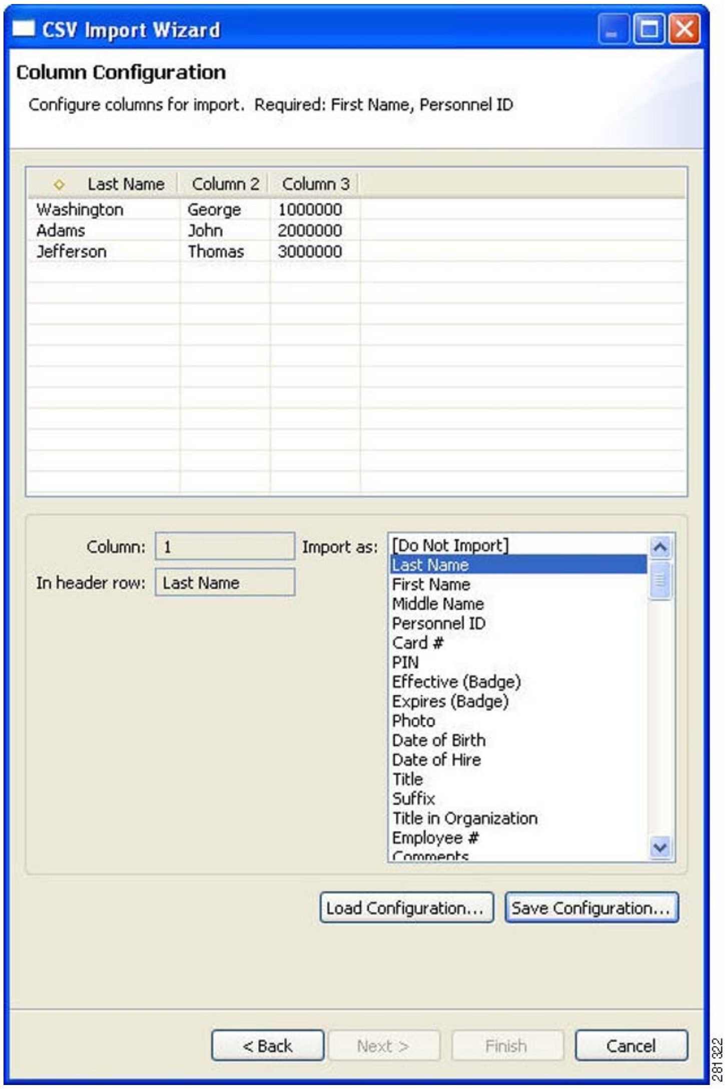
b. Select the check box for **File has a header row** if the CVS file includes data for a header row.

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

d. Click **Next**.

Step 5 In the **Column Configuration** window (Figure 9-13), 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 9-13 CSV Import Column Selection



CSV Import Wizard

Column Configuration

Configure columns for import. Required: First Name, Personnel ID

Last Name	Column 2	Column 3
Washington	George	1000000
Adams	John	2000000
Jefferson	Thomas	3000000

Column: 1

In header row: Last Name

Import as: [Do Not Import], **Last Name** (selected), First Name, Middle Name, Personnel ID, Card #, PIN, Effective (Badge), Expires (Badge), Photo, Date of Birth, Date of Hire, Title, Suffix, Title in Organization, Employee #, Comments

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 ICPAM database.

Step 6 Assign a ICPAM field for each CSV field to be imported (Figure 9-13). 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.

a. Select the **Import as** field in the lower right-hand window. This defines the ICPAM field that corresponds with the selected CSV field.

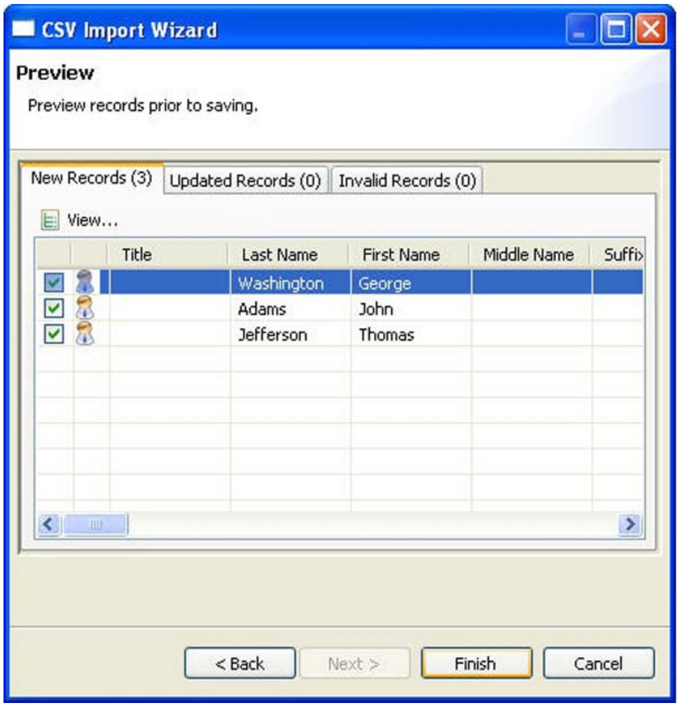
b. Assign all CSV columns to an **Import as** field.

c. Click **Next**. The **Next** button is not enabled until all CSV fields are assigned.

Note Personnel photos in the `.jpg` format can be imported. The CSV field assigned to the ICPAM 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 7 In the Preview window, verify the records and fields before importing, as shown in Figure 9-14.

Figure 9-14 CSV Preview



CSV Import Wizard

Preview

Preview records prior to saving.

New Records (3) | Updated Records (0) | Invalid Records (0)

View...

		Title	Last Name	First Name	Middle Name	Suffi>
☑			Washington	George		
☑			Adams	John		
☑			Jefferson	Thomas		

- **New Records** and **Updated Records** tabs: Select or deselect the check box 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 8 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 9-16
- Scan a License to Create a New Personnel Record, page 9-20

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

Install and Configure the SnapShell Scanner

Note 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 ICPAM 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 ICPAM 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 9-15).

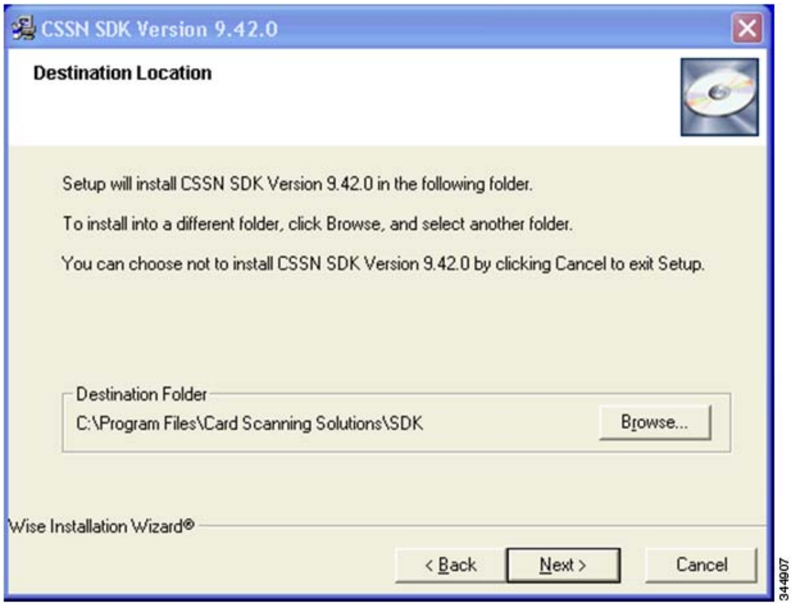
Step 3 Click **Run**, **Continue**, **OK**, or **Next** when prompted to accept the default settings and options.

a. In the Destination Location window (Figure 9-15), record the directory where the software is installed.

For example: `C:\Program Files\Card Scanning Solutions\SDK`

Note The installation directory path is used to update the Windows environmental variables to recognize the new scanner, as described in the following steps.

Figure 9-15 SnapShell Scanner Destination Location



CSSN SDK Version 9.42.0

Destination Location

Setup will install CSSN SDK Version 9.42.0 in the following folder.

To install into a different folder, click Browse, and select another folder.

You can choose not to install CSSN SDK Version 9.42.0 by clicking Cancel to exit Setup.

Destination Folder
C:\Program Files\Card Scanning Solutions\SDK

Note 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 4 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 9-15.

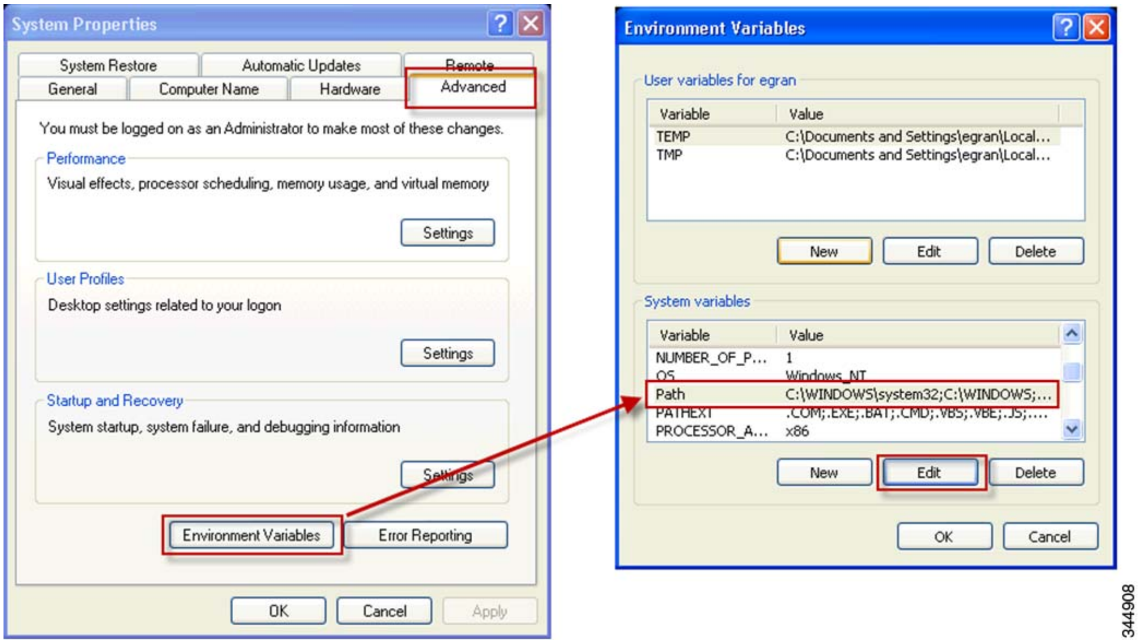
a. Right click **My Computer**.

b. Select **Properties**.

c. Select **Advanced**.

d. Click the **Environmental Variables** button (Figure 9-16).

Figure 9-16 Windows Environmental Variables



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

User variables for egran

Variable	Value
TEMP	C:\Documents and Settings\egran\Local...
TMP	C:\Documents and Settings\egran\Local...

System variables

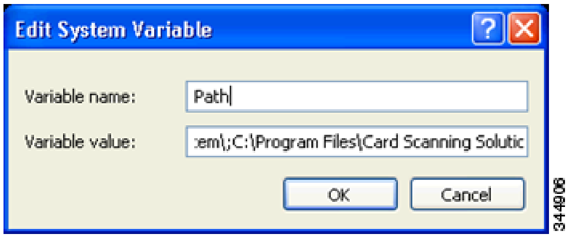
Variable	Value
NUMBER_OF_P...	1
OS	Windows_NT
Path	C:\WINDOWS\system32;C:\WINDOWS;...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;....
PROCESSOR_A...	x86

e. Select **Path** from the System Variables list (Figure 9-16).

f. Click **Edit** (Figure 9-16).

The Edit System Variables window appears (Figure 9-17).

Figure 9-17 Edit System Variables



Variable name: Path

Variable value: :em\;C:\Program Files\Card Scanning Solutic

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 5 Connect the scanner USB cable to a PC USB port.

Step 6 Enable the scanner in the ICPAM System Configuration.

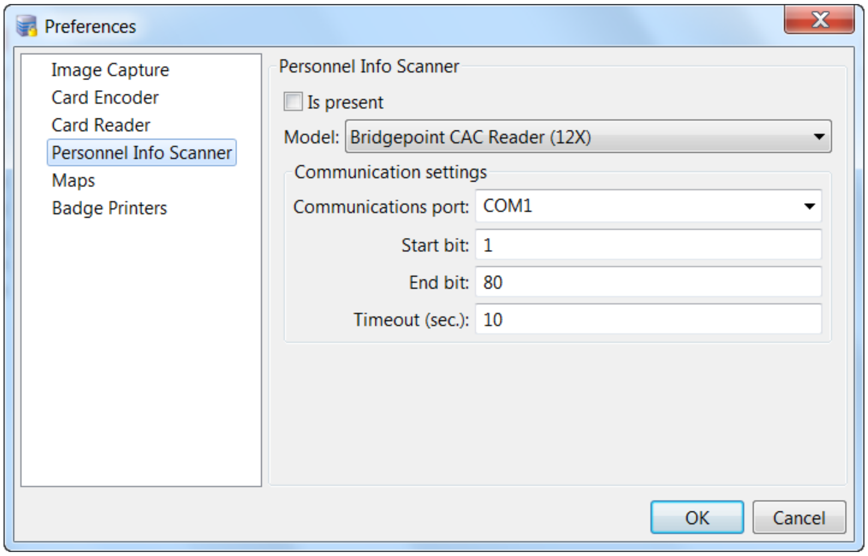
a. Launch the ICPAM desktop client.

See the "Logging into ICPAM Client" section on page 3-3.

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

c. Select **Personnel Info Scanner** (Figure 9-18).

Figure 9-18 Preferences for the Personnel Info Scanner



Personnel Info Scanner

☐ Is present

Model: Bridgepoint CAC Reader (12X)

Communication settings

Communications port: COM1

Start bit: 1

End bit: 80

Timeout (sec.): 10

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 ICPAM 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 9-16.

Step 2 Log on to the ICPAM desktop client.

See the "Logging into ICPAM Client" section on page 3-3.

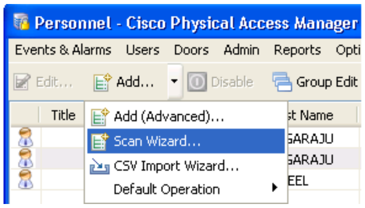
Step 3 Select **Personnel** from the **Users** menu.

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 9-19).

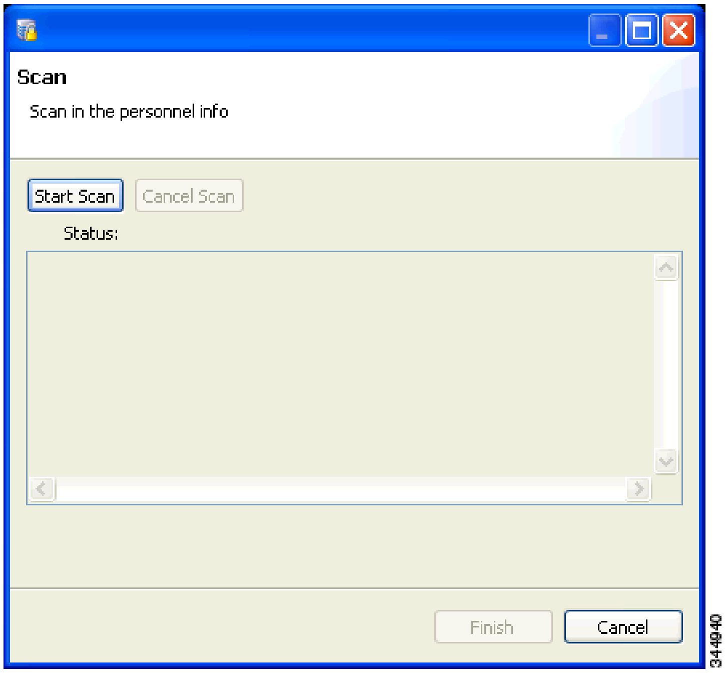
Figure 9-19 Scan Wizard in the Personnel Module



Note The Scan Wizard menu option only appears if the scanner was enabled. See the "Install and Configure the SnapShell Scanner" section on page 9-16.

Step 6 Select **Start Scan** (Figure 9-20).

Figure 9-20 Scan Wizard


Scan
Scan in the personnel info

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 9-1 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.

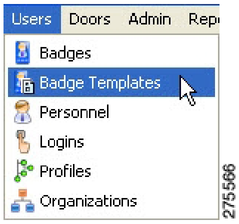
- Configuring Badge Templates, page 9-22
- Badge Properties, page 9-23
- Badge Authentication, page 9-32
- Printing Badges, page 9-44

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.

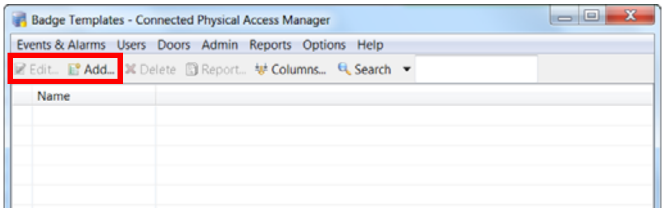
Configuring Badge Templates

To configure a badge template:

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

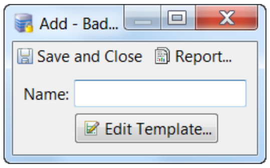


Step 2 Click **Add**, or select an existing template and click **Edit**.



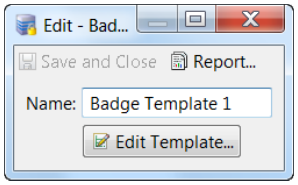
Step 3 Do one of these:

- If you select Add, the Add Badge Template dialog appears:



Enter the new template name then click **Edit Template**.

- If you select Edit, the Edit Badge Template dialog appears. Click **Edit Template**.

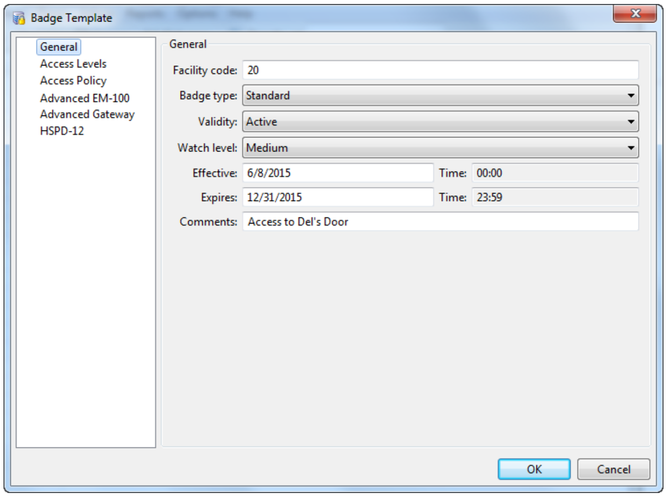


Name: Badge Template 1

Step 4 Follow these steps:

a. Enter the badge properties. See Badge Properties, page 9-23 for field descriptions.

b. Click **OK**.



General

Facility code: 20

Badge type: Standard

Validity: Active

Watch level: Medium

Effective: 6/8/2015 Time: 00:00

Expires: 12/31/2015 Time: 23:59

Comments: Access to Del's Door

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 most often-used 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.

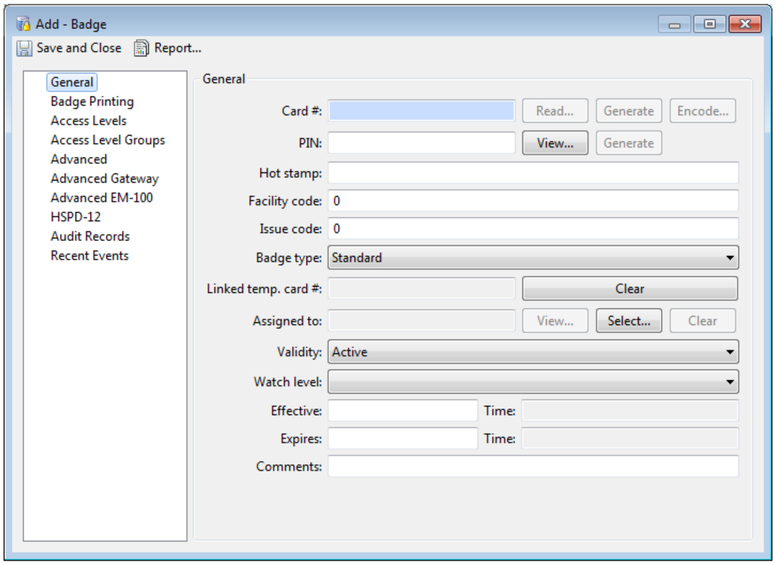
This section includes the following information:

- Badges Module: General, page 9-24
- Badges Module: Access Policies, page 9-27
- Badges Module: Advanced, page 9-27
- Badges Module: Advanced Gateway, page 9-28
- Badges Module: Advanced EM-100, page 9-29
- Badges Module: HSPD-12 Badge Extension, page 9-30
- Badges Module: Audit Records, page 9-31
- Badges Module: Recent Events, page 9-31

Badges Module: General

The General tab as shown in Figure 9-21 includes basic information about the badge.

Figure 9-21 Badges Module: General Window



Facility code: 0
Issue code: 0
Badge type: Standard
Validity: Active

The fields in this window are explained in Table 9-6.

Table 9-6 Badges Module: General Fields

Field	Description
Card #	(Required) Also known as a badge. A type of credential encoded with a card number, generally on a magnetic stripe or internally like a proximity card, and used to enter access points. **Tip** If unsure what the card # is on the card, use the card in the access-control system reader. Open the **Events** module and view the event with the description **Access denied: Card not in database**. The **Data** field of the event displays the card number read from the card. See Viewing Audit Records and Events for Personnel Records, page 9-9.
PIN	(Required) Personal Identification Number. A badge has a PIN associated with it, which, depending on the configuration of an access point, is entered into the keypad on the access point's reader.
Hot stamp	(Optional) The number physically printed or embossed on a badge. This number is generally independent of the Card Number. Not all badges have a hot stamp number.
Facility code	(Optional) A segment of bits encoded on a card that represent a number for a facility. Often all cards issued for a single facility have the same facility code.
Exempt from Anti-passback	(Optional) If the access point is configured for anti-passback, the badge is exempt from anti-passback enforcement.

Table 9-6 Badges Module: General Fields (continued)

Field	Description
Grant One Free APB Pass	(Optional) The badge holder will be anti-passback exempt during the next reader use only.
Badge Type	The type of badge. The options are: • **Standard** • **Temporary** • **Visitor**
Assigned to	(Optional) The personnel record the badge is assigned to.
Validity	(Optional) The current status of the badge. Only the **Active** option provides access for the badge. The options include: • **Active:** Must be set to this value for access to be granted. • **Inactive:** Access is denied for all access points in system. • **Lost:** Access is denied for all access points in system. • **Stolen:** Access is denied for all access points in system. • **Destroyed:** Access is denied for all access points in system. To define new validity types, refer to Credential Validity Types, page 9-25.
Effective	(Optional) The beginning date the badge can be used in the system. If blank, badge access begins immediately. **Note** If a date is entered, the badge can be used at 12.00 AM on the specified day.
Expires	(Optional) The date the badge expires. If blank, the badge never expires. **Note** If a date is entered, the badge expires at 12.00 AM on the specified day.
Site	(Optional) A site is a single instance of a ICPAM database.
Comments	(Optional) Any additional comments or notes about the badge.

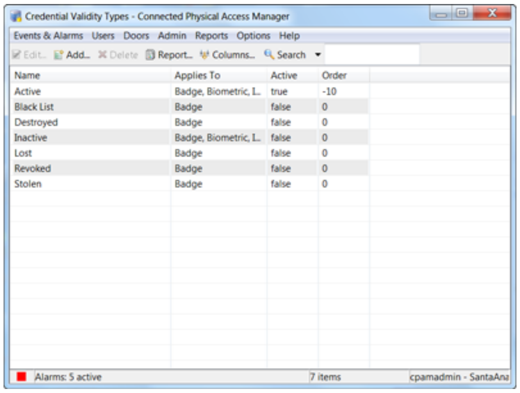
Credential Validity Types

Credential validity types are supplied as options in the drop-down 'Validity' field of the Badges General page (Badges Module: General, page 9-24) for both Badges and Badge Templates. There are several options that are supplied as default, but the qualified administrator can define more options as the need arises.

To define new types of credential validity:

Step 1 From the **Admin** menu, select the **Credential Validity Types** option.

The Credential Validity Types window appears:


Credential Validity Types - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Delete Report... Columns... Search

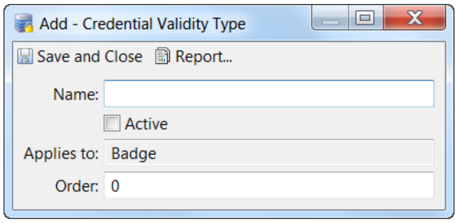
Name	Applies To	Active	Order
Active	Badge, Biometric, L...	true	-10
Black List	Badge	false	0
Destroyed	Badge	false	0
Inactive	Badge, Biometric, L...	false	0
Lost	Badge	false	0
Revoked	Badge	false	0
Stolen	Badge	false	0

Alarms: 5 active 7 items cpamadmin - SantaAna

Notice that the default field options appear in this window.

Step 2 Click **Add...**

The Add Credential Validity Type dialog box appears.



Name:

□ Active

Applies to: Badge

Order: 0

Step 3 Fill in the form as needed. The fields included on this form include:

Name	Enter the name of this new type
Active	Check this box to indicate that this type is currently active.
Applies to:	Enter the type of item (device) to which this option applies. The default value is **Badge**.
Order	Enter the order in which this option is presented in the option list.

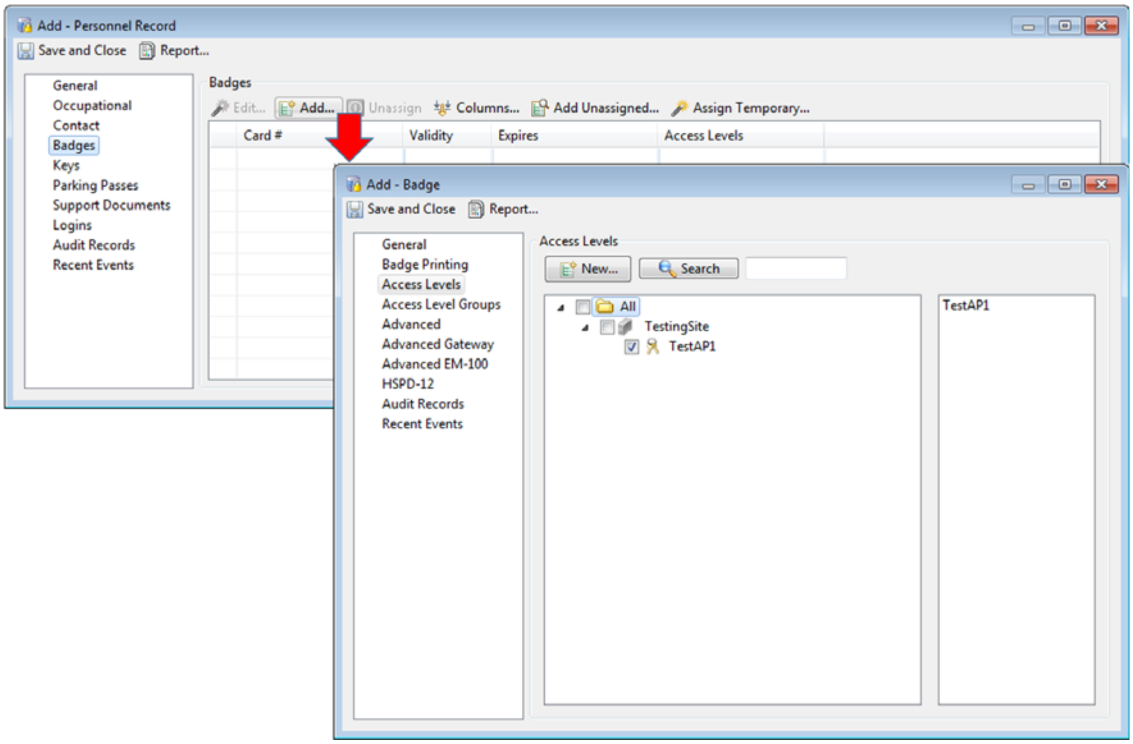
Step 4 Click **Save and Close**.

The new credential validity type appears in the credential validity type window.

Badges Module: Access Policies

Select the door access policies for the user badge. See Configuring Access Policies, page 11-2.

Figure 9-22 Adding Badges from Personnel Record Option

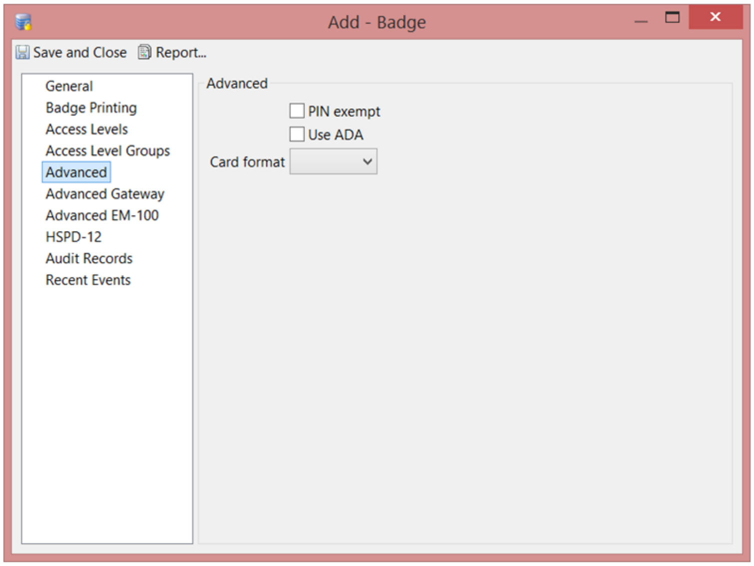


Note In ICPAM 2.1, when a user assigns access policies to a badge, both the access policies up to the root of the location hierarchy for the logged-in user and the levels in the location of the user are available for selection. This feature is applicable only if the profile enhancement feature is set in the configuration settings. For more information on this, see Logins Settings, page 17-10.

Badges Module: Advanced

The Advanced option window is shown in Figure 9-23.

Figure 9-23 Advanced Screen



□ PIN exempt

□ Use ADA

Card format

Table 9-7 describes the settings for the Advanced option.

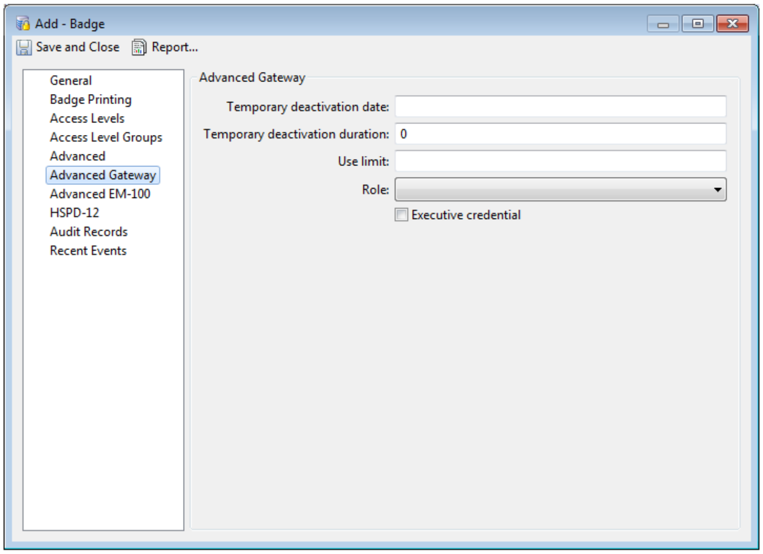
Table 9-7 Badges Module: Advanced Fields

Field	Description
PIN exempt	Check this box to ensure that the designated badge is exempt from using a PIN for authorization on either the gateway or EM-100 reader.
Use ADA	Check this box to specify that this badge uses ADA specifications for its use at either the gateway or EM-100 reader.
Card format	From the drop-down box, specify the card format this badge can use. Only those card formats previously defined for this system appear in the list. For more on creating card formats, refer to Configuring Credential Templates.

Badges Module: Advanced Gateway

The Advanced Gateway option window is shown in Figure 9-24.

Figure 9-24 Advanced Gateway Screen



Temporary deactivation date:

Temporary deactivation duration: 0

Use limit:

Role:

□ Executive credential

Table 9-8 describes the settings for the Advanced Gateway.

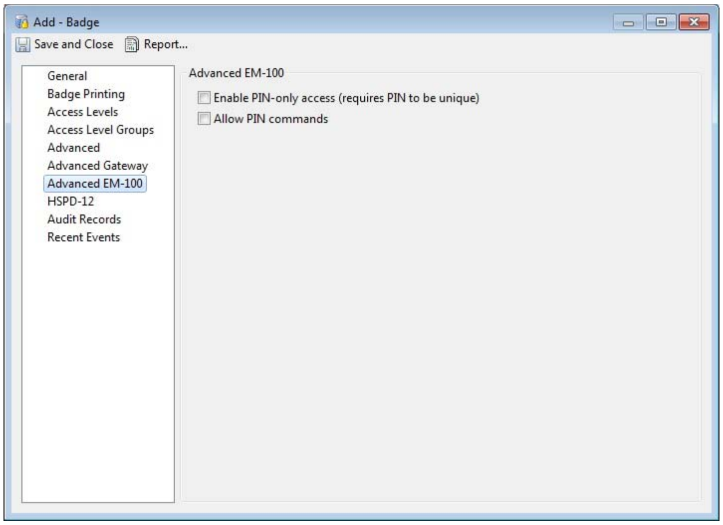
Table 9-8 Badges Module: Advanced Gateway Fields

Field	Description
Temporary deactivation date	(Optional) The start date to temporarily deactivate a badge. Click on the entry field to open a pop-up calendar, and then double-click to select a date. For example, to deactivate a badge for a one-week vacation beginning January 1, select the date from the pop-up calendar, and then enter **7** in the following **duration** field. If a date is entered, the badge deactivation begins at 12.00 AM on the specified day.
Temporary deactivation duration	(Optional) The duration of the temporary deactivation, in days. For example, to deactivate a badge for a 7 day vacation, enter **7**.
Use limit	(Optional) The maximum number of times a badge can be used. When the limit is reached, the badge is deactivated.
Role	The role of the person who carries the badge: Employee, Contractor, Vendor, Temporary, Employee_full_time, Employee_part_time, Intern, Visitor, or Other.
Executive credential	If checked, specifies that the badge belongs to an executive.

Badges Module: Advanced EM-100

The Advanced EM-100 option window is shown in Figure 9-25.

Figure 9-25 Advanced EM-100



☐ Enable PIN-only access (requires PIN to be unique)

☐ Allow PIN commands

Table 9-9 describes the fields appearing in this window.

Table 9-9 Badges Module: Advanced EM-100 Fields

Field	Description
Enable PIN-only access (requires PIN to be unique)	Check this box to enable this badge to use PIN-only access at an EM-100 reader. This requires that the badge PIN be unique.
Allow PIN commands	Check this box to allow this badge to use PIN commands at an EM-100 reader.

Badges Module: HSPD-12 Badge Extension

Table 9-10 describes the HSPD-12 Smart Card badge extension settings.

Note The HSPD-12 badge extension is experimental and may be changed or removed in future ICPAM releases. For this reason, the extension should not be used in a production setting.

Table 9-10 Badges Module: HSPD-12 Badge Extension Fields

Field	Description
Full name	The full name of the card holder.
Agency Code	Identify the government agency issuing the credential.
System Code	Identifies the system that issued the card
Credential Number	The number encoded by the issuing agency.Only one credential number can be active in a system.
Credential Series	Credential series code used to reflect major system changes.
ICI	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`.

Table 9-10 Badges Module: HSPD-12 Badge Extension Fields (continued)

Field	Description
Full name	The full name of the card holder.
FASC-N	The Federal Agency Smart Credential Number. This data is in the BCD (Binary coded decimal) format and is comprised of fields such as Agency Code, System Code, Credential Number, Credential Series, Individual Credential Issue code, and other fields.
Expiration date	The date the credential expires and is deemed invalid.
Card Type	The specified Smart Card credential type. The currently supported type is PIV.

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 9-11 Badges Module: Audit Records Fields

Field	Description
Time	The time and date when the modification occurred.
Type	The type of change made.
Description	A description of the modification: what type of record was modified, and whether it was inserted, updated, or deleted.
Device	The name of the workstation device where the modification occurred.
Credential	The login that the operator was logged in with when the modification occurred.
Data	Additional information about the modification.
View Current...	Opens a new window displaying the current settings.
View Before...	Opens a new window displaying the settings before the change was made.
View After...	Opens a new window displaying the settings after the change was made.

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 9-12 Badges Module: Recent Events Fields

Field	Description
Time	The time and date when the event occurred.
Description	A description of the event.
Device	The device associated with the event.
Address	The address of the device.
Personnel Record	The personnel record associated with the event.

Table 9-12 Badges Module: Recent Events Fields (continued)

Field	Description
Data	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.
Credential	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.
Site	The site where the event occurred.

Badge Authentication

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

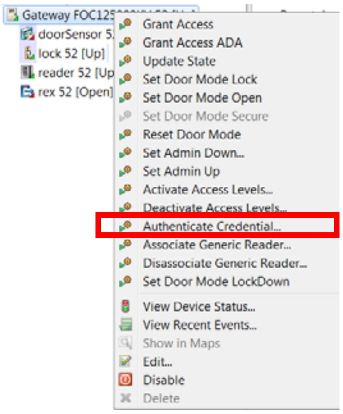
Procedure

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

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

Step 3 Enter the badge ID and timestamp.

Figure 9-26 Authenticate Credential



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

Select the **ICPAM** option to perform badge authentication at the ICPAM 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 ICPAM server and the controller (one at a time).
- Doors configured with an APB policy can only verify badge authentication at the ICPAM 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

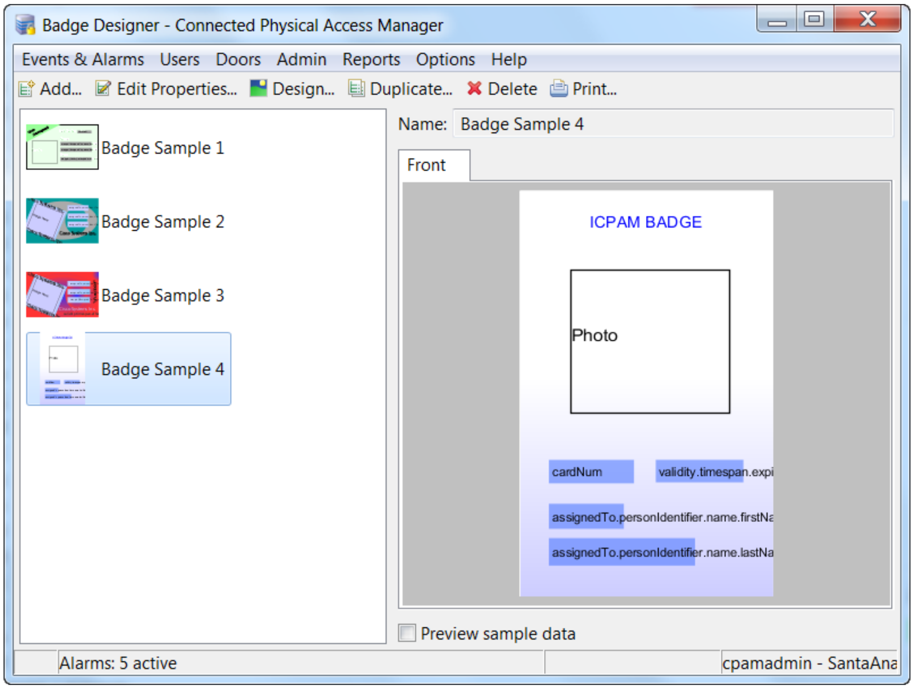
- The **Authenticate Credential** door command does not support facility code based authentication (if the door is configured based on facility code authentication).
- The command does not authenticate the badge based on a Badge ID and Pin Number combination.
- The command does not support Pin Exempt 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 Policies and Activate Access Policies** 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.

Figure 9-27 Badge Designer Main Window



Name: Badge Sample 4

□ Preview sample data

Alarms: 5 active

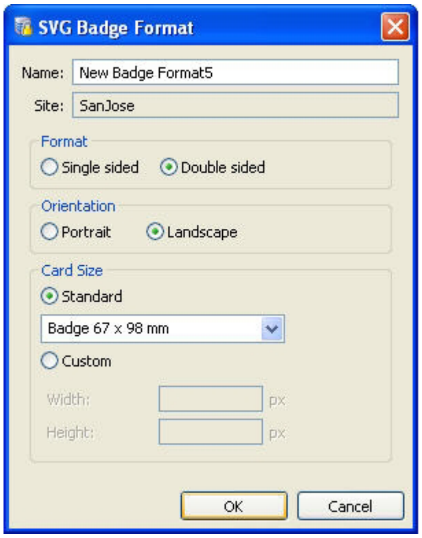
cpamadmin - SantaAna

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 **Preview Sample Data** check box 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 9-28.

Figure 9-28 New Badge Format



Name: New Badge Format5

Site: SanJose

Format: ○ Single sided ● Double sided

Orientation: ○ Portrait ● Landscape

Card Size: ● Standard

Badge 67 x 98 mm

○ Custom

Width: px

Height: px

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.

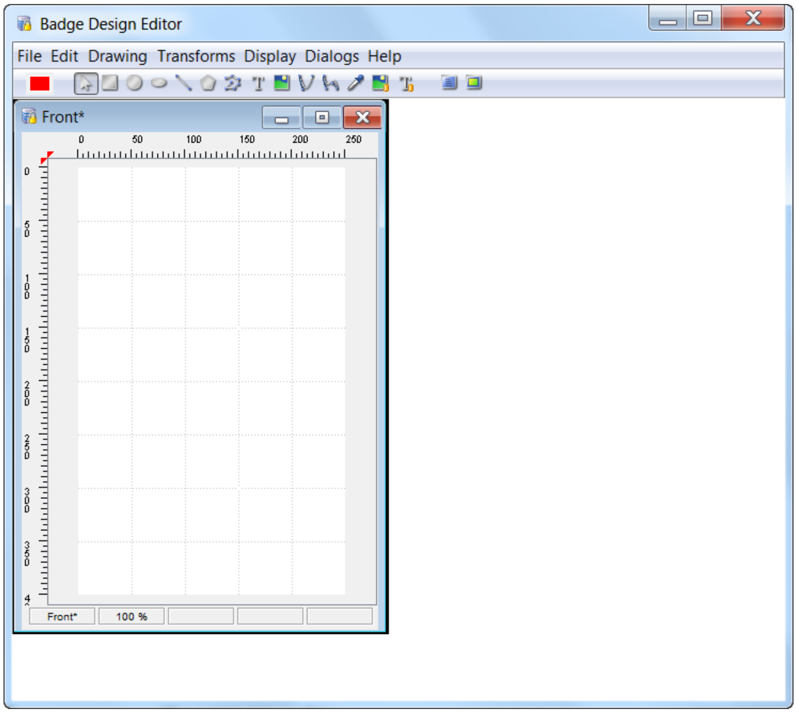
d. **Card Size**: Select a standard size, or enter custom dimensions. Standard size options include:

- 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** 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 9-29.

Figure 9-29 Badge Designer Editor



Step 6 Use the **Tool Bar** icons at the top of the window to design the template. The icons include the following tools (from left to right):

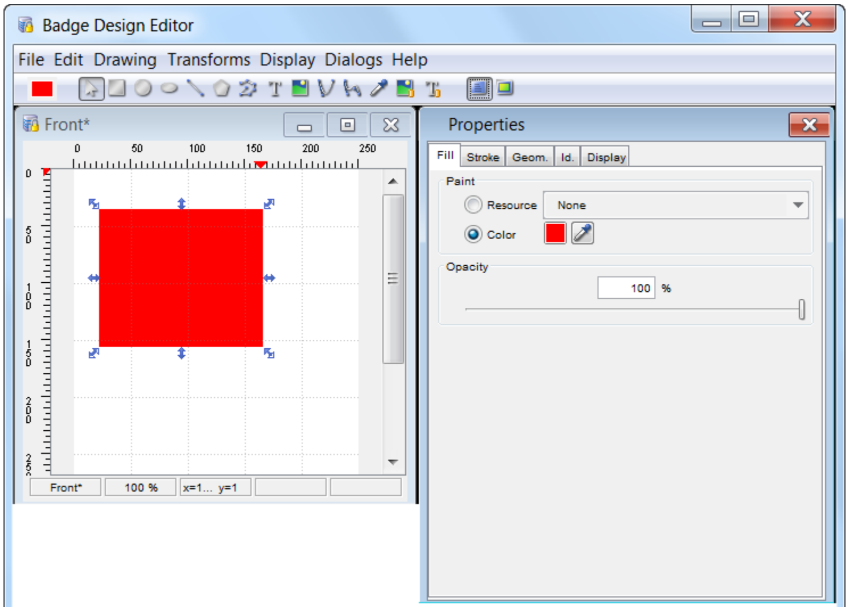
Tip Hold the mouse cursor over an icon to view the icon title.

- **Color**: Click the icon to select a color and then drag and drop the color on a shape to apply that color.
- **Mouse Pointer Tool**: Select and move objects on the badge template.
- **Rectangle Tool**: Draw rectangle objects.
- **Circle Tool**: Draw a circle.
- **Ellipse Tool**: Draw an ellipse.
- **Line Tool**: Draw a line.
- **Polygon Tool**: Draw a polygon.
- **Polyline Tool**: Draw an a polygon with operator defined line lengths.
- **Text**: Add text to the template.
- **Image**: Add an image to the template.
- **Quadratic Bezier Curve**: Create a line between 3 points.
- **Cubic Bezier Curve**: Create a line between 4 points.
- **Color Picker Tool**: Select a color from the palette.
- **Image Link**: Create an image link to the ICPAM database. Options include: personnel photos or signatures.

- **Text Link**: Create a text link to the ICPAM 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 9-30.

Figure 9-30 Badge Designer Editor: Rectangle Tool



Paint

○ Resource None

● Color

Opacity 100 %

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:

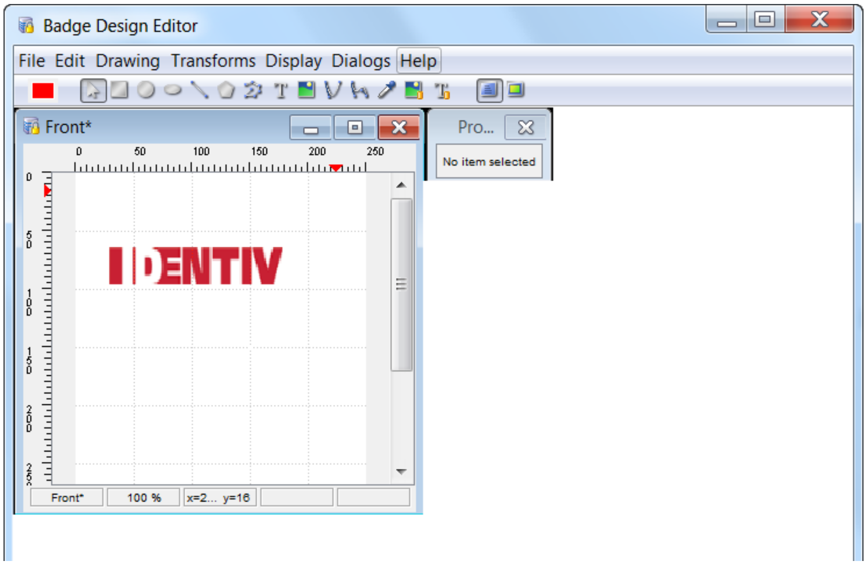
a. Click the **Image** button.

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 9-31.

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

Figure 9-31 Badge Design Editor: Logo



Step 11 To add a dynamic text field to the badge template:

a. Click the **Text Link** button in the **Tool Bar**.

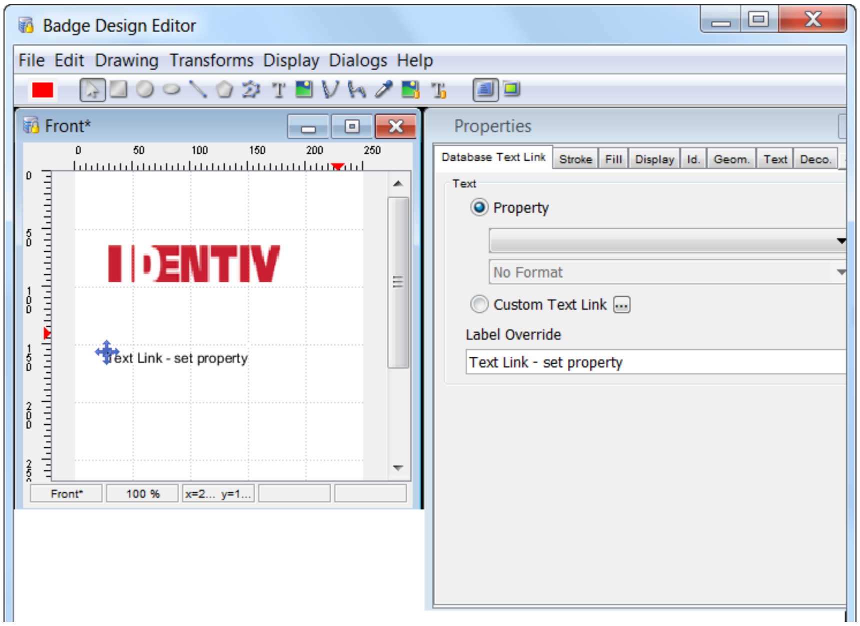
b. In the **Properties** section select the **Database Text Link** tab, as shown in Figure 9-32.

c. In the field drop-down select the correct text link. This text link extracts the field from the database. For example the **Title** text link field extracts the personnel title from the database.

d. (Optional) In the **Properties** section select the other attributes of the text, such as size and font.

e. Click and drag the text to a desired location.

Figure 9-32 Badge Design Editor: Database Text Link



Text

● Property

No Format

○ Custom Text Link

Label Override: Text Link - set property

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.

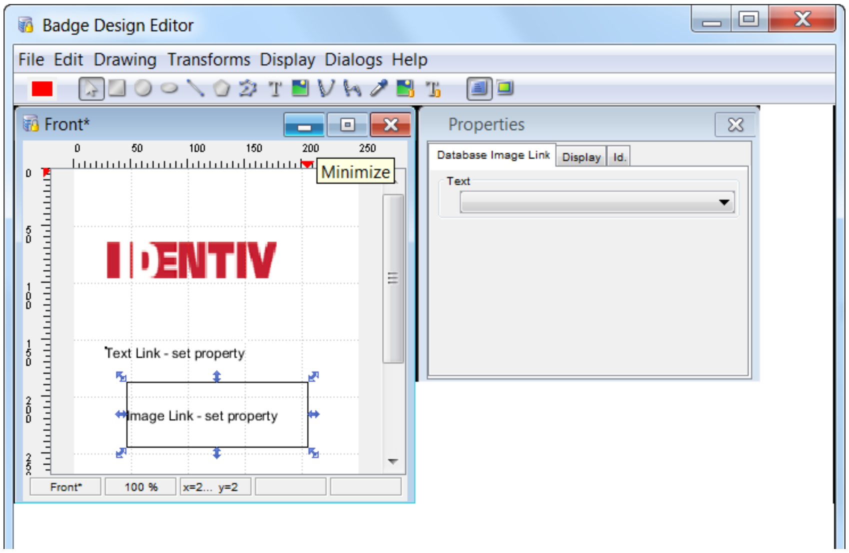
c. In the **Properties** section select the **Database Image Link** tab.

d. In the field drop-down select **Photo**, as shown in Figure 9-33. 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 to achieve the best possible print quality. See Printing High Resolution Images, page 9-50 for more information.

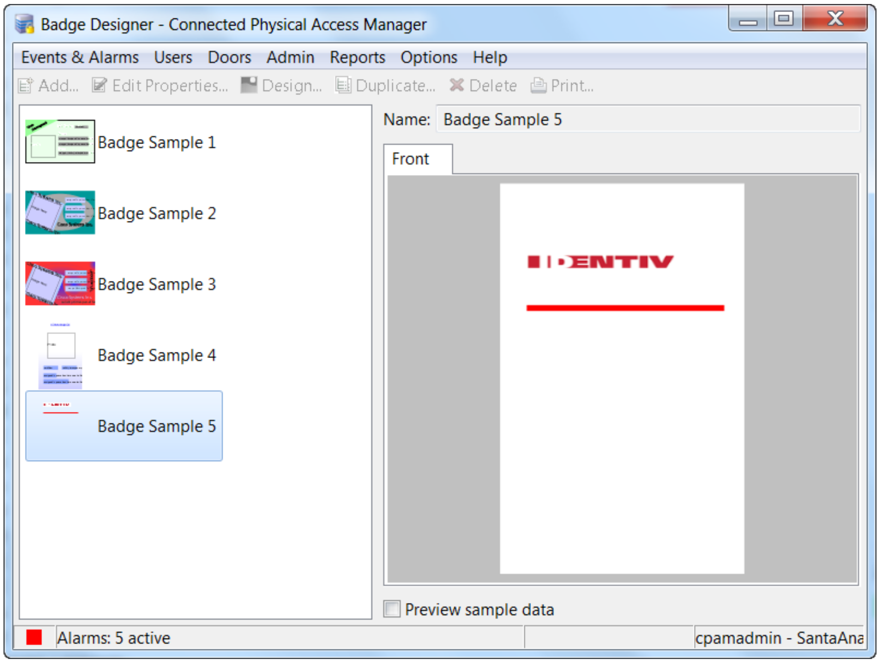
Figure 9-33   Badge Designer Editor: Database Image Link



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**. The new template appears in the **Badge Designer**, as shown in Figure 9-33.

Figure 9-34   Badge Designer With New Template


Badge Designer - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Add... Edit Properties... Design... Duplicate... Delete Print...
Badge Sample 1
Badge Sample 2
Badge Sample 3
Badge Sample 4
Badge Sample 5
Front
IDENTIV
□ Preview sample data
Alarms: 5 active
cpamadmin - SantaAna

Name: Badge Sample 5

Installing and Using a Barcode Font

To use barcode fonts for printing certain fields on a badge that is designed using the ICPAM badge designer, you can add the desired font to the system and use it with the Badge Designer.

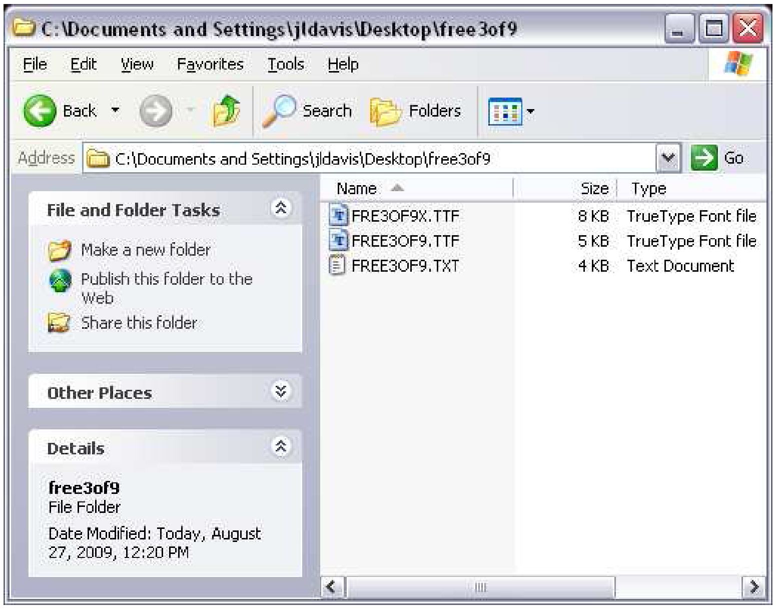
To install the barcode font, follow the process:

Note For the following process, 3 of 9 barcode font is used.

Step 1 Download 3 of 9 font using attached font or from a webpage.

Step 2 Unzip the font archive.

Figure 9-35 Documents and settings window



Address: C:\Documents and Settings\jldavis\Desktop\free3of9

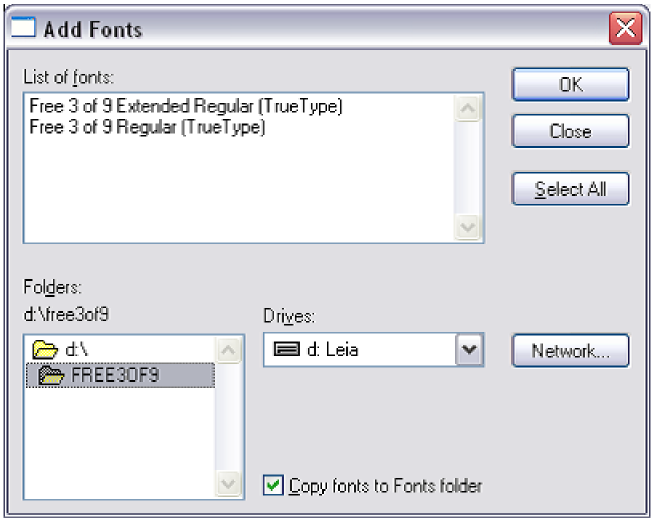
Name	Size	Type
FRE3OF9X.TTF	8 KB	TrueType Font file
FREE3OF9.TTF	5 KB	TrueType Font file
FREE3OF9.TXT	4 KB	Text Document

free3of9
File Folder
Date Modified: Today, August 27, 2009, 12:20 PM

Step 3 Navigate to **Settings**> **Control Panel** > **Fonts**.

Step 4 Click **File**> **Install**> **New Font**, and browse to the location of the unzipped font files

Figure 9-36 Add Fonts



Add Fonts

List of fonts:
Free 3 of 9 Extended Regular (TrueType)
Free 3 of 9 Regular (TrueType)

Folders:
d:\free3of9
d:\
FREE3OF9

Drives:
d: Leia

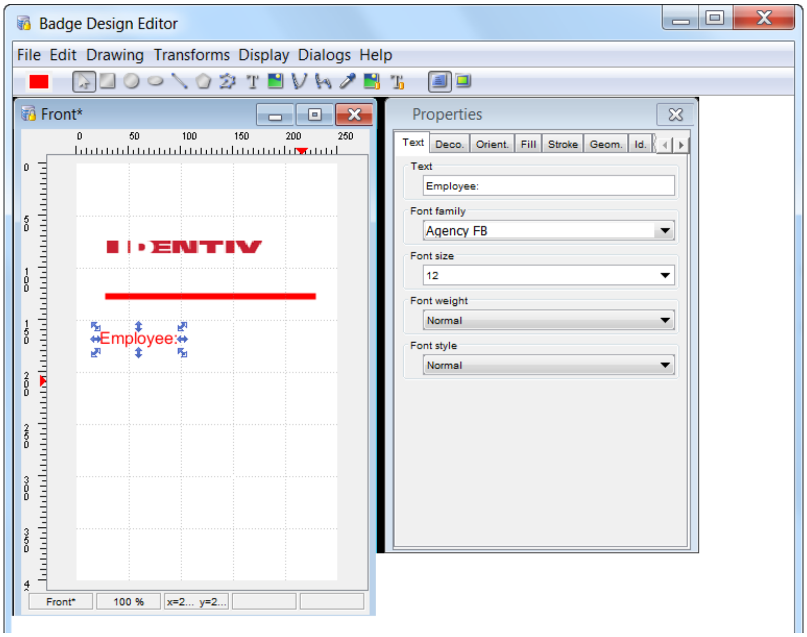
☑ Copy fonts to Fonts folder

Step 5 Select the required fonts and click **OK**.

Step 6 Run ICPAM client and navigate to badge designer.

Step 7 Add a text or a text link.

Figure 9-37 Badge Format - Adding a Text



Badge Design Editor

Properties

Text: Employee:
Font family: Agency FB
Font size: 12
Font weight: Normal
Font style: Normal

File Edit Drawing Transforms Display Dialogs Help
Front*
0 50 100 150 200 250
IDENTIV
Employee:
Text Deco. Orient. Fill Stroke Geom. Id.
Front* 100 % x=2... y=2...

Figure 9-38 Badge Properties - Show Properties

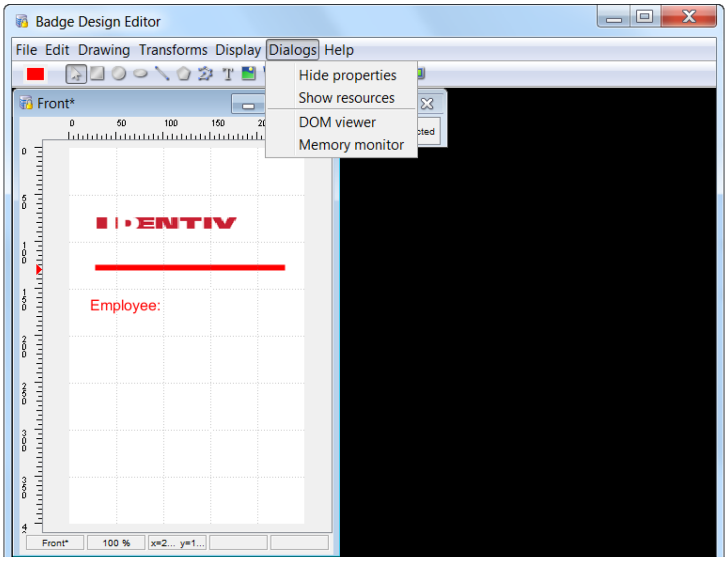
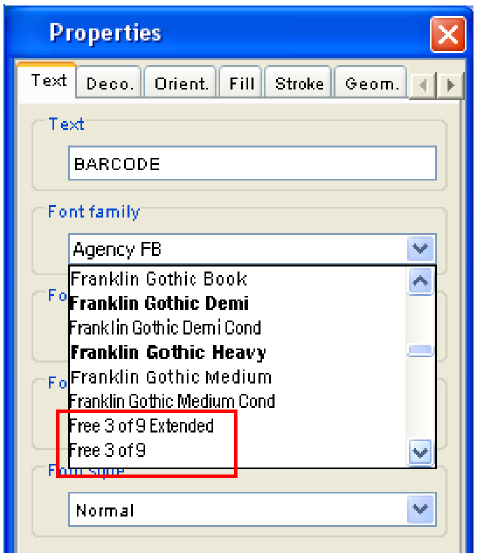


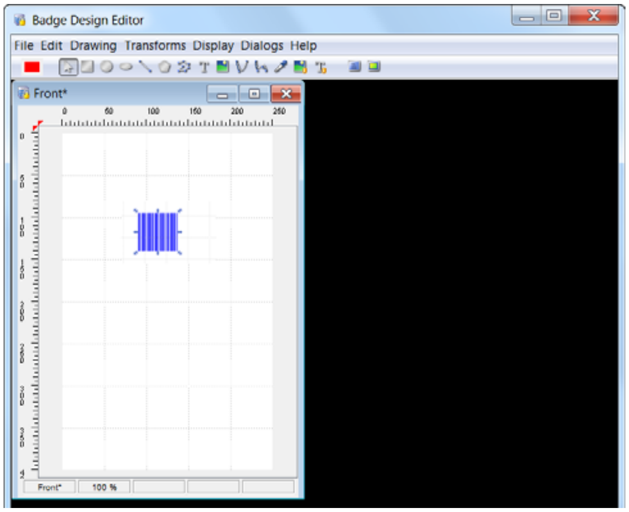
Figure 9-39 Properties Window



Step 8 From the **Properties** window, choose the **Text** tab.

Step 9 From the **Font Family** drop down list, choose the installed **3 of 9 font**.

Figure 9-40 Badge Barcode Example



Printing Badges

To print badges, you must first assign a format to the badge (designs created using the badge designer, as described in Badge Authentication, page 9-32).

After a design is assigned to the badge, you can print badges individually, or in groups.

Note 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 9-44
- Printing Individual Badges, page 9-46
- Printing Multiple Badges, page 9-47
- Printing High Resolution Images, page 9-50
- Changing the Default Badge Printer, page 9-51
- System Configuration Settings for Badge Printing, page 9-52

List of Recommended Badge Printers

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

Note ICPAM 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 ICPAM.

The recommended printers are:

Fargo Printers (www.fargo.com)

- HDP600 Card Printer
- HDP600 CR100 Card Printer
- HD5000 Card Printer
- HD4000 Card Printer
- DTC400 Card Printer
- DTC400e Card Printer
- DTC550 Card Printer
- DTC1000 Card Printer
- DTC4000 Card Printer
- DTC4500 Card Printer
- Persona C30e Card Printer
- Persona C30 Card Printer

Magicard Printers (www.ultramagicard.com)

- Enduro Card Printer
- Rio2e Card Printer
- Rio Pro 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)

- Dualys 3
- Pebble 4
- Securion

Datacard Printers (www.datacard.com)

- SD360

Zebra Printers (www.zebra.com)

- 110i
- 330i
- P430i

Printing Individual Badges

To print a single badge, do the following:

Step 1 (Optional) Create the badge formats (designs), as described in Using the Badge Designer, page 9-33. You can also use one of the designs included with ICPAM.

Step 2 To define a badge format for a single badge, do the following:

a. Select **Badges** from the **User** menu.

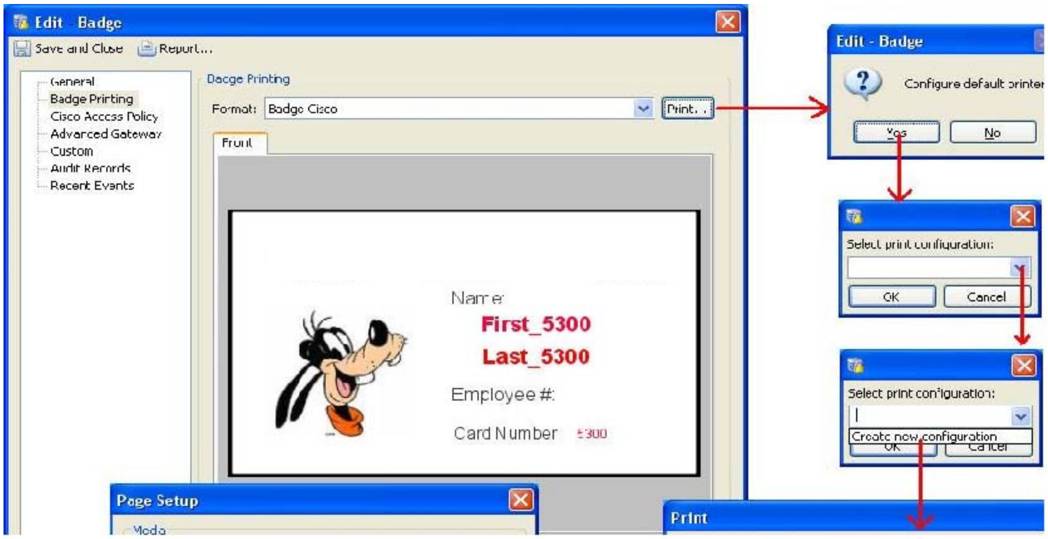
b. Right-click a badge and select **Edit** from the drop-down menu.

c. Click the **Badge Printing** tab and select a **Format**, as shown in Figure 9-41.

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.

Figure 9-41 Printing a Single Badge



Format: Badge Cisco

Configure default printer

Select print configuration:

Create new configuration

Step 3 Configure a default printer, as shown in Figure 9-41.

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 ICPAM 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 (Optional) Create the badge formats (designs), as described in Using the Badge Designer, page 9-33. You can also use one of the designs included with ICPAM.

Step 2 Enable batch badge printing.

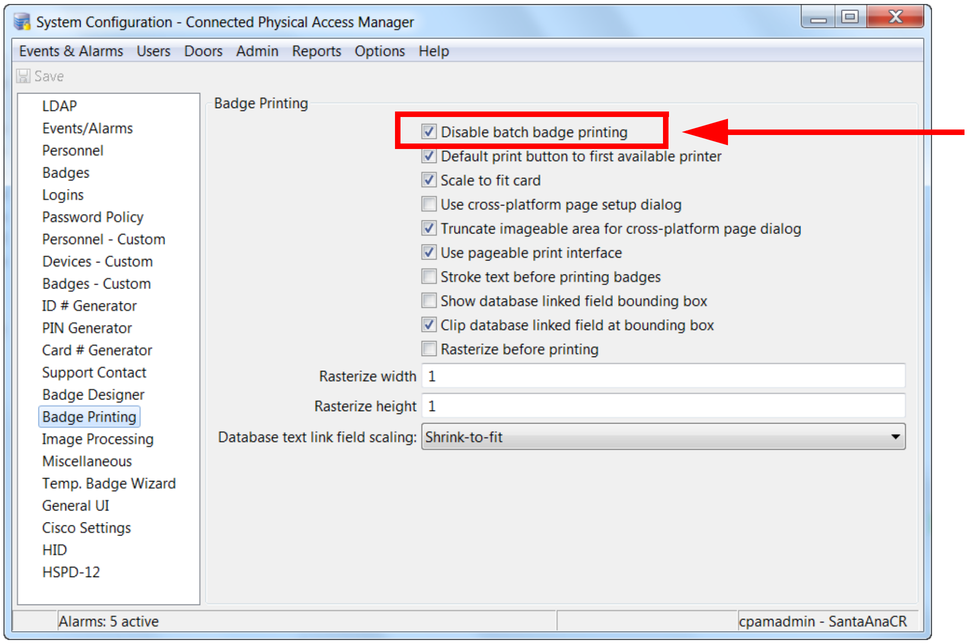
a. Select **System Configuration** from the **Admin** menu.

b. Select **Badge Printing**, as shown in Figure 9-42.

c. Uncheck the **Disable batch badge printing** box.

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

Figure 9-42 Enabling Batch Badge Printing



Badge Printing

☑ Disable batch badge printing
☑ Default print button to first available printer
☑ Scale to fit card
☐ Use cross-platform page setup dialog
☑ Truncate imageable area for cross-platform page dialog
☑ Use pageable print interface
☐ Stroke text before printing badges
☐ Show database linked field bounding box
☑ Clip database linked field at bounding box
☐ Rasterize before printing

Rasterize width: 1
Rasterize height: 1
Database text link field scaling: Shrink-to-fit

Step 3 Define the format for the badges to be printed.

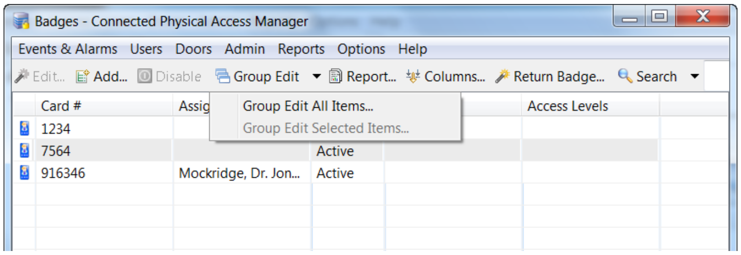
Tip If a format is already assigned for all of the selected badges, skip to Step 4. Check the Format column to view the assigned format, if any (Figure 9-43).

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 9-43).

Figure 9-43 Group Edit Badges

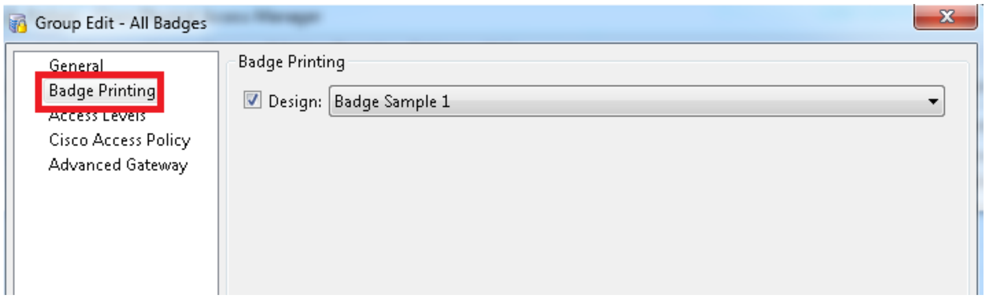

Badges - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Disable Group Edit Report... Columns... Return Badge... Search
Group Edit All Items...
Group Edit Selected Items...

Card #	Assig		Access Levels
1234			
7564		Active	
916346	Mockridge, Dr. Jon...	Active	

d. Click the **Badge Printing** tab, and check the **Design** check box as shown in Figure 9-44.

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

Figure 9-44 Badge Printing Format for Multiple Badges



☑ Design: Badge Sample 1

Step 4 Print the badges.

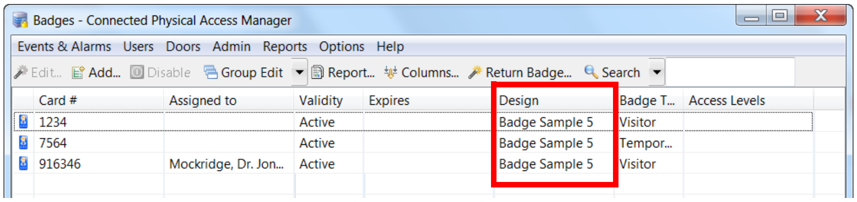
Note If a format is not assigned for any of the selected badges, as described in Step 3, the print job will fail. To view the status of print jobs, select **Batch Badge Printing** from the **User** menu.

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 9-45).

Figure 9-45 Printing Multiple Badges



Card #	Assigned to	Validity	Expires	Design	Badge T...	Access Levels
1234		Active		Badge Sample 5	Visitor	
7564		Active		Badge Sample 5	Tempor...	
916346	Mockridge, Dr. Jon...	Active		Badge Sample 5	Visitor	

Step 5 (Optional) Configure a default printer, as shown in Figure 9-41 on page 9-46. These steps only occur the first time you print a badge.

a. Click **Yes** to configure the default printer. This defines the printer used to print ICPAM badges.

b. In the **Select print configuration** window, select **Create new configuration**.

c. In the **Print** window, select a printer, and click **OK**.

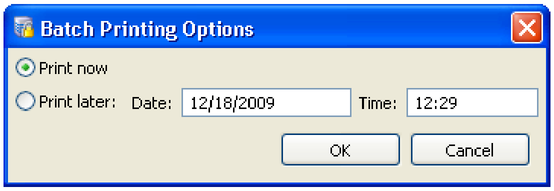
d. In the **Page Setup** window, adjust the settings if necessary, and click **OK**.

e. Enter a name for the printer configuration and click **OK**. For example: `USB Printer`.

Tip To change the default printer, see Changing the Default Badge Printer, page 9-51.

Step 6 Select a **Batch Printing Option**, as shown in Figure 9-46.

Figure 9-46 Batch Printing Options



● Print now

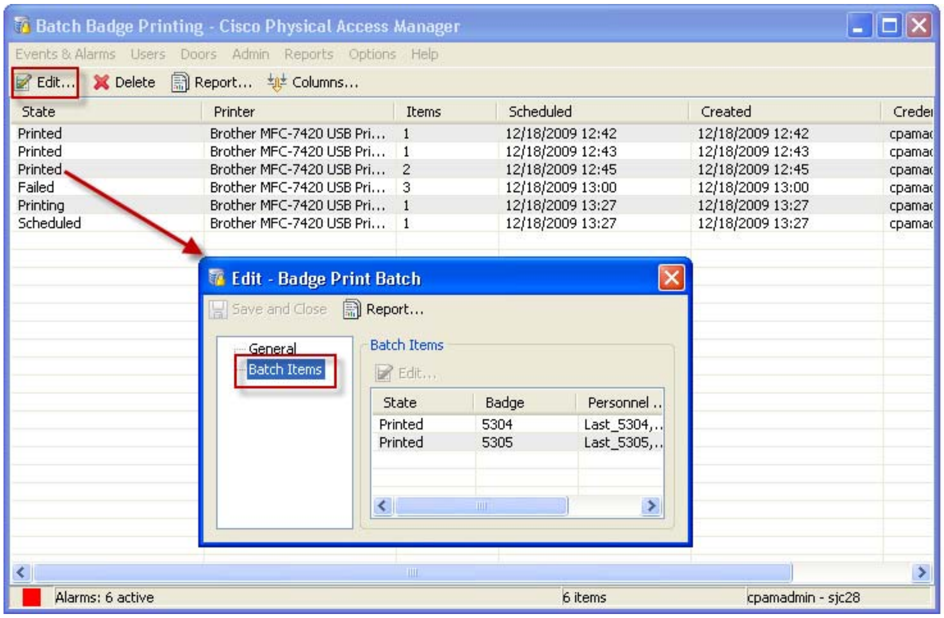
○ Print later: Date: 12/18/2009 Time: 12:29

- 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 7 To view the status of the print job, do the following:

a. Select **Batch Badge Printing** from the **Admin** menu, as shown in Figure 9-47.

Figure 9-47 Batch Badge Printing Status



State	Printer	Items	Scheduled	Created	Crede
Printed	Brother MFC-7420 USB Pri...	1	12/18/2009 12:42	12/18/2009 12:42	cpamad
Printed	Brother MFC-7420 USB Pri...	1	12/18/2009 12:43	12/18/2009 12:43	cpamad
Printed	Brother MFC-7420 USB Pri...	2	12/18/2009 12:45	12/18/2009 12:45	cpamad
Failed	Brother MFC-7420 USB Pri...	3	12/18/2009 13:00	12/18/2009 13:00	cpamad
Printing	Brother MFC-7420 USB Pri...	1	12/18/2009 13:27	12/18/2009 13:27	cpamad
Scheduled	Brother MFC-7420 USB Pri...	1	12/18/2009 13:27	12/18/2009 13:27	cpamad

State	Badge	Personnel ..
Printed	5304	Last_5304,..
Printed	5305	Last_5305,..

Alarms: 6 active 6 items cpamadmin - sjc28

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.

Tip If the **State** of the print job is `Failed`, verify that a **Format** is assigned to every selected badge, as described in Step 3.

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 inch area is 300 x 300 pixels, a 2 x 2 inch area is 600 x 600 pixels, and a 2 x 3 inch area is 600 x 900 pixels.

Mathematically, the ideal resolution can be calculated as (rX, rY) = (w*DPI, h*DPI) where:

- (`rX`, `rY`) is the resolution of the photo
- `rX` is the number of pixels in width
- `rY` is the number of pixels in height
- `w` is the target width of the image on the badge
- `h` is the target height of the image on the badge
- `DPI` is the resolution (dots-per-inch) of the printer

The **Badge Format** 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**.
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 to achieve the best possible print quality.

Changing the Default Badge Printer

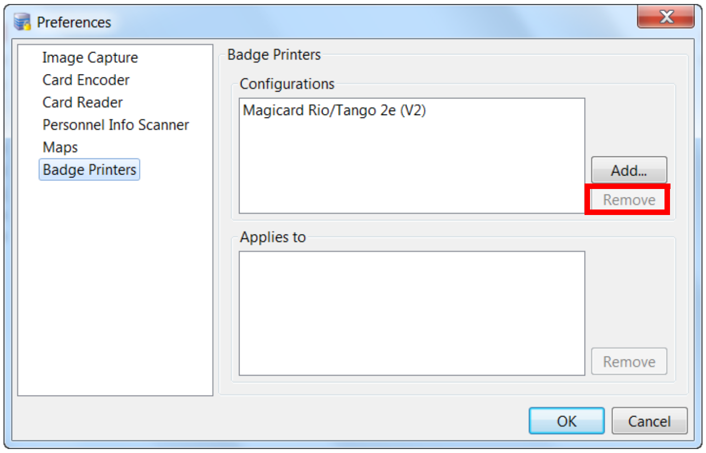
The default printer is configured when you print a badge. Complete the following instructions to remove the default printer and select a new printer.

Step 1 Select **Preferences** from the **Options** menu.

Step 2 Click the **Badge Printers** tab.

Step 3 In the Configurations section, select the printer that displays **Badge: Badge Printing** in the **Applies to** section, as shown in Figure 9-48.

Figure 9-48 Removing the Default Badge Printer



Magicard Rio/Tango 2e (V2)

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:

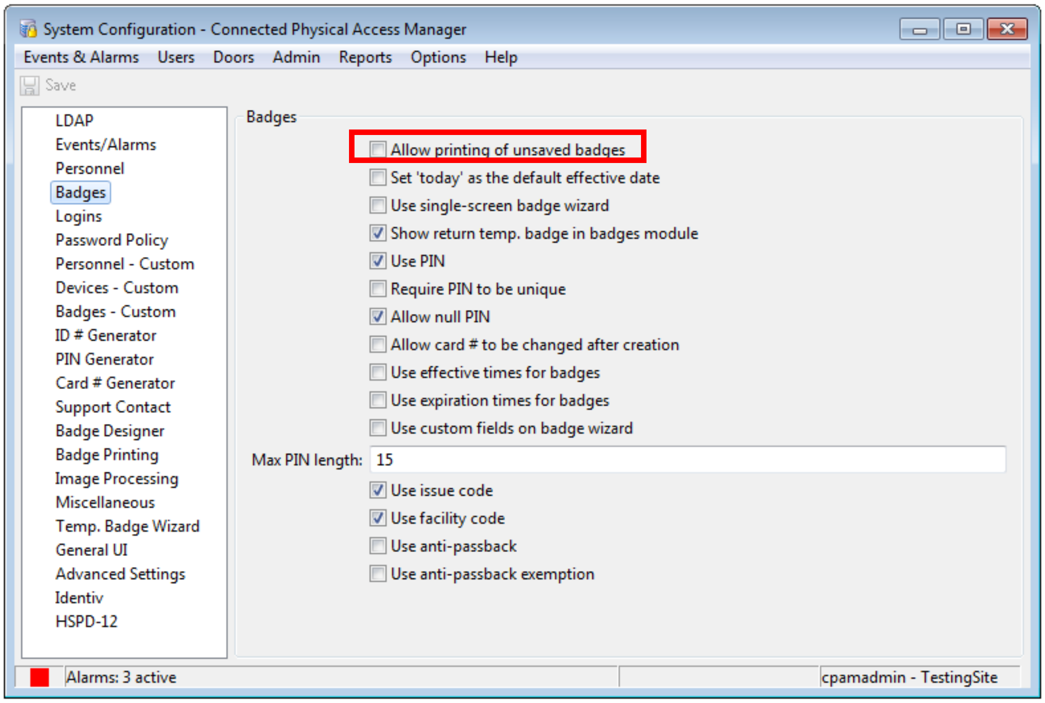
- **Data Entry/Validation - Badge**
- **Miscellaneous**

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 9-49).

Figure 9-49 Badge Printing Options in Badges



Badges

□ Allow printing of unsaved badges
□ Set 'today' as the default effective date
□ Use single-screen badge wizard
☑ Show return temp. badge in badges module
☑ Use PIN
□ Require PIN to be unique
☑ Allow null PIN
□ Allow card # to be changed after creation
□ Use effective times for badges
□ Use expiration times for badges
□ Use custom fields on badge wizard

Max PIN length: 15

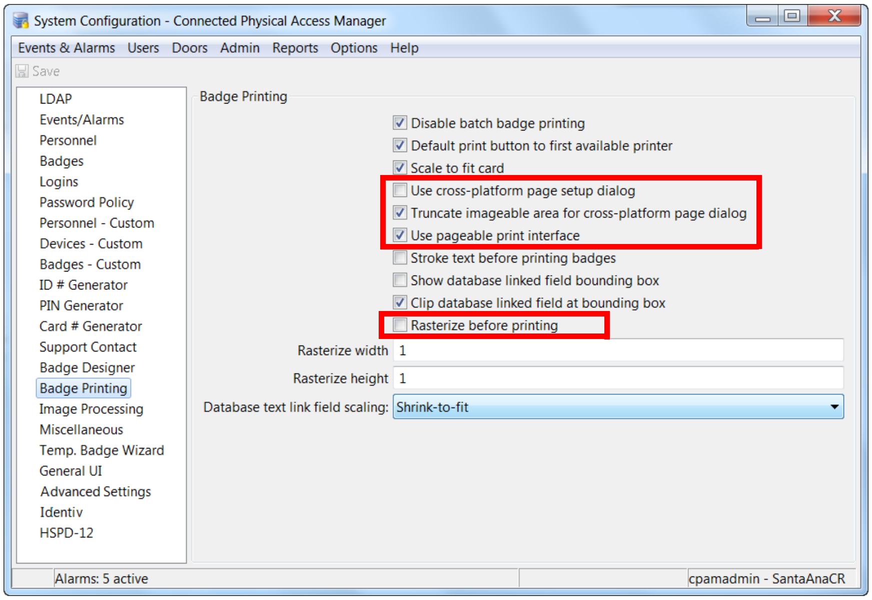
☑ Use issue code
☑ Use facility code
□ Use anti-passback
□ Use anti-passback exemption

Step 3 Select or deselect one or more of the following options.

Field	Description
Allow printing of unsaved badges	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.

Step 4 Select the **Badge Printing** tab (Figure 9-50).

Figure 9-50 Badge Printing Options in Badge Printing Settings



Badge Printing

☑ Disable batch badge printing
☑ Default print button to first available printer
☑ Scale to fit card
□ Use cross-platform page setup dialog
☑ Truncate imageable area for cross-platform page dialog
☑ Use pageable print interface
□ Stroke text before printing badges
□ Show database linked field bounding box
☑ Clip database linked field at bounding box
□ Rasterize before printing

Rasterize width: 1
Rasterize height: 1
Database text link field scaling: Shrink-to-fit

Step 5 Select or deselect one or more of the following options.

Field	Description
Use cross-platform page setup dialog for badge printing	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).
Truncate imageable area values used to initialize cross-platform page dialog	If the image is still truncated using the cross-platform Java page dialog, select this option to apply 0.01 inch margins.
Use pageable print interface for badge printing	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.
Rasterize before printing	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.

Step 6 Click **Save** to save the changes.

Step 7 Log out and log back in to the ICPAM 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

ICPAM supports image capture from the following devices:

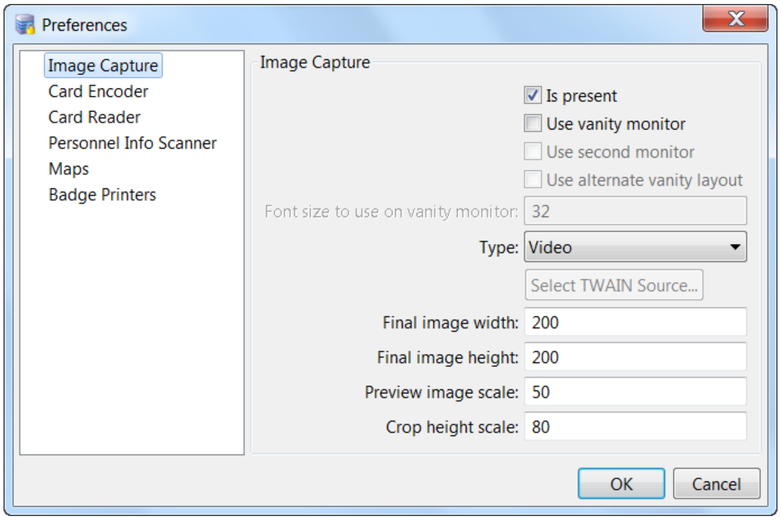
- Badging cameras which have a dedicated TWAIN driver
- Webcams which do not have a TWAIN driver.

Before proceeding to the steps below, install all necessary camera drivers including TWAIN drivers (if available). 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 9-51.

Figure 9-51 Preferences: Image Capture



Preferences

Image Capture
Card Encoder
Card Reader
Personnel Info Scanner
Maps
Badge Printers

Image Capture

☑ Is present
□ Use vanity monitor
□ Use second monitor
□ Use alternate vanity layout

Font size to use on vanity monitor: 32
Type: Video
Select TWAIN Source...
Final image width: 200
Final image height: 200
Preview image scale: 50
Crop height scale: 80

OK Cancel

Step 3 Check the **Is present** check box.

Step 4 Select the image capture device type from the **Type:** drop-down menu. The options are:

- **Video <Use this option in case of a non-TWAIN device like a normal webcam attached to the PC from which the client is run>**
- **TWAIN <Use this option if the camera being used has a dedicated TWAIN driver>**

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 is recommended that the crop height and final image height are equal.

Step 7 Click **OK** to save the settings.

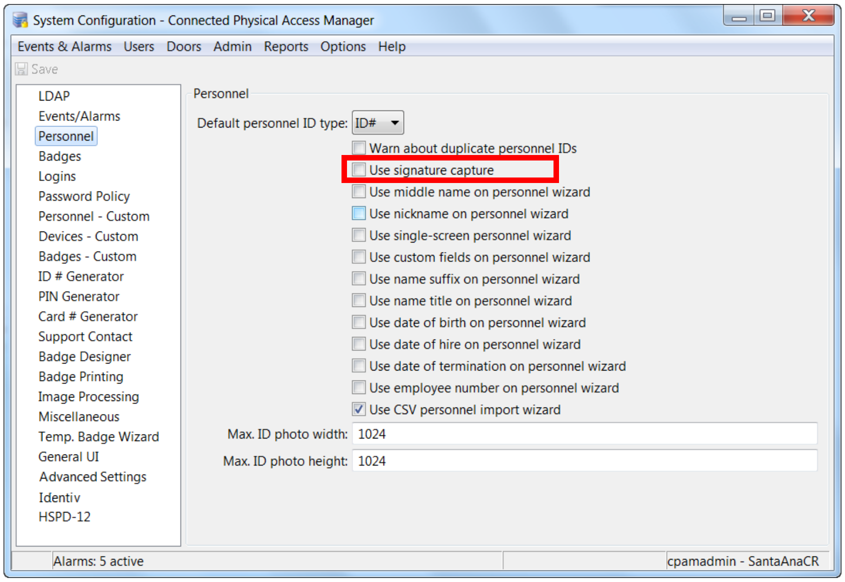
The **Capture** button is activated in the Personnel module. See Configuring Personnel, page 9-1 for more information. Click the **Capture** button and verify that the TWAIN driver is selected and opens properly.

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 9-52.

Figure 9-52 System Configuration: Personnel



Personnel

Default personnel ID type: ID#

□ Warn about duplicate personnel IDs
□ Use signature capture
□ Use middle name on personnel wizard
□ Use nickname on personnel wizard
□ Use single-screen personnel wizard
□ Use custom fields on personnel wizard
□ Use name suffix on personnel wizard
□ Use name title on personnel wizard
□ Use date of birth on personnel wizard
□ Use date of hire on personnel wizard
□ Use date of termination on personnel wizard
□ Use employee number on personnel wizard
☑ Use CSV personnel import wizard

Max. ID photo width: 1024
Max. ID photo height: 1024

Alarms: 5 active
cpamadmin - SantaAnaCR

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 ICPAM application to activate the changes (select Logout from the Options menu).

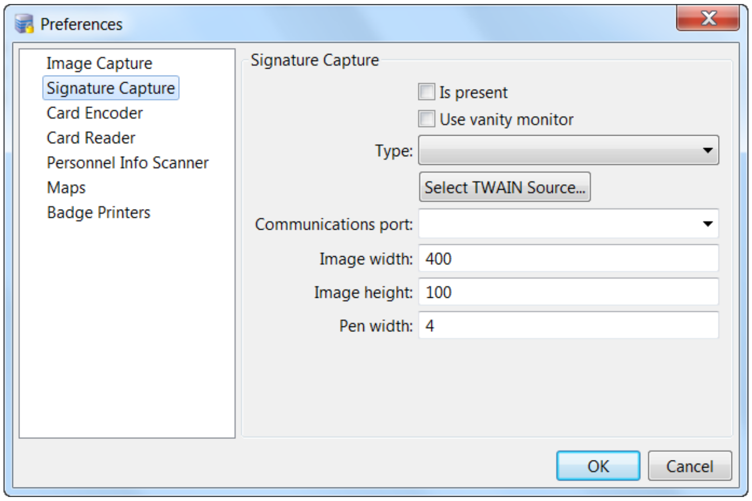
Note You must log out and log back in for the Signature Capture menu to appear in the Preferences window.

Step 6 Log in to the ICPAM 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 9-53.

Figure 9-53 Preferences: Signature Capture



□ Is present

□ Use vanity monitor

Type:

Communications port:

Image width: 400

Image height: 100

Pen width: 4

Step 9 Check the **Is Present** check box and the **Type** of signature pad from the drop-down.

Step 10 Select the communications port from the drop-down.

Step 11 Click **OK** to save the settings. The signature detail in the Personnel module now includes an **Import** and **Capture** button. See Configuring Personnel, page 9-1 for more information.

CHAPTER 10

Multifactor Authentication

The user can integrate additional access control devices like biometric devices to the ICPAM to ensure security. These devices are configured as generic readers in the ICPAM server. The generic readers are associated with doors and finally configured to a specific controller. Once configured, the controller maps the data from the generic reader and matches it with the server. If matched, the events are triggered accordingly.

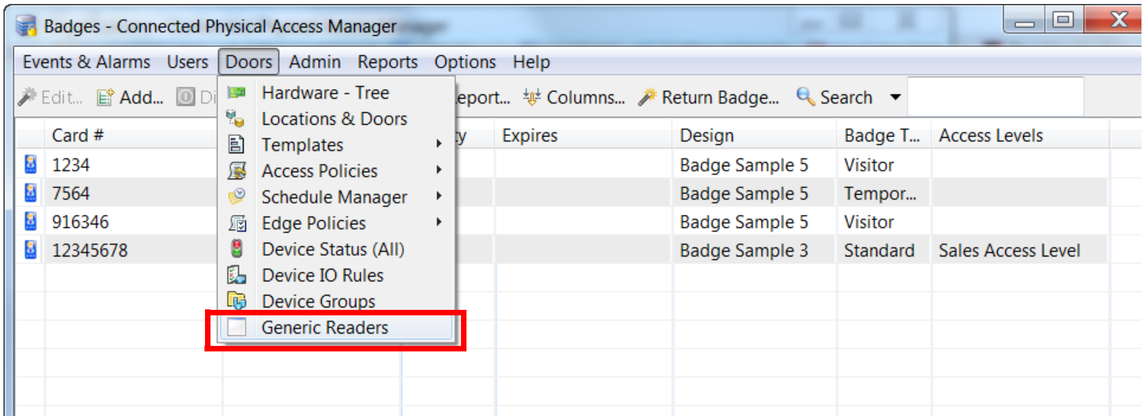
The generic readers are restricted by the location hierarchy when the hierarchical location is set in Logins Settings, page 17-10.

Contents

Configuring Generic Readers

To configure a generic reader, follow this procedure.

Step 1 From the Doors menu, click **Generic Readers**.



Card #	y	Expires	Design	Badge T...	Access Levels
1234			Badge Sample 5	Visitor	
7564			Badge Sample 5	Tempor...	
916346			Badge Sample 5	Visitor	
12345678			Badge Sample 3	Standard	Sales Access Level

Step 2 The Generic Reader window opens. Click **Add**.

Enter the following fields:

- Name (alpha-numeric characters)
- ID (numeric)

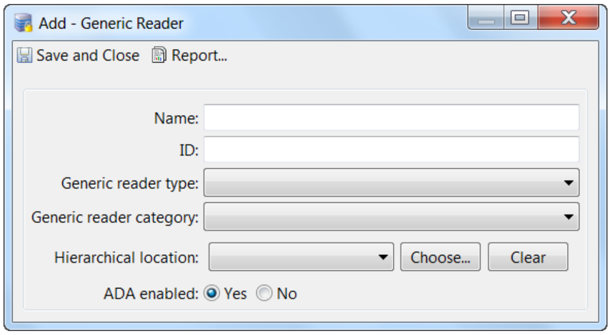
Select values in the following drop down lists:

- Generic reader type

Note This option should be used when using Microsoft Active Directory. Two types of generic readers are configurable. These are face detection (used for facial recognition devices) and biometric (for all other devices like fingerprint readers).

- Generic reader category
- Hierarchical location

Select the ADA enabled radio button.



Name:

ID:

Generic reader type:

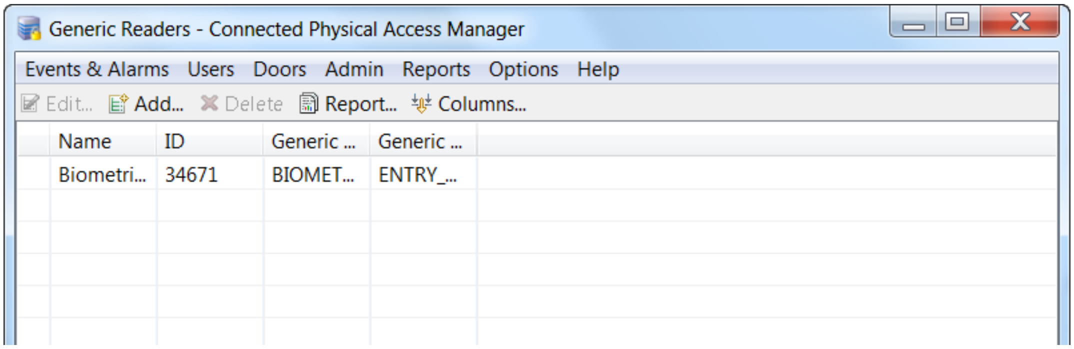
Generic reader category:

Hierarchical location:

ADA enabled: ● Yes ○ No

Tip Ensure that Name and ID are similar.

Step 3 Click **Save and Close**. The Reader information is listed in the Generic Reader window.



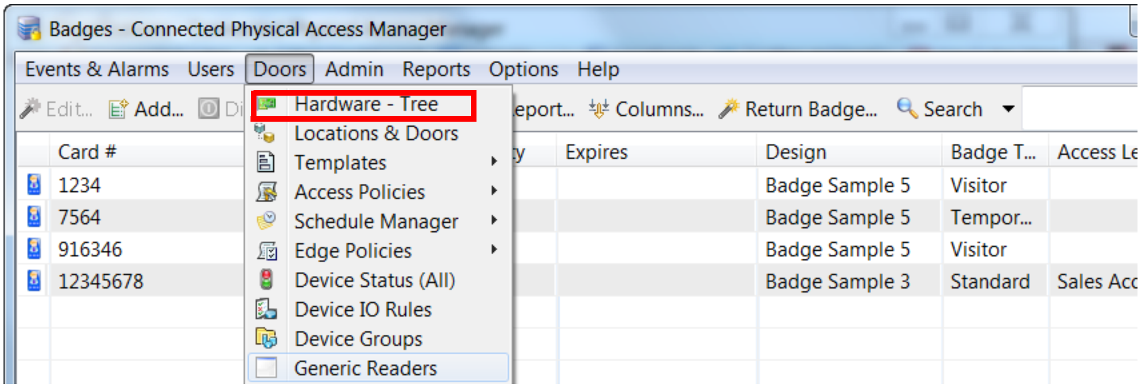
Name	ID	Generic ...	Generic ...
Biometri...	34671	BIOMET...	ENTRY_...

Note Only users with Admin rights are permitted to configure generic readers.

Associating Generic Readers with Doors

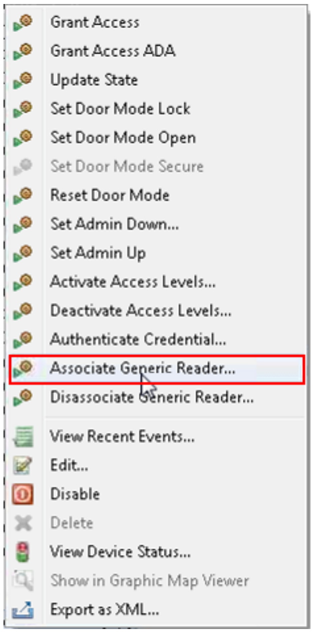
To associate a generic reader with a door, follow this procedure.

Step 1 From the **Doors** menu, select **Hardware - Tree**. The controllers, gateway drivers, and doors are displayed.

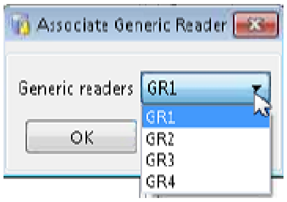


Card #	y	Expires	Design	Badge T...	Access Le
1234			Badge Sample 5	Visitor	
7564			Badge Sample 5	Tempor...	
916346			Badge Sample 5	Visitor	
12345678			Badge Sample 3	Standard	Sales Acc

Step 2 Select the door and right click to view the drop-down menu. Click **Associate Generic Reader**. An Associate Generic reader window opens.

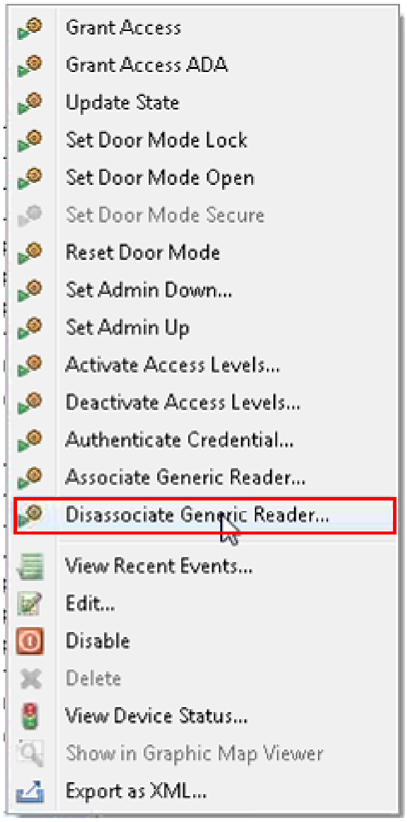


Step 3 Select the generic reader from the list and click **OK**. The generic reader is configured to the door.



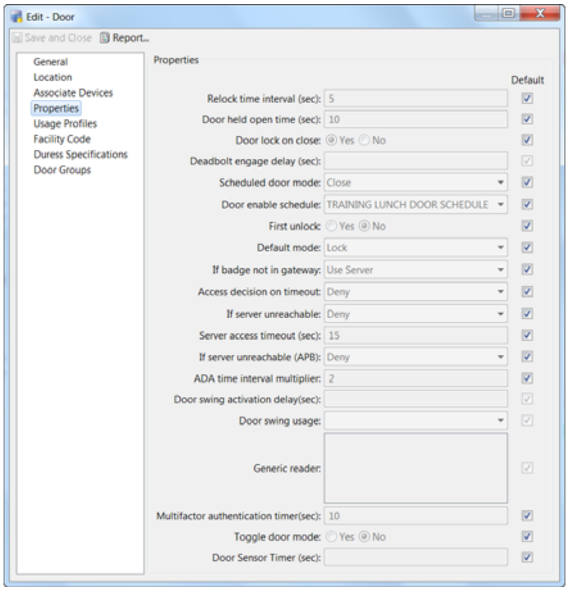
Note You can associate a maximum of six generic readers to a door.

Step 4 Click **Dissociate Generic Reade**r to remove a reader from the door configuration.



Note The drop-down menu displays the list of generic readers assigned to the door.

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 (in seconds). You can edit the timer and set the time.



Properties

		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

Note The default value of Multifactor Authentication timer (sec) is 10 seconds.

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 ICPAM's system configuration; otherwise, the ICPAM 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 ICPAM receives from the generic reader. The ICPAM does not claim support to authenticate the received data. The controller 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 ICPAM.

The external system must send the following HTTPS request for establishing a session with GW

For example:

```
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:

```
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 (supports a maximum 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.

CHAPTER 11

Configuring ICPAM Access Policies

This chapter describes how to create the ICPAM 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.

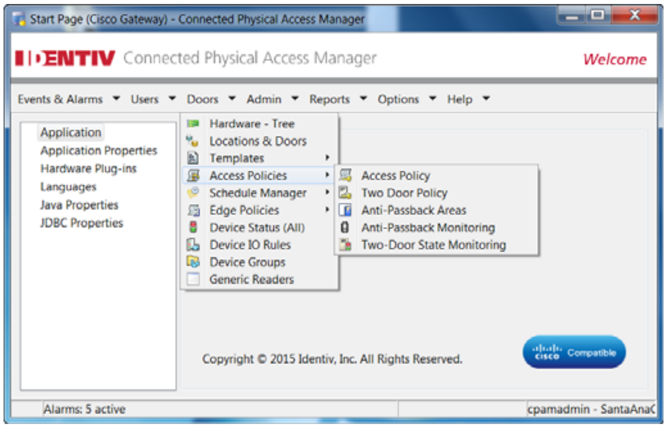
In addition, you can create access policy schedules for doors that define when the doors are available.

Contents

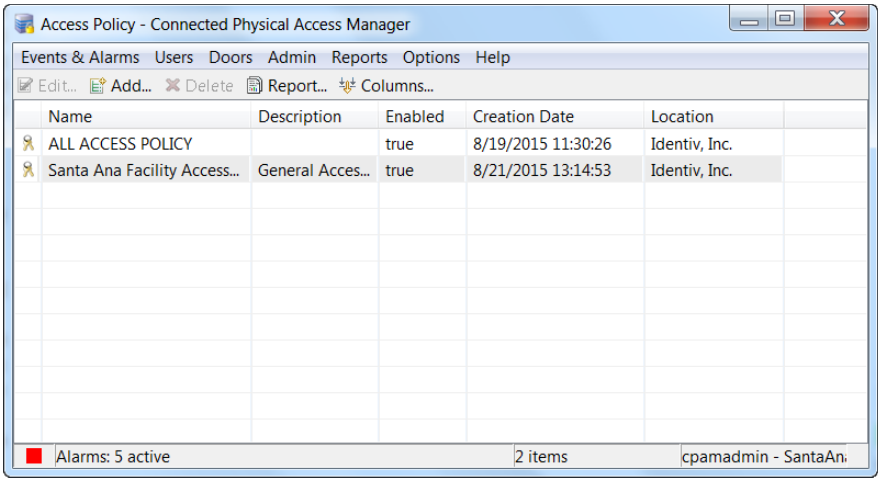
Configuring Access Policies

This section describes how to create an access policy and assign it to a user badge.

Step 1 Select **Access Policy** from the Doors menu, under the **Access Policies** submenu.



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



Name	Description	Enabled	Creation Date	Location
ALL ACCESS POLICY		true	8/19/2015 11:30:26	Identiv, Inc.
Santa Ana Facility Access...	General Acces...	true	8/21/2015 13:14:53	Identiv, Inc.

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.

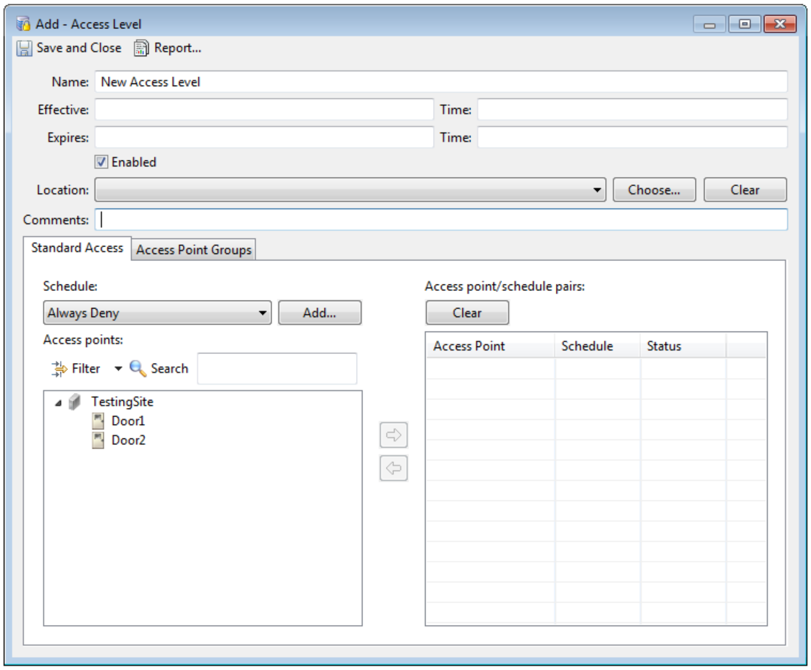
Step 3 Enter the general information for the policy:

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 check box 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.



Add - Access Level

Name: New Access Level

Effective: Time:

Expires: Time:

☑ Enabled

Location:

Comments:

Schedule: Always Deny

Access Point	Schedule	Status

Step 4 Add or remove sets of door and schedule settings for the access policy.

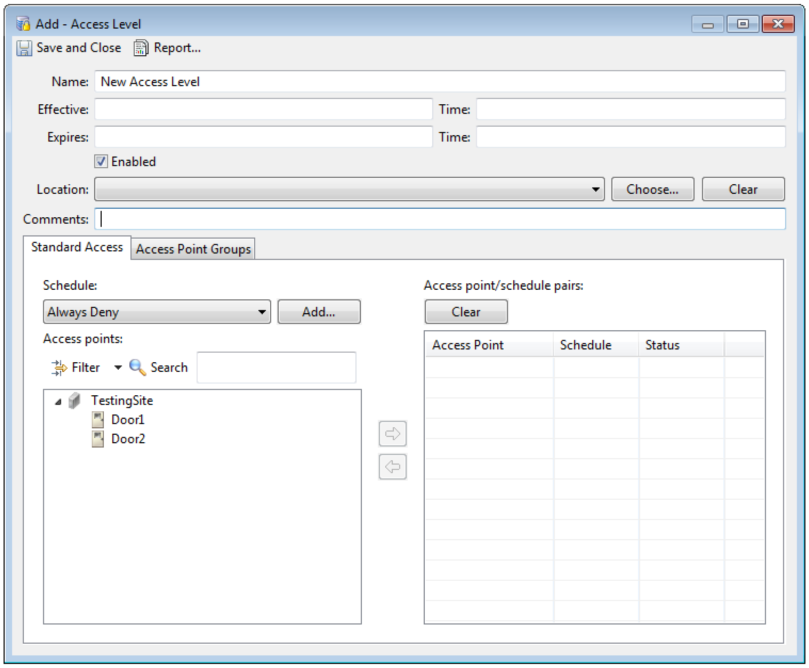
a. Select a door or door group from the list box on the left. You can change the doors listed using the following controls:

- **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 7-22.

b. Select a **Schedule**. To create a new schedule, click the **New Schedule** button. See Using the Schedule Manager, page 11-9 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**.



Name: New Access Level

Effective: Time:

Expires: Time:

☑ Enabled

Location:

Comments:

Schedule: Always Deny

Access points:

- TestingSite
  - Door1
  - Door2

Access point/schedule pairs:

Access Point	Schedule	Status

Step 5 Click **Save and Close** to save the access policy.

Step 6 Assign the access policy to one or more user badges:

a. Open the **Personnel** module from the **Users** menu.

b. Click **Add**, or select an existing personnel entry and click **Edit**.

c. Select the **Badges** submenu.

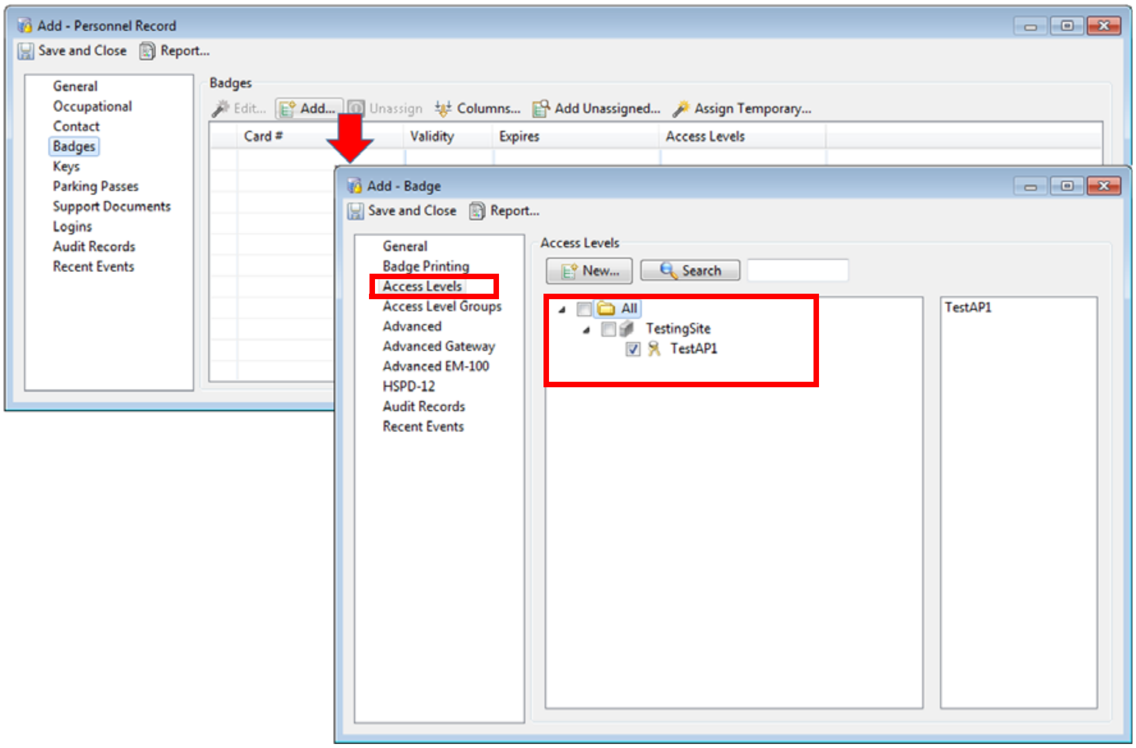
d. Click **Add**, or select an existing badge entry and click **Edit**.

e. Select **Access Policies** (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 ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), 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.

The number of access policies available is dependent on the type of controller.

- Cisco gateway supports up to 50 access policies
- EM-100 controller supports up to 8 access policies

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 ICPAM System Configuration settings; otherwise, the ICPAM appliance retains its behavior as in the previous version(1.3).

Managing Door Access With Access 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 Policies

Command or action	Description
Activate Access Policy	Right-click a door and select the **Activate Access Policy** activate a policy and select **Deactivate Access Policy** to deactivate the access policy.
Reset Gateway	Right-click a gateway icon and select the **Reset Gateway** command to perform a soft reset of the controller. Access policies are activated during a soft reset.
Reload Gateway Configuration	Right-click a Gateway icon and select the **Reload Gateway Configuration** command to replace the existing controller configuration with a new copy. Access policies are activated during this process.
Power cycle the Gateway module	Access policies are activated whenever a controller is powered up. For example, after a power failure or anytime power is disconnected and restored.

Procedure:

Complete the following instructions to deactivate and reactivate door access policies.

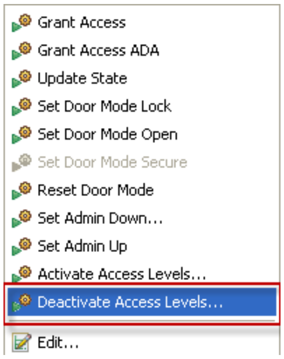
Step 1 View the status of access policies on a door:

a. Select **Hardware - Tree** or **Door/Location-based Hardware** from the **Doors** menu.

b. Click the door to highlight it.

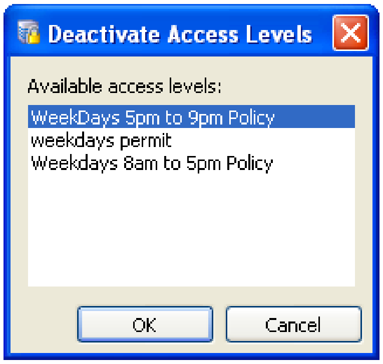
c. In the Extended Status field, click the **Access Policies** tab to view the policies and status for the door.

Step 2 To manually deactivate a policy, right-click the door icon and select **Deactivate Access Policies**.



Tip To deactivate access policies for multiple doors, select the command from a location (Door/Location-based Hardware module) or from the Physical Driver (Hardware - Tree module).

Step 3 Select the access policies to deactivate and click **OK**.



WeekDays 5pm to 9pm Policy
weekdays permit
Weekdays 8am to 5pm Policy

Tip Use Shift-click or Ctrl-click to select multiple items from the list.

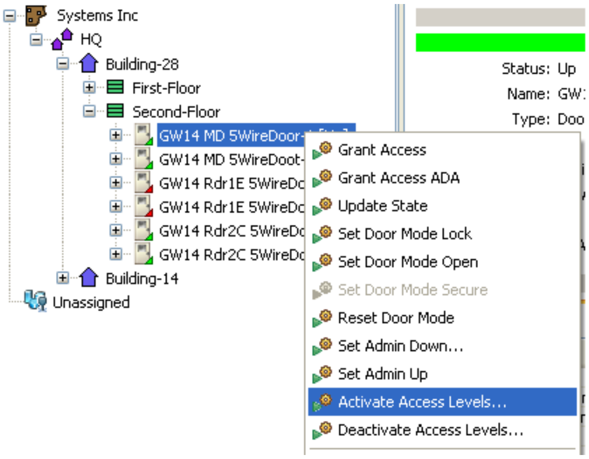
Step 4 Verify that the status of the access policy is **No**:

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 policy, right click the door icon and select **Activate Access Policies**. Select one or more levels from the list and click **OK**.



Note Access policies remain deactivated until manually reactivated using this command. See Table 11-1 on page 11-6 for other methods to reactivate access policies.

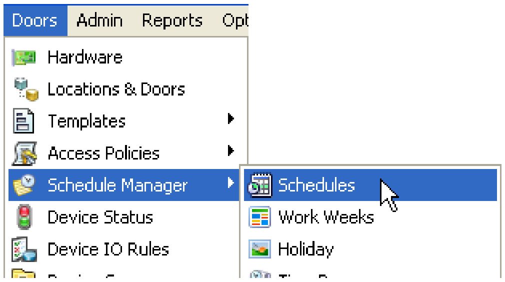
Using the Schedule Manager

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 5-25 and the "Adding New Doors" section on page 7-2 for more information.

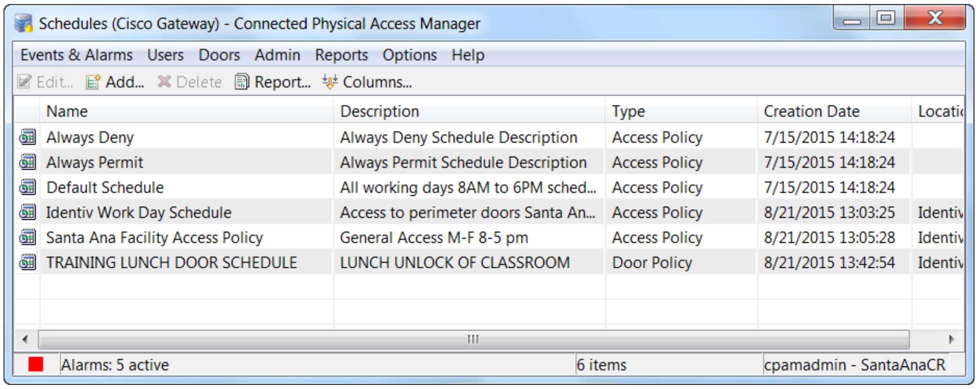
To add or edit schedules, do the following:

Step 1 Select **Schedules** from the **Doors** menu, in the Schedule Manager submenu.



Step 2 Click **Add**, or select an exiting entry and click **Edit**.

To remove a schedule, highlight the entry and click **Delete**.

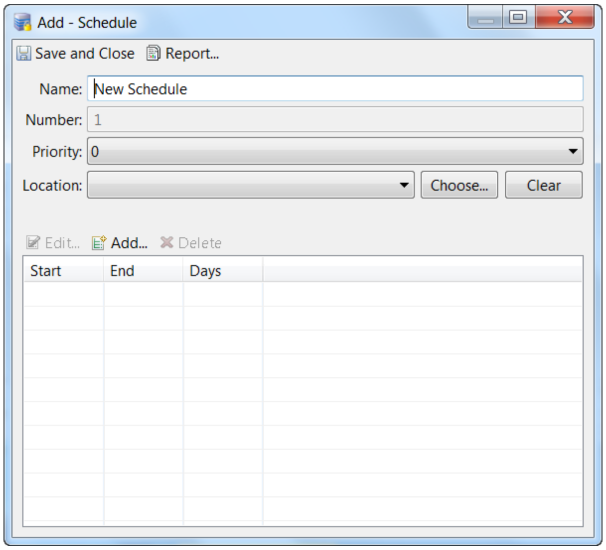


Name	Description	Type	Creation Date	Locati
Always Deny	Always Deny Schedule Description	Access Policy	7/15/2015 14:18:24	
Always Permit	Always Permit Schedule Description	Access Policy	7/15/2015 14:18:24	
Default Schedule	All working days 8AM to 6PM sched...	Access Policy	7/15/2015 14:18:24	
Identiv Work Day Schedule	Access to perimeter doors Santa An...	Access Policy	8/21/2015 13:03:25	Identiv
Santa Ana Facility Access Policy	General Access M-F 8-5 pm	Access Policy	8/21/2015 13:05:28	Identiv
TRAINING LUNCH DOOR SCHEDULE	LUNCH UNLOCK OF CLASSROOM	Door Policy	8/21/2015 13:42:54	Identiv

🟥 Alarms: 5 active 6 items cpamadmin - SantaAnaCR

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.

Step 3 Enter the Name, Hierarchical location and description for the schedule.



Add - Schedule

Save and Close | Report...

Name: New Schedule

Number: 1

Priority: 0

Location:

Step 4 Select a **Schedule Type**:

- **Door Policy**: door schedules appear in the door properties window under the menu: **Door enable schedule**. See Step 4. on page 8-5 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.

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.

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**:

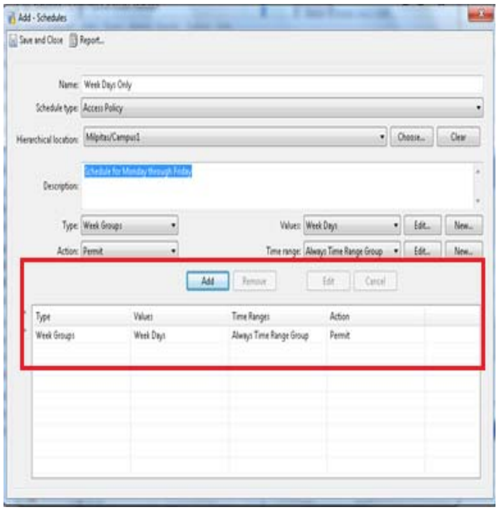
- Access Policy schedules: select **Deny** or **Permit** to define if the user should t have access during the defined schedule.
- Door schedules: select **Use Schedule Mode**.

Note The option **Default Mode** enables the default door mode defined in the door Properties window. See 4. on page 8-5 in Configuring Door Templates for more information.

Step 7 Select a **Time Range** for the schedule.

To create or modify the available values, see Ranges, page 11-15.

Step 8 Click **Add** to add the entry to the list of defined schedules.



Name: Week Days Only

Schedule type: Access Policy

Hierarchical location: Milpitas/Campus1

Description: Schedule for Monday through Friday

Type: Week Groups

Values: Week Days

Action: Permit

Time range: Always Time Range Group

Type	Values	Time Ranges	Action
Week Groups	Week Days	Always Time Range Group	Permit

a. Repeat Step 5 to a. to add additional schedules, if necessary.

b. Click **Save and Close**.

Step 9 To apply schedules to an access policy, see Configuring Access Policies, page 11-2.

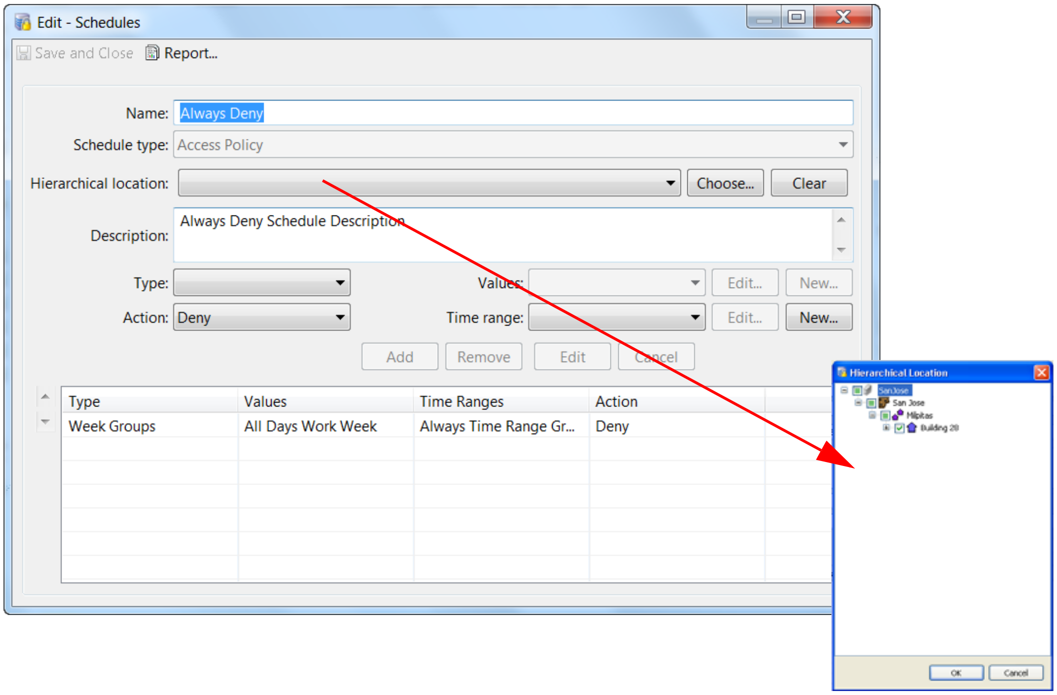
To apply a schedule to a door configuration, see Configuring Door Templates, page 8-2 and Adding New Doors, page 7-2. Door schedules are selected in the Properties window under the **Use Schedule Mode** menu.

Schedule Manager in ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), 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



Name: Always Deny

Schedule type: Access Policy

Hierarchical location:

Description: Always Deny Schedule Description

Type:

Values:

Action: Deny

Time range:

Type	Values	Time Ranges	Action
Week Groups	All Days Work Week	Always Time Range Gr...	Deny

☐ SanJose
☐ San Jose
☐ Milpitas
☑ Building 20

- 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.

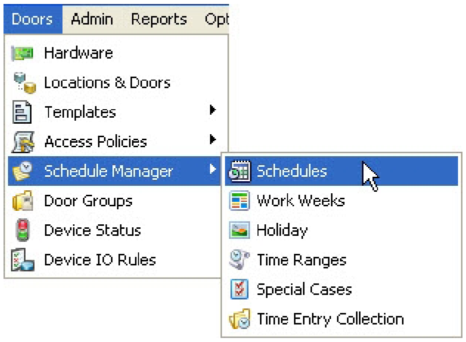
Tip If the cpamadmin assigns a door policy from an unprivileged location to the logged in location-restricted user, the policy continues to work but it is not auto-populated to the logged in location-restricted user. This observation is seen across all modules. Hence it is recommended to use legitimate policies for seamless working of the profile enhancement feature.

Note The above points are applicable only when the Profile enhancement feature is set in the System Configuration of the ICPAM. Otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

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 submenu (Figure 11-2).

Figure 11-2 Schedule Manager Submenu



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 11-9 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 11-13
- Modifying Holidays, page 11-14
- Ranges, page 11-15
- Modifying Special Cases, page 11-16
- Entry Collections, page 11-17

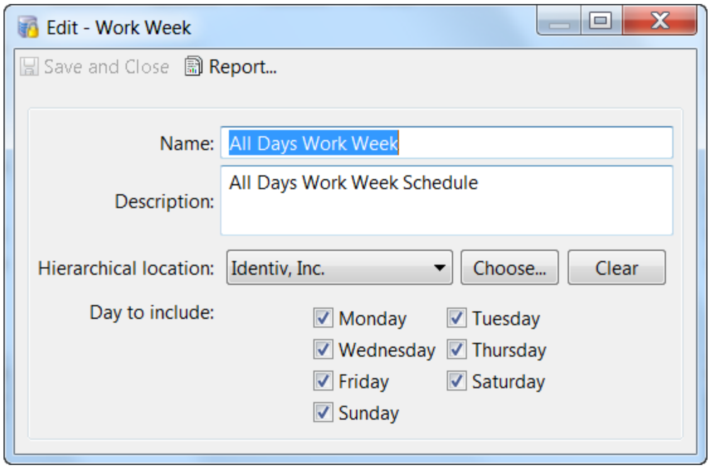
Modifying Work Weeks

Work weeks define the days of the week for a schedule.

To edit one or more work weeks:

Step 1 Select **Work Weeks** from the Doors menu, under the Schedule Manager submenu.

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



Name: All Days Work Week

Description: All Days Work Week Schedule

Hierarchical location: Identiv, Inc.

Day to include:

☑ Monday ☑ Tuesday
☑ Wednesday ☑ Thursday
☑ Friday ☑ Saturday
☑ Sunday

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 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 (Logins Settings, page 17-10).

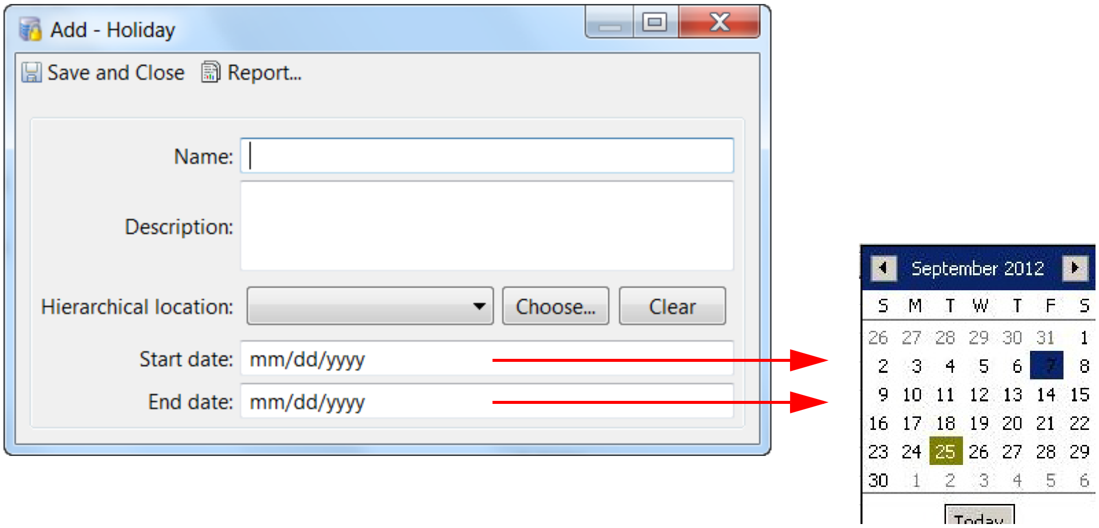
Modifying Holidays

Holiday defines a single date, or a range of consecutive dates.

To modify one or more holiday dates:

Step 1 Select **Holiday** from the Doors menu, under the Schedule Manager submenu.

Step 2 Click **Add**, or select an existing entry and click **Edit**. A screen like this example appears.



Name:

Description:

Hierarchical location:

Start date: mm/dd/yyyy

End date: mm/dd/yyyy

S	M	T	W	T	F	S
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

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 Holidays can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. For more information, see Logins Settings, page 17-10.

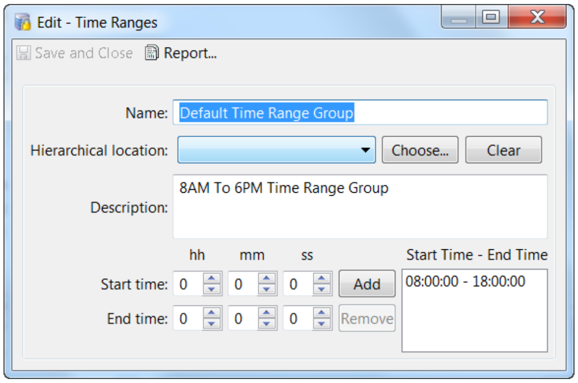
Ranges

Time Ranges specify the time span for a schedule type.

To define a time range:

Step 1 Select **Time Range** from the Doors menu, under the Schedule Manager submenu.

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



Name: Default Time Range Group

Hierarchical location:

Description: 8AM To 6PM Time Range Group

Start time: 0 0 0

End time: 0 0 0

Start Time - End Time: 08:00:00 - 18:00:00

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.

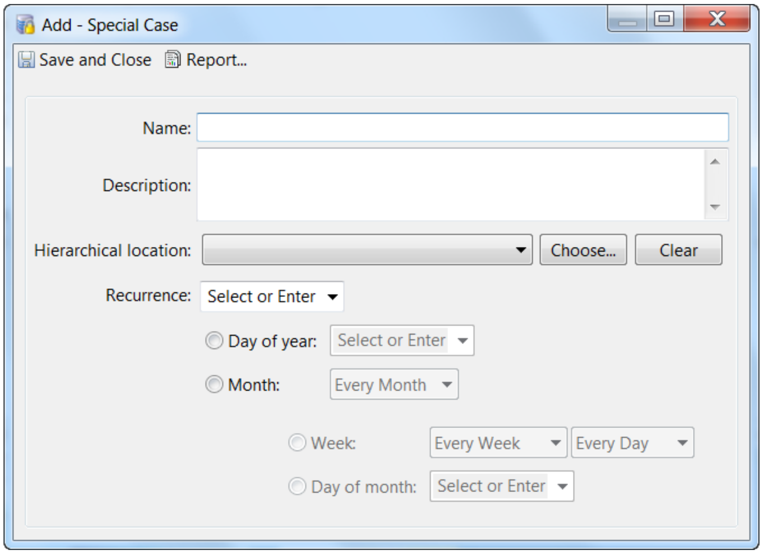
Step 8 To remove a range, highlight the entry and select **Remove**.

Step 9 Click **Save and Close** when you are done.

Note Time Ranges can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. For more information, see Logins Settings, page 17-10.

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** submenu.

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 option for either **Week** or **Day of month**.

Step 9 Click **Save and Close** when you are done.

Note Special Cases can be added by users only for locations or sublocations assigned to their user profile. This is based on system configuration settings. For more information, see Logins Settings, page 17-10.

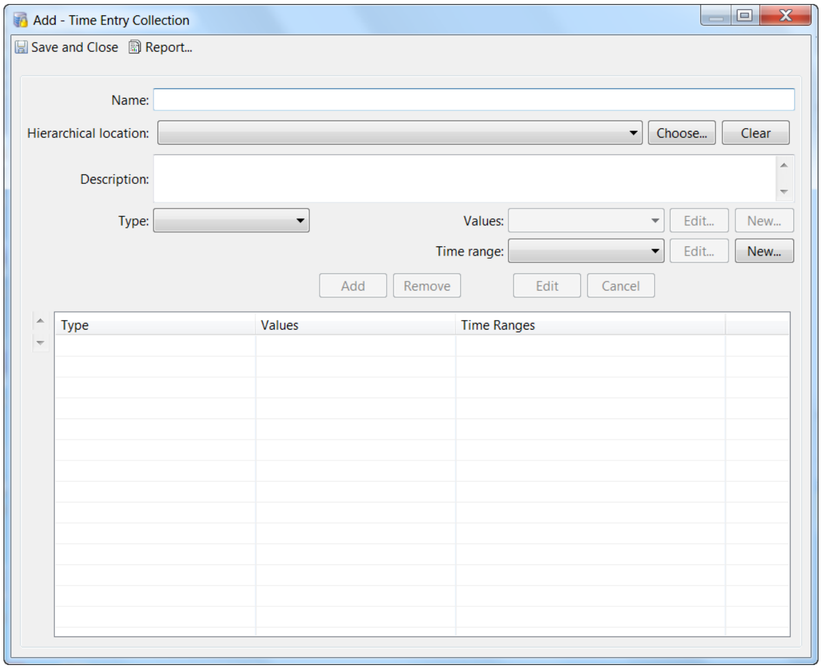
Entry Collections

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.

Figure 11-3 Add-Time Entry Collection



Step 1 Select **Time Entry Collection** from the Doors menu, under the Schedule Manager submenu.

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.

Step 11 Repeat these steps to add additional entries to the collection.

Step 12 Click **Save and Close** when you are done.

Note Time Entry collections can be added by user's only for locations or sublocations assigned to their user profile. This is based on system configuration settings. For more information, see Logins Settings, page 17-10.

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:

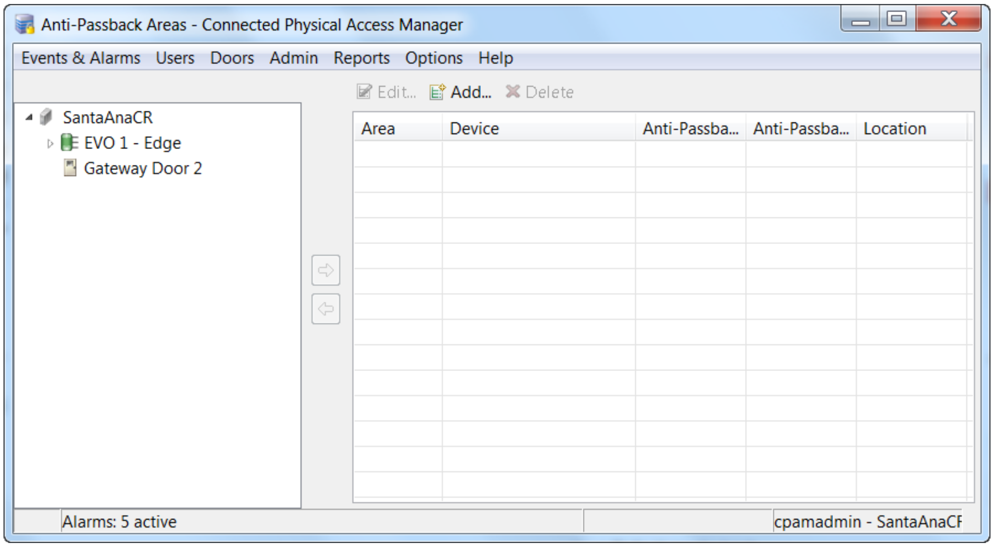
- Anti-Passback Areas in ICPAM 2.1, page 11-19
- Configuring Anti-Passback Areas, page 11-20
- Using Local (Controller) Credentials if Network Communication is Lost, page 11-22
- Evicting a Badge from APB if the User Does Not Enter the APB Area, page 11-24
- Monitoring Anti-Passback Events, page 11-26
- Anti-Passback Events Displayed in the Events Module, page 11-26

Anti-Passback Areas in ICPAM 2.1

In ICPAM 2.1, if the profile enhancement feature is set in the system configuration settings (see Logins Settings, page 17-10), the following changes are impacted in this module:

- The user can create anti-passback 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 are displayed (see Figure 11-6 on page 11-22). If the user wants to view all doors, then the system configuration settings should be set accordingly as shown in Figure 11-4 on page 11-20.

Figure 11-4 Anti-passback areas based on hierarchical locations



- The hierarchical location is auto-populated for a profile when a new APB policy is created.
- When a location restricted user selects the doors for the APB policy, only doors within the user's location are listed for selection.
- The cpamadmin must assign appropriate locations for the APB area and its corresponding doors with that of the logged in user for the existing APB areas to avoid any behavior discrepancy.
- The APB monitoring window displays all badges but the location-restricted user can reset badges related only to the user's location.

Tip While configuring an APB policy it is required to have all the entities that is the policy location and the door in the policy to the location of the logged in user.

Note These points are applicable only when the profile enhancement feature is set in the System Configuration dialog boxes of the ICPAM; otherwise, the ICPAM appliance retains its behavior as in the previous version (1.5.1).

Configuring Anti-Passback Areas

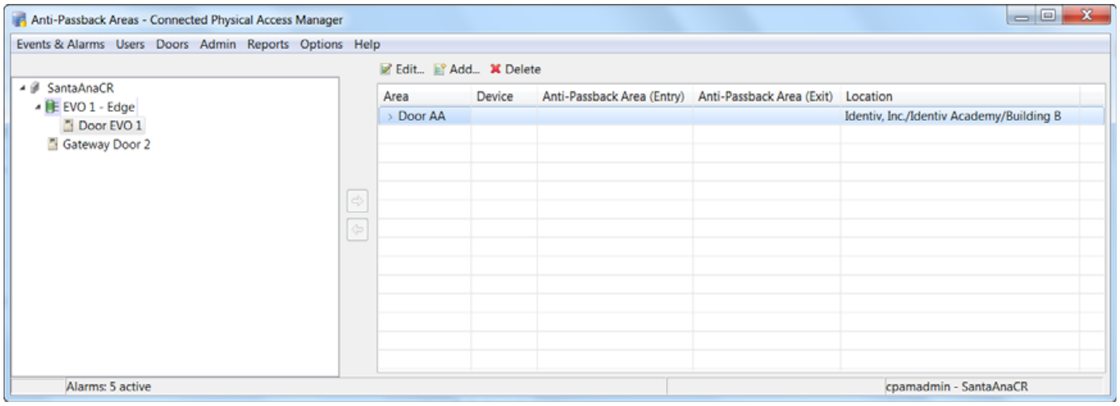
Procedure

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 submenu. The main window lists the currently defined areas, as shown in Figure 11-5.

- To modify an existing area, select the area name and choose **Edit...** to open the detail window.
- To add a new area, click **Add...** to open the detail window.
- To remove an area, highlight the area name and click **Delete**.

Figure 11-5 *Anti-Passback Area Main Window*



Area	Device	Anti-Passback Area (Entry)	Anti-Passback Area (Exit)	Location
Door AA				Identiv, Inc./Identiv Academy/Building B

Alarms: 5 active

cpamadmin - SantaAnaCR

Step 2 Complete the following fields in the detail window (see Figure 11-6).

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.

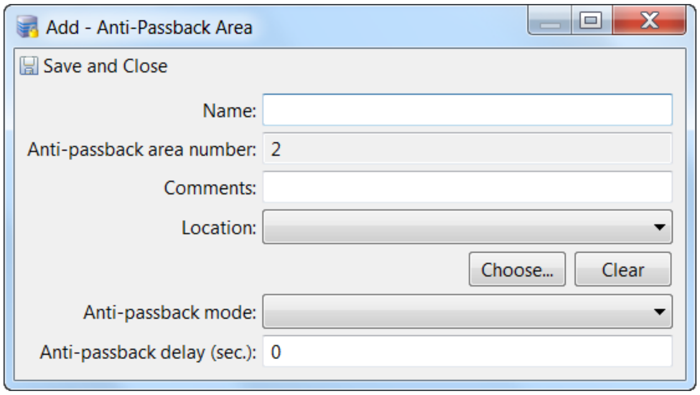
e. **Site**: Read-only.

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 ICPAM 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.

Figure 11-6 *Anti-Passback Areas Add Window*



Name:

Anti-passback area number: 2

Comments:

Location:

Anti-passback mode:

Anti-passback delay (sec.): 0

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 11-5):

a. Choose a door from the left column.

b. Choose Entry or Exit for an anti-passback area in the fight column.

c. Click the arrows to add or remove the door for an entry or exit point.

Using Local (Controller) Credentials if Network Communication is Lost

If network communication is lost between the access control controllers and the ICPAM 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 controller).

Usage Notes

- Allowing local controller authentication as described in this section means that the badge can be used multiple times (potentially by different users) at the entry controller. Use the local authentication option only if necessary. APB areas are only fully effective when stable network communication exists between the controllers and the ICPAM appliance.
- We recommend using the *Soft (grant access)* anti-passback mode when local controller 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 controller authenticates a badge locally.
  - Once network communication is reestablished between the controller and the ICPAM appliance, any controller 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 controller 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 ICPAM appliance when the network communication is reestablished. When the user swipes their badge at the exit door, the ICPAM appliance evicts the badge from the APB area.
- If the entry and exit doors are configured to use two different controllers, 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 controller, and network communication is restored between ICPAM and the (second) exit door controller while the user is still in the APB area (before they access the exit door controller). This occurs because there is no record on the ICPAM appliance that the user entered the APB area (the record only exists on the entry controller). To prevent this scenario, we recommend the following:
  - Configure all APB area doors on a single controller. To support more than two doors on a single controller, a Reader module is required.
  - Install working phones that can reach the ICPAM administrator within the APB area. A badge can be modified to allow one free APB pass for the trapped user.

Procedure

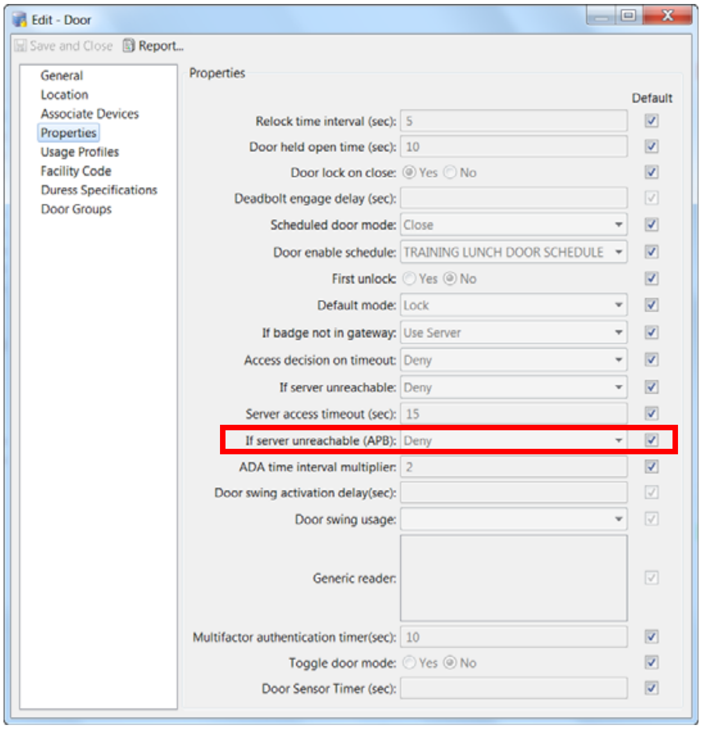
To configure local authentication of user credentials (using data stored on the local controller and not the ICPAM appliance), do the following:

Step 1 Use either the **Hardware - Tree** or **Locations & Door** module to edit the door or door template configuration.

- For example, choose **Hardware - Tree** 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 7-10.
- To change the setting for a door template, see the "Configuring Door Templates" section on page 8-2 and the "Door Configuration Properties" section on page 8-24.

Step 2 Select the **Properties** tab (Figure 11-7).

Figure 11-7 Authenticating Credentials Locally (at the Controller)



Edit - Door

Save and Close | Report...

General
Location
Associate Devices
Properties
Usage Profiles
Facility Code
Duress Specifications
Door Groups

Properties

		Default
Relock time interval (sec):	5	☑
Door held open time (sec):	10	☑
Door lock on close:	● Yes ○ No	☑
Deadbolt engage delay (sec):		☑
Scheduled door mode:	Close	☑
Door enable schedule:	TRAINING LUNCH DOOR SCHEDULE	☑
First unlock:	○ Yes ● No	☑
Default mode:	Lock	☑
If badge not in gateway:	Use Server	☑
Access decision on timeout:	Deny	☑
If server unreachable:	Deny	☑
Server access timeout (sec):	15	☑
If server unreachable (APB):	Deny	☑
ADA time interval multiplier:	2	☑
Door swing activation delay(sec):		☑
Door swing usage:		☑
Generic reader:		☑
Multifactor authentication timer(sec):	10	☑
Toggle door mode:	○ Yes ● No	☑
Door Sensor Timer (sec):		☑

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" section on page 7-12.

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 APB area, but decides not to enter the door, then a *Door Not Used* event is generated by the door's controller. 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 controller credentials are used. See the "Configuring Anti-Passback Areas" section on page 11-20.

Procedure

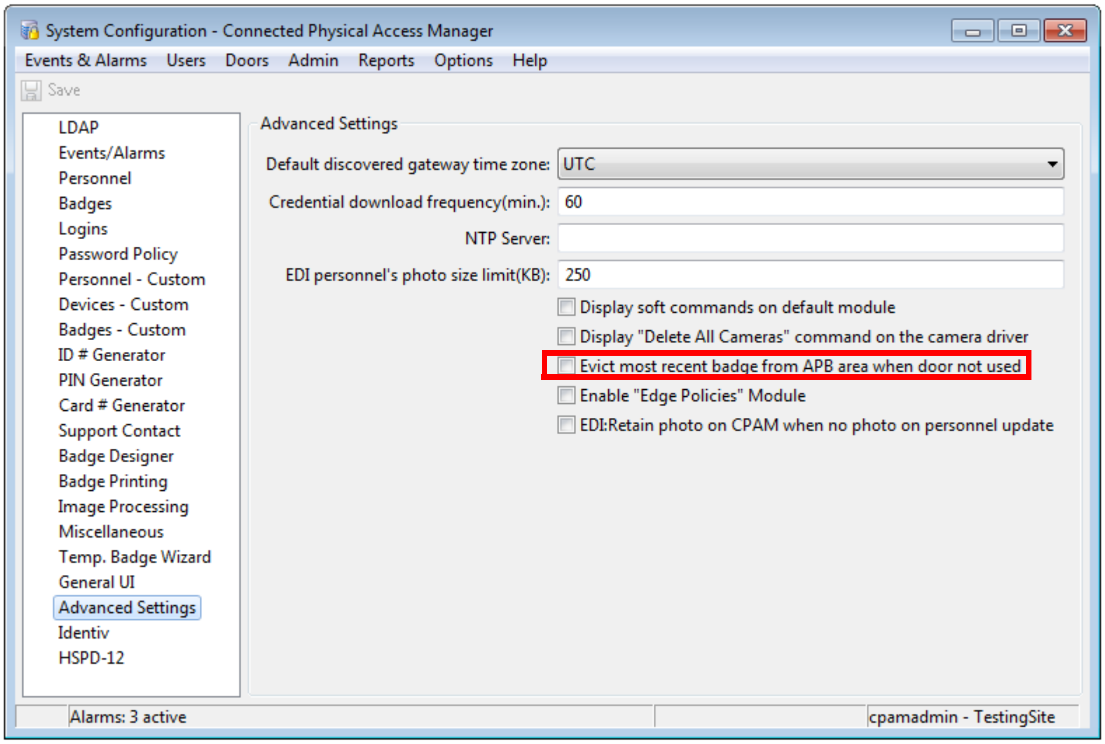
To evict badges from an APB area when a *Door Not Used* event is generated by the door's controller, do the following:

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

Step 2 Click the **Advanced Settings** tab (Figure 11-8).

Step 3 Select the check box for **Evict most recent badge from APB area when door not used**.

Figure 11-8 Advanced Settings



Advanced Settings

Default discovered gateway time zone: UTC

Credential download frequency(min.): 60

NTP Server:

EDI personnel's photo size limit(KB): 250

□ Display soft commands on default module

□ Display "Delete All Cameras" command on the camera driver

□ Evict most recent badge from APB area when door not used

□ Enable "Edge Policies" Module

□ EDI:Retain photo on CPAM when no photo on personnel update

Step 4 Restart the ICPAM appliance to activate the change. See the Using the Web Admin Menus, Commands and Options, page 2-18 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 11-9. 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 submenu. Figure 11-9 shows the main window.
- To reset the state of a badge, select an entry and click the **Reset** button.

Figure 11-9 Anti-Passback Monitoring Window

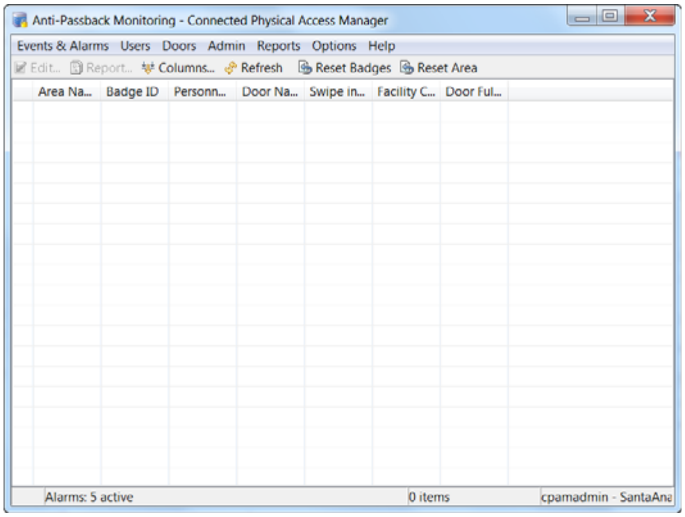


Table 11-2 Anti-Passback Monitoring Properties

Field	Description
Area Name	The anti-passback area accessed by the badge. See Creating Anti-Passback Areas, page 11-19 for more information.
Badge ID	The ID number of the badge.
Door Name	The name of the door accessed.
Policy Name	The name of the Anti-Passback area. See Creating Anti-Passback Areas, page 11-19for more information.
Swipe In Time	The day and time when the entry door was accessed.
Facility Code	The facility code.

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”.

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 ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (see Logins Settings, page 17-10), 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 ICPAM’s system configuration; otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

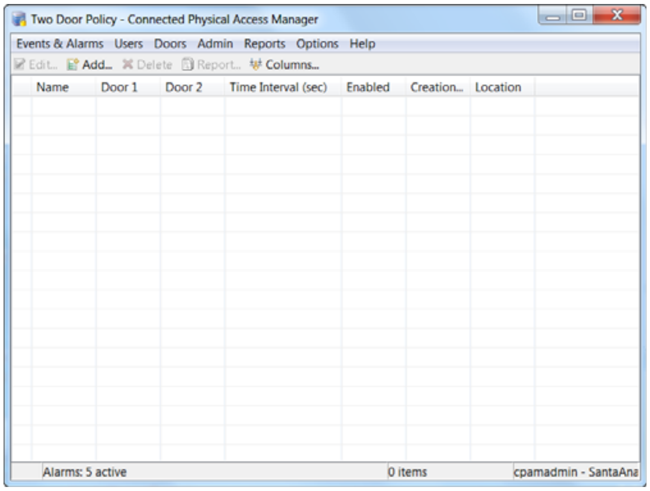
Configuring Two-Door Policies

To configure two-door policies, do the following:

Step 1 Select **Two-Door Policy** from the Doors menu, under the Access Policies submenu. The main window is shown (see Figure 11-10).

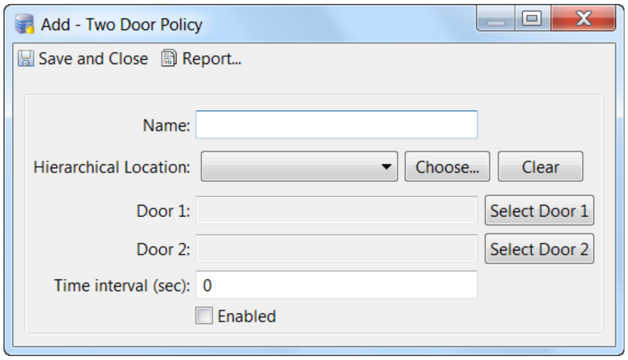
- To modify an existing policy, select the entry and choose **Edit...** to open the detail window. You can also double-click the entry.
- To add a new policy, click **Add...** to open the detail window.
- To remove an policy, highlight the entry and click **Delete**.

Figure 11-10 Two-Door Policy Main Window



Step 2 Complete the fields in the detail window, as shown in the following Figure 11-11:

Figure 11-11 Two-Door Policy Detail Window



Name:

Hierarchical Location:

Door 1:

Door 2:

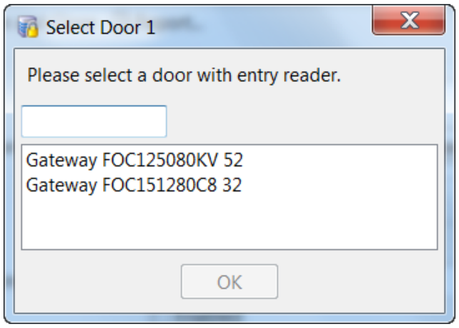
Time interval (sec): 0

□ Enabled

- **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 11-12). 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 11-12 Select Door 1 Window



Please select a door with entry reader.

Gateway FOC125080KV 52
Gateway FOC151280C8 32

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.

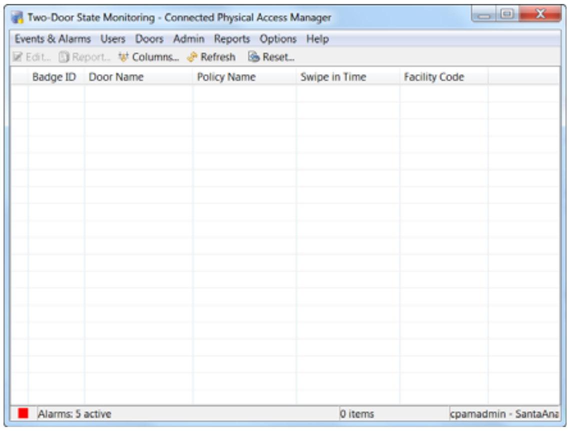
Two-Door State Monitoring

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** submenu. The main window is shown (see Figure 11-13).

Step 2 To display details for the event, highlight an entry and click **Edit...**.

Figure 11-13 Two-Door State Monitoring Main Window


Two-Door State Monitoring - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Report... Columns... Refresh Reset...
Badge ID Door Name Policy Name Swipe in Time Facility Code
Alarms: 5 active
0 items
cpamadmin - SantaAna

An two-door state event has the properties described below, available in the table view or detail window:

Table 11-3 Two-Door State Monitoring Properties

Field	Description
Badge ID	The ID number of the badge.
Door Name	The name of the door accessed.
Policy Name	The name of the two-door policy. See Two-Door Policies, page 11-27 for more information.
Swipe In Time	The day and time when the entry door was accessed.
Facility Code	The facility code.

Step 3 Click **Close** to close the detail window.

CHAPTER 12

Events & Alarms

This chapter describes how to view events and alarms in ICPAM. 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

Events and alarms are captured in real time, and are accessed in the **Events & Alarms** menu, under the **Monitoring** submenu. 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 12-19

Tip See Configuring Events and Alarms, page 12-34 to define or modify event types. To copy or move events to a historical events archive, see Backing Up and Archiving Events, page 12-57.

Events and Alarms in ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), 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 ICPAM. Otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

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 12-57 for more information.

Understanding Event Timestamps

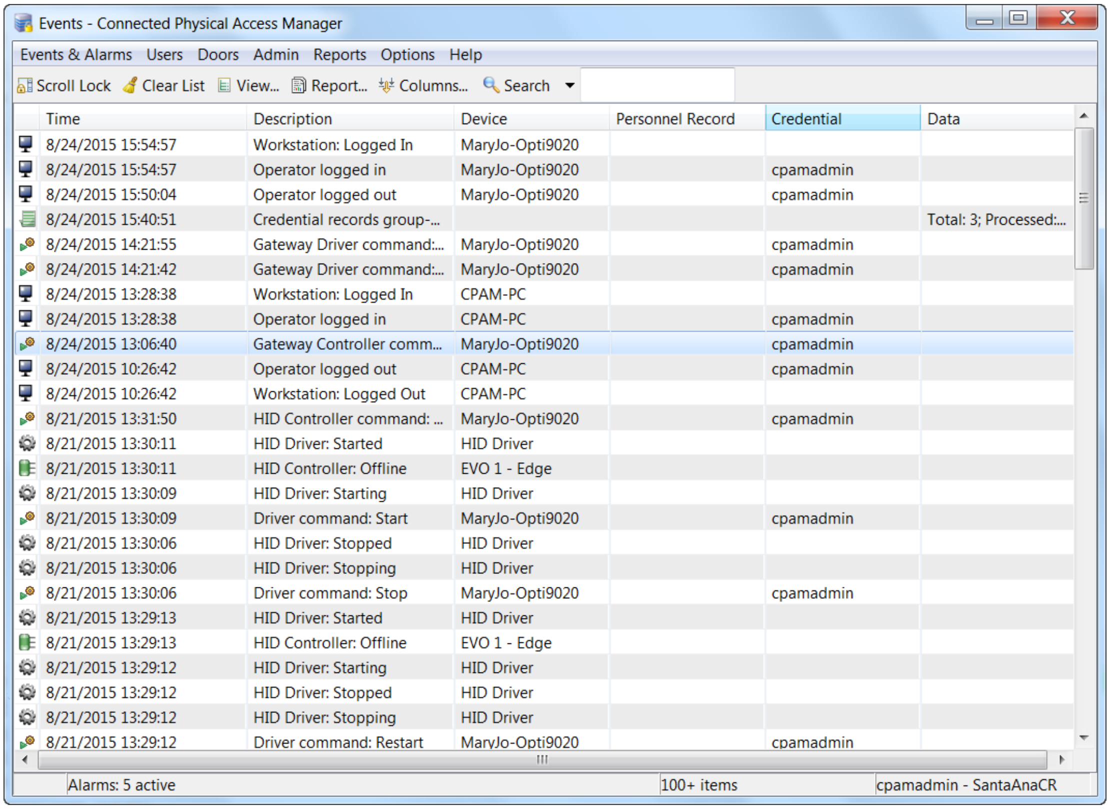
Beginning with Release 1.3.0, events display the timestamp of the ICPAM PC workstation used to view the events. In previous releases, events displayed the ICPAM appliance timestamp.

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** submenu. The Events window (Figure 12-1) shows the most recent events in the access-control system.

Figure 12-1 Events Module Main Window


Events - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Scroll Lock Clear List View... Report... Columns... Search
Alarms: 5 active
100+ items
cpamadmin - SantaAnaCR

Time	Description	Device	Personnel Record	Credential	Data
8/24/2015 15:54:57	Workstation: Logged In	MaryJo-Opti9020			
8/24/2015 15:54:57	Operator logged in	MaryJo-Opti9020		cpamadmin	
8/24/2015 15:50:04	Operator logged out	MaryJo-Opti9020		cpamadmin	
8/24/2015 15:40:51	Credential records group-...				Total: 3; Processed:...
8/24/2015 14:21:55	Gateway Driver command:...	MaryJo-Opti9020		cpamadmin	
8/24/2015 14:21:42	Gateway Driver command:...	MaryJo-Opti9020		cpamadmin	
8/24/2015 13:28:38	Workstation: Logged In	CPAM-PC			
8/24/2015 13:28:38	Operator logged in	CPAM-PC		cpamadmin	
8/24/2015 13:06:40	Gateway Controller comm...	MaryJo-Opti9020		cpamadmin	
8/24/2015 10:26:42	Operator logged out	CPAM-PC		cpamadmin	
8/24/2015 10:26:42	Workstation: Logged Out	CPAM-PC			
8/21/2015 13:31:50	HID Controller command: ...	MaryJo-Opti9020		cpamadmin	
8/21/2015 13:30:11	HID Driver: Started	HID Driver			
8/21/2015 13:30:11	HID Controller: Offline	EVO 1 - Edge			
8/21/2015 13:30:09	HID Driver: Starting	HID Driver			
8/21/2015 13:30:09	Driver command: Start	MaryJo-Opti9020		cpamadmin	
8/21/2015 13:30:06	HID Driver: Stopped	HID Driver			
8/21/2015 13:30:06	HID Driver: Stopping	HID Driver			
8/21/2015 13:30:06	Driver command: Stop	MaryJo-Opti9020		cpamadmin	
8/21/2015 13:29:13	HID Driver: Started	HID Driver			
8/21/2015 13:29:13	HID Controller: Offline	EVO 1 - Edge			
8/21/2015 13:29:12	HID Driver: Starting	HID Driver			
8/21/2015 13:29:12	HID Driver: Stopped	HID Driver			
8/21/2015 13:29:12	HID Driver: Stopping	HID Driver			
8/21/2015 13:29:12	Driver command: Restart	MaryJo-Opti9020		cpamadmin	

Tip Beginning with Release 1.3.0, events display the timestamp of the ICPAM PC workstation used to view the events. In previous releases, events displayed the ICPAM appliance timestamp.

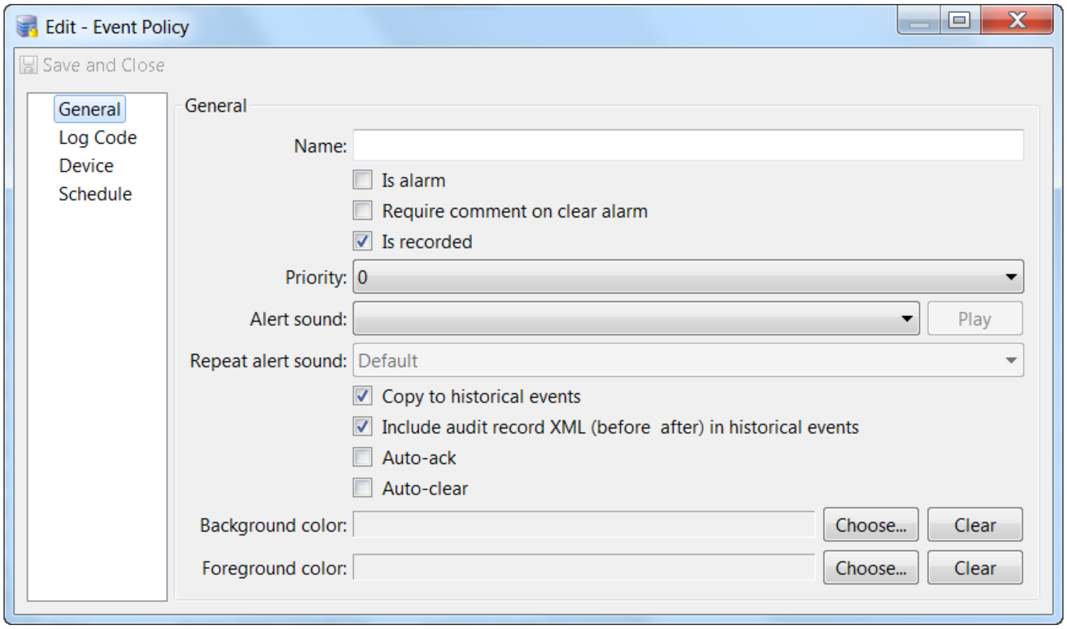
Step 2 Modify the list of records using the following toolbar controls:

- **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 3-10.
- **Columns...**: Define the columns displayed and their order. See Revising the Column Display, page 3-14.
- **Filter**: Filter the events to display a subset of records. To change the number of viewable events, select **Max rows**. See Using Filters, page 3-12.
- **Search**: See Search, page 3-15.

Step 3 Select a record and click **View...** to open the detail window (Figure 12-2). You can also double-click the record.

Figure 12-2 Events Module Detail Window



General

Name:

☐ Is alarm
☐ Require comment on clear alarm
☑ Is recorded

Priority: 0

Alert sound:

Repeat alert sound: Default

☑ Copy to historical events
☑ Include audit record XML (before after) in historical events
☐ Auto-ack
☐ Auto-clear

Background color:

Foreground color:

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

Field	Description
Time	The time and date when the event occurred. **Note** Beginning with Release 1.3.0, events display the timestamp of the ICPAM PC workstation used to view the events. In previous releases, events displayed the ICPAM appliance timestamp.
Time received	The time the event was received and stored in the database. If the event was processed by an external device such as a controller, this may differ from the time, depending on delays or interruptions in communications between the host and the device.
Type	The type of event. The types of events are: • **Event:** A general occurrence within the system, often from external hardware such as a controller. • **Alarm:** An event configured to be an alarm. • **Alarm Annotation:** An event caused by commenting, clearing, or acknowledging alarms. • **Audit Record:** An event caused by an operator modifying a record, such as a badge or personnel record. • **Device Command:** An event caused by an operator executing a device command. • **Device Command Result:** Notification of a completed device command.
Log Code	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 12-34.
Priority	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 12-43.
Description	A description of the event.
Device	The device associated with the event, such as a workstation or hardware module. • **Edit...**: Displays information about the device including type, name, and address. Some fields are editable, depending on the type of device. • **View Status...**: Displays the status of the associated device. For example, if the workstation is logged in to the system or if the hardware module is enabled. • **Commands**: lists any available commands for the device. For example, apply a controller configuration, or send a message to a workstation. • **Show in Graphics Map**: see Map Viewer, page 12-47.
Credential	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. • **Edit...**: Revise the credential (badge, login, etc.) record associated with the event.

Table 12-1 Event Properties (continued)

Field	Description
Personnel Record	If a personnel record is associated with the event, this field displays the person's name. • **Edit...**: Edit the personnel record associated with the event. • **View Photo...**: Displays the associated personnel record photo, if any.
Data	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.
camera	The Video event information of a camera device. • **Live Video**: opens the video player to view live video from the camera associated with the device. • **Event Video**: displays archived video associated with the event, if available. • **Live and Event Video**: opens both live and archived video windows. • **Arrangement**: displays all camera arrangement that includes the camera associated with the event. See Chapter 15, "Video Monitoring" for more information.
Parent Device	Parent Device name of the device on which the event is associated.
Address	Address of the device associated with event.
Sequence Number	Sequence number of credentials during controller credential related events
Watch Level	Displays the credential watch level for the badge associated with the event.

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 12-39.

This section includes the following:

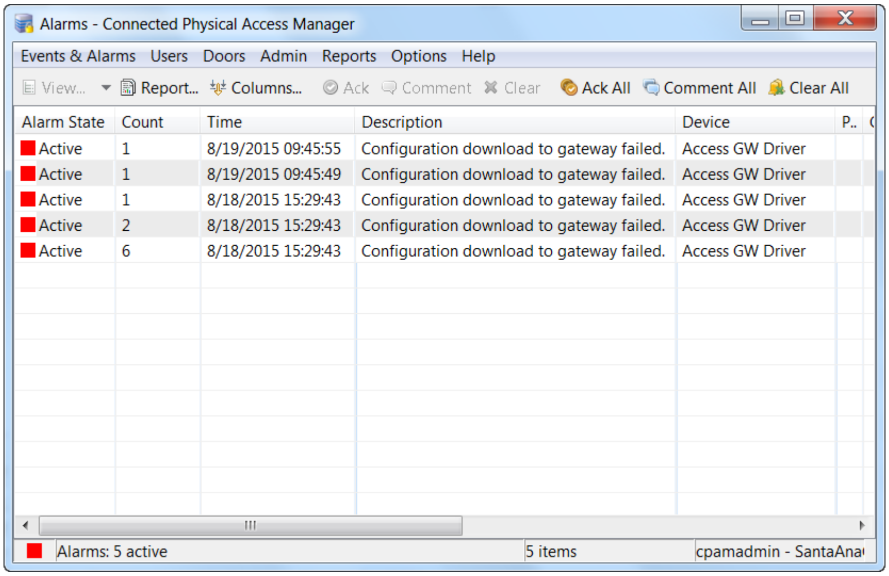
- Main Alarm Window, page 12-8
- Alarm States, page 12-9
- Alarm Detail Window, page 12-9
- Alarm Properties, page 12-10

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



Alarm State	Count	Time	Description	Device	P..
🟥 Active	1	8/19/2015 09:45:55	Configuration download to gateway failed.	Access GW Driver	
🟥 Active	1	8/19/2015 09:45:49	Configuration download to gateway failed.	Access GW Driver	
🟥 Active	1	8/18/2015 15:29:43	Configuration download to gateway failed.	Access GW Driver	
🟥 Active	2	8/18/2015 15:29:43	Configuration download to gateway failed.	Access GW Driver	
🟥 Active	6	8/18/2015 15:29:43	Configuration download to gateway failed.	Access GW Driver	

🟥 Alarms: 5 active   5 items   cpamadmin - SantaAna

Step 2 Modify the list of records using the following toolbar controls:

- **Scroll Lock**: Disables or enables automatic scrolling of the list as new events are inserted.
- **Report...**: View the selected alarms in a separate window, or save the information in a file. See Creating Reports, page 3-10.
- **Columns...**: Define the columns displayed and their order. See Revising the Column Display, page 3-14.

- **Filter**: Filter the alarms to display a sub-set of records. To change the number of displayed alarms, select **Max rows**. See Using Filters, page 3-12.

Step 3 Change the state of an alarm, add a comment, or acknowledge the alarm.

Use the following toolbar buttons or right-click the entry and select an option from the menu.

- **Ack**: Acknowledges an alarm, placing it in an acknowledged state. This means that the operator is aware of the alarm, but it has not been resolved. A solid orange color indicates this state.
- **Comment**: Adds a comment to an alarm. Does not change the state of the alarm. A new comment may be entered, or a previously entered comment may be selected from the drop-down list.
- **Clear**: Places the alarm in a cleared state (resolved) and changes the icon to green.
- **Ack All**: Acknowledges all currently unacknowledged alarms. This means that the operator is aware of the alarms, but they have not been resolved. A solid orange color indicates this state.
- **Comment All**: Adds a comment to all currently unacknowledged alarms. Does not change the state of the alarms. A new comment may be entered, or a previously entered comment may be selected from the drop-down list.
- **Clear All**: Places the alarms in a cleared state (resolved) and changes the icon to green. Make sure all the alarms have been acknowledged before performing this task.

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 can be in one of several states and these states have an associated solid or blinking color as shown in Table 12-2.

Table 12-2 Alarm States

State	Color	Description
Active	Blinking red	The alarm is new, unacknowledged, and unresolved.
Acknowledged	Solid orange	An operator is aware of the alarm, though it remains unresolved.
Cleared	Solid green	The alarm has been acknowledged and resolved. Note that the default filter in the **Alarms** module hides cleared alarms, so these are generally not seen.

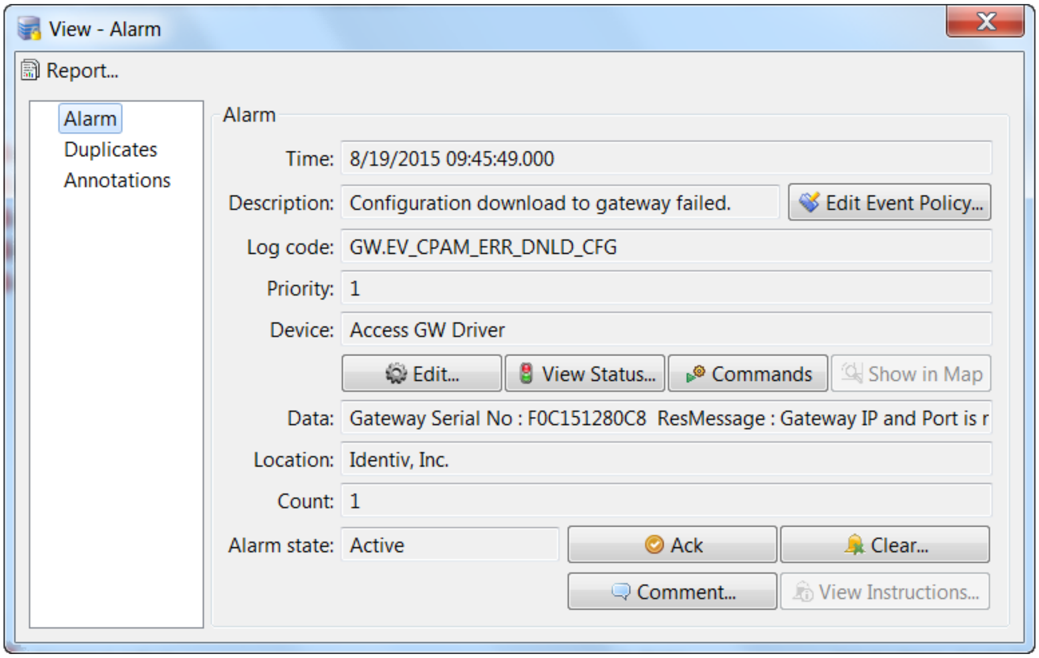
Alarm Detail Window

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

Figure 12-4 Alarms Module Detail Window



View - Alarm

Report...

Alarm

Time: 8/19/2015 09:45:49.000

Description: Configuration download to gateway failed.

Log code: GW.EV_CPAM_ERR_DNLD_CFG

Priority: 1

Device: Access GW Driver

Data: Gateway Serial No : F0C151280C8 ResMessage : Gateway IP and Port is r

Location: Identiv, Inc.

Count: 1

Alarm state: Active

Alarm Properties

An alarm has the following properties, available in the table view or the detail window:

Table 12-3 Alarm Properties

Field	Description
Time	The date and time when the alarm occurred.
Time Received	The time the alarm was received and stored in the database. If the event was processed by an external device such as a controller, this may differ from the time, depending on delays or interruptions in communications between the host and the device.
Site	The site where the alarm occurred.
Log Code	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 12-34.
Priority	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 12-43.
Description	A description of the alarm.

Table 12-3 Alarm Properties (continued)

Field	Description
Device	The device associated with the alarm, such as a workstation or hardware module. • **Edit...**: Displays information about the device including type, name, and address. Some fields are editable, depending on the type of device. • **View Status...**: Displays the status of the associated device. For example, if the workstation is logged in to the system or if the hardware module is enabled. • **Commands**: lists any available commands for the device. For example, apply a controller configuration, or send a message to a workstation. • **Show in Graphics** : see Map Viewer, page 12-47.
Credential	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. • **Edit...**: Revise the credential (badge, login, etc.) record associated with the event.
Watch Level	Displays the Credential Watch Level for the badge associated with the event. See Adding a Color Border to Event Photos (Credential Watch), page 12-24. • **Edit...**: Revise the credential watch level associated with the badge.
Address	The address of the device.
Personnel Record	If a personnel record is associated with the alarm, this field displays the person's name. • **Edit...**: Edit the personnel record associated with the event. • **View Photo...**: Displays the associated personnel record photo, if any.
Data	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.
Count	The number of times this alarm has occurred, including duplicates. Duplicate alarms have all attributes the same except time).

Table 12-3 Alarm Properties (continued)

Field	Description
Alarm State	The state of the alarm. See Alarm States, page 12-9. • **Ack...**: 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. • **Clear...**: Clears the alarm, placing it in a cleared state. This means that the alarm has been resolved. A solid green 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. For more on commenting, refer to Alarm Comments, page 12-12. • **View Instructions...**: Opens a detail window with instructions for dealing with the type of alarm, if any. This button is only active if instructions have been previously defined for this alarm. For more on creating and viewing instructions, refer to Alarm Comments, page 12-12.
Target device	The device associated with the event. For example, the device where a command was executed. • **Edit**: modify the device settings.
camera	The camera associated with the device. • **Live Video**: opens the video player to view live video from the camera associated with the device. • **Event Video**: displays archived video associated with the event, if available. See Chapter 15, "Video Monitoring" for more information.

Alarm Comments

When an alarm occurs, a qualified user has the option to comment on that occurrence by doing the following:

Step 1 Right click on the alarm and press **View** as specified in the Alarm Detail window (Table 12-3).

Step 2 Press the **Comments** button.

The comment window appears.

Step 3 Enter the comment in the comment window then click **OK**.

Optionally, perform this procedure:

Step 1 From the main alarm window, click to highlight the alarm then click the **Comment** button in the task bar.

Alternatively, click the **Comment All** button to type a comment regarding all currently unacknowledged alarms.

The comment window appears.

Step 2 Enter the comment required in the comment window then click **OK**.

Alarm Instructions - Creating

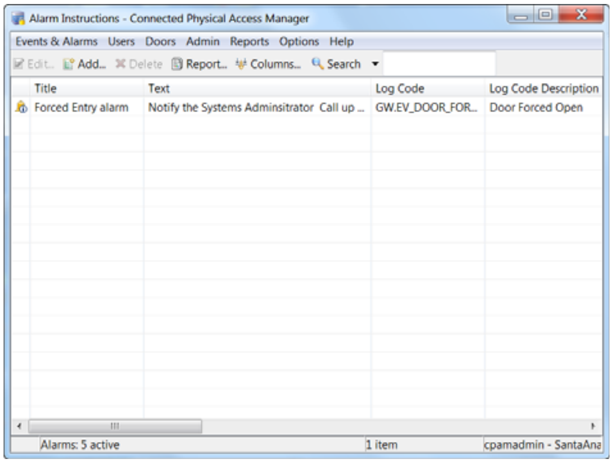
Instructions can be provided for any alarm or group of alarms within the system. These instructions enable the qualified operator to receive and follow instructions for a specific alarm whenever that alarm occurs. Instructions can be designed to appear for the general system or be customized for specific devices, locations, time periods, or device types.

To create and customize an alarm instruction:

Step 1 Select **Alarm Instructions** from the **Configuration** option under **Events & Alarms**.

The Alarm Instructions dialog box appears (Figure 12-5 on page 12-13).

Figure 12-5 Alarm Instructions



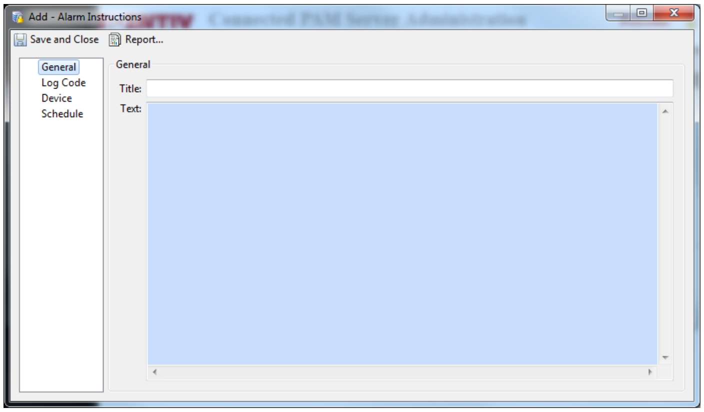
Title	Text	Log Code	Log Code Description
Forced Entry alarm	Notify the Systems Adminsitrator Call up ...	GW.EV_DOOR_FOR...	Door Forced Open

Alarms: 5 active 1 item cpamadmin - SantaAna

Step 2 Click **Add...**

The Add Alarm Instructions dialog box appears as shown in Figure 12-6.

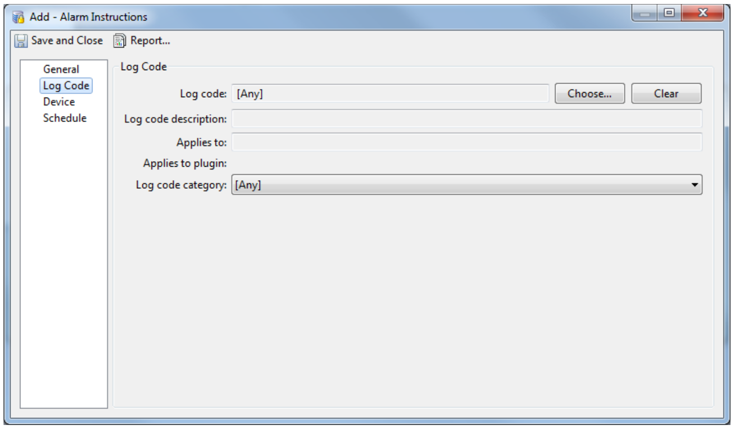
Figure 12-6 Add Alarm Instructions General Window



Step 3 At the General tab page, enter a title for these instructions then click in the Text box and enter the instructions that apply to this alarm instruction set.

Step 4 If necessary, click the **Log Code** tab and the Log Code page appears as shown in Figure 12-7.

Figure 12-7 Add Alarm Instruction Log Code Window

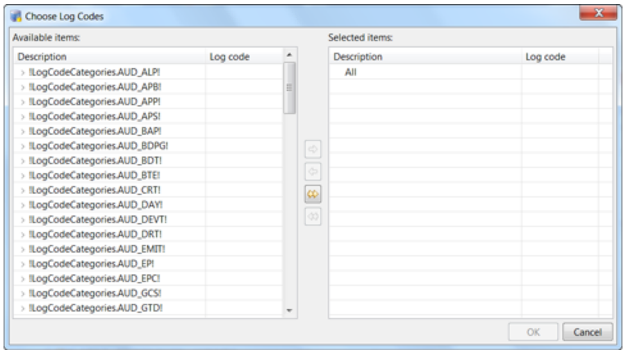


Log Code

Log code: [Any]
Log code description:
Applies to:
Applies to plugin:
Log code category: [Any]

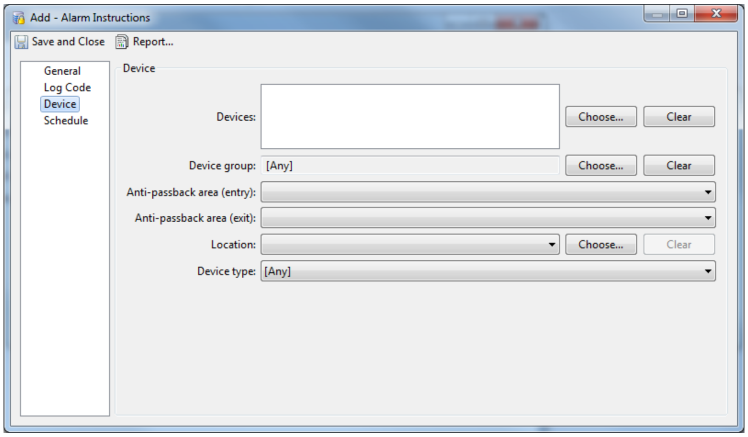
The fields available on this page include:

Table 12-4 Add Alarm Instruction Log Code Properties

Field	Description
Log code	The internal code to identify the event. To select a log code, click **Choose**... The Choose Log Code window appears.  Available items: Description / Log code !LogCodeCategories.AUD_ALP! !LogCodeCategories.AUD_APB! !LogCodeCategories.AUD_APP! !LogCodeCategories.AUD_APS! !LogCodeCategories.AUD_BAP! !LogCodeCategories.AUD_BDPG! !LogCodeCategories.AUD_BDT! !LogCodeCategories.AUD_BTE! !LogCodeCategories.AUD_CRT! !LogCodeCategories.AUD_DAY! !LogCodeCategories.AUD_DEVT! !LogCodeCategories.AUD_DRT! !LogCodeCategories.AUD_EMIT! !LogCodeCategories.AUD_EP! !LogCodeCategories.AUD_EPC! !LogCodeCategories.AUD_GCS! !LogCodeCategories.AUD_GTD! Selected items: Description / Log code All If required, select the appropriate log code for this instruction. The default is [Any]. Log codes can be viewed in the **Event Policy Manager** and defined as alarms. See Modifying Default Event Policies, page 12-34.
Log code description	Enter a description of this log code, if needed.
Applies to	Enter a description of the component(s) or conditions to which this log code applies.
Applies to plugin	If this log code applies to a plug-in component, enter a description of this.
Log code category	If required, click the drop-down option list and select a category to which this log code set applies. The default option is [Any].

Step 5 Click the **Device** tab and the device page appears as shown in Figure 12-8 on page 12-15.

Figure 12-8 Add Alarm Instruction Device Window



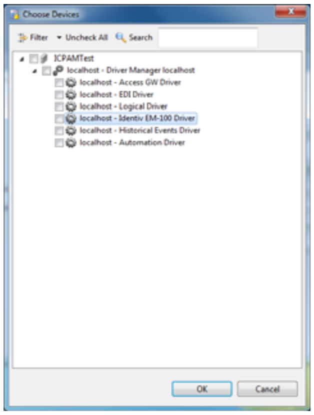
Device group: [Any]

Device type: [Any]

The fields available on this page include:

Table 12-5 Add Alarm Instruction Device Properties

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Devices</b></td><td>Enter the devices to which this instruction set applies. To include devices in this instruction set, click <b>Choose...</b> and the Choose Devices window appears.


Choose Devices
Filter
Uncheck All
Search
ICPAMTest
localhost - Driver Manager localhost
localhost - Access GW Driver
localhost - EDI Driver
localhost - Logical Driver
localhost - Identiv EM-100 Driver
localhost - Historical Events Driver
localhost - Automation Driver
OK
Cancel

Expand the device tree as required and check the boxes of one or more devices then click <b>OK</b>.</td></tr>
</table>

Table 12-5 Add Alarm Instruction Device Properties (continued)

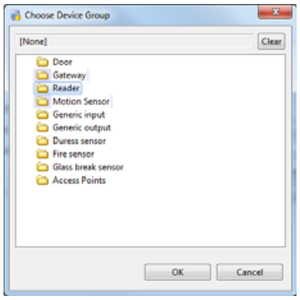
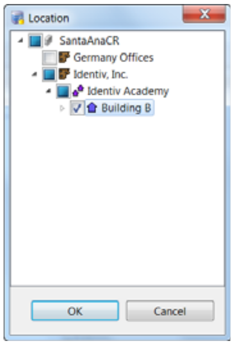
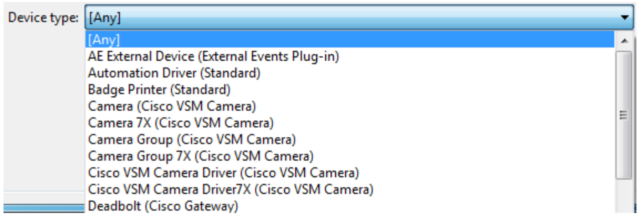
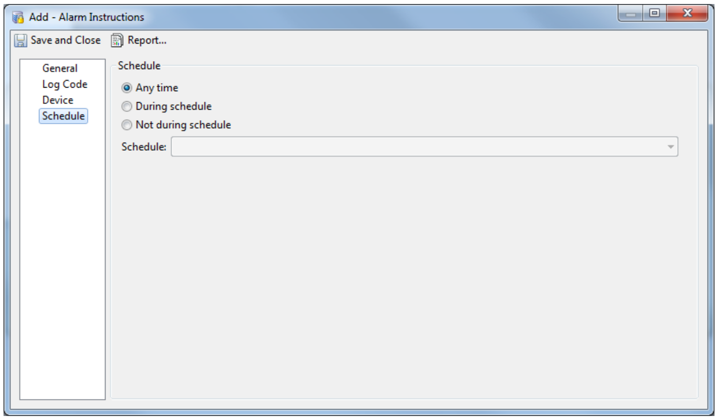
Field	Description
Device group	Select the device group to which this instruction set applies. To select the group, click to drop down the option list.  Choose Device Group [None] Clear Door Gateway Reader Motion Sensor Generic input Generic output Duress sensor Fire sensor Glass break sensor Access Points OK Cancel Select a group then click **OK**. The default is [None].
Anti-passback area (entry)	From the drop-down option list, select the entry point of the anti-passback area to which this instruction set applies. Only those anti-passback areas previously defined for this system appear in this list. For more on defining anti-passback areas, refer to Creating Anti-Passback Areas, page 11-19.
Anti-passback area (exit)	From the drop-down option list, select the exit point of the anti-passback area to which this instruction set applies. Only those anti-passback areas previously defined for this system appear in this list. For more on defining anti-passback areas, refer to Creating Anti-Passback Areas, page 11-19.
Location	Select one or more designated locations where this instruction set applies. Only these locations can use the instruction set. To specify locations, click **Choose...** and the Location window appears.  Location SantaAnaCR Germany Offices Identiv, Inc. Identiv Academy Building B OK Cancel Select one or more locations by checking the required box then click **OK**.

Table 12-5 Add Alarm Instruction Device Properties (continued)

Field	Description
Device type	Select the type of device to which this instruction set applies. To select a device type, click in this field and a drop-down option list appears.  Device type: [Any] [Any] AE External Device (External Events Plug-in) Automation Driver (Standard) Badge Printer (Standard) Camera (Cisco VSM Camera) Camera 7X (Cisco VSM Camera) Camera Group (Cisco VSM Camera) Camera Group 7X (Cisco VSM Camera) Cisco VSM Camera Driver (Cisco VSM Camera) Cisco VSM Camera Driver7X (Cisco VSM Camera) Deadbolt (Cisco Gateway) Click to select the device type required. The default value is [Any].

Step 6 Click the **Schedule** tab and the Schedule page appears like Figure 12-9 on page 12-17.

Figure 12-9 Add Alarm Instructions Schedule Page



Schedule

● Any time
○ During schedule
○ Not during schedule

Schedule:

The fields available on this page include:

Table 12-6 Add Alarm Instruction Schedule Properties

Field	Description
Any time	Select this radio button if this instruction set should apply at any time. This is the default selection.
During schedule	Select this radio button to specify a defined schedule during which this instruction set applies. The Schedule field is activated. Select from one of the existing schedules.

Table 12-6 Add Alarm Instruction Schedule Properties (continued)

Field	Description
Not during schedule	Select this radio button to specify that this instruction set is not active during the designated schedule. The Schedule field is activated. Select from one of the existing schedules.
Schedule	If the 'During schedule' or 'Not during schedule' option is selected, this field is activated. Click to select an existing schedule from the drop-down list. Only those schedules previously defined for this system appear in this option list. To create new schedules, refer to Using the Schedule Manager, page 11-9.

Alarm Instructions - Viewing

To view existing alarm instructions:

Step 1 From the Alarm window, right click on the alarm to investigate and press **View** as specified in Viewing Alarms, page 12-8.

The Alarm Detail window appears as shown in Alarm Detail Window, page 12-9.

Step 2 Press the **Instructions** button.

The instructions window appears. The Instructions button is only active if instructions have been specified for this alarm. For more on defining alarm instructions, refer to Alarm Instructions - Creating, page 12-13.

Step 3 Read the instructions on this page and perform the operation specified.

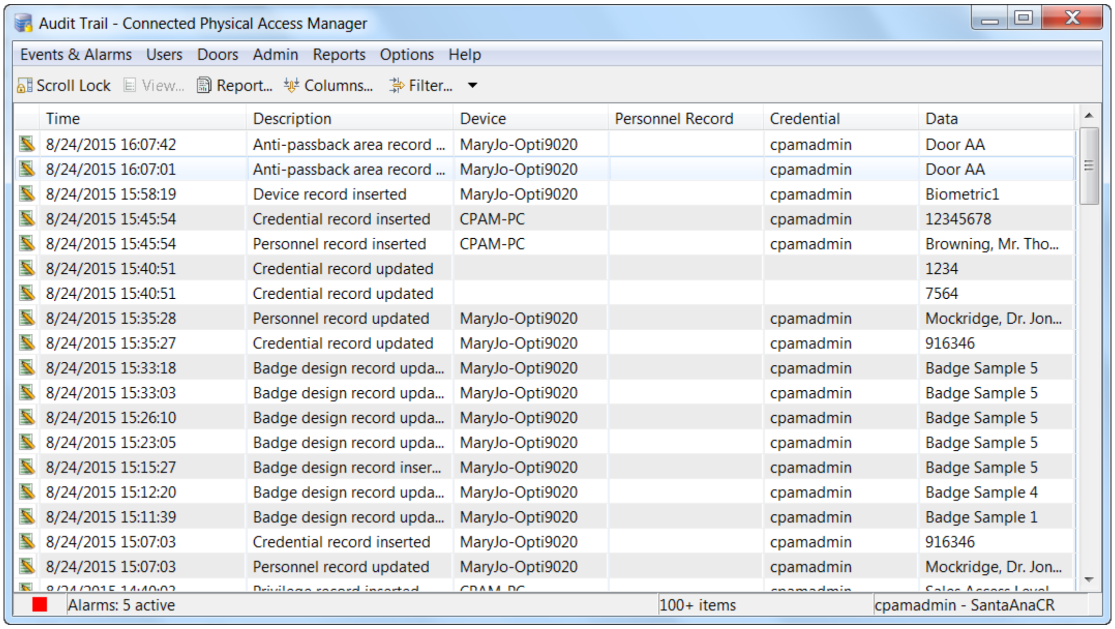
Step 4 Click **OK** when finished.

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 12-10) shows the most recent audit records.

Figure 12-10 Audit Trail Main Window



Audit Trail - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Scroll Lock View... Report... Columns... Filter...

Time	Description	Device	Personnel Record	Credential	Data
8/24/2015 16:07:42	Anti-passback area record ...	MaryJo-Opti9020		cpamadmin	Door AA
8/24/2015 16:07:01	Anti-passback area record ...	MaryJo-Opti9020		cpamadmin	Door AA
8/24/2015 15:58:19	Device record inserted	MaryJo-Opti9020		cpamadmin	Biometric1
8/24/2015 15:45:54	Credential record inserted	CPAM-PC		cpamadmin	12345678
8/24/2015 15:45:54	Personnel record inserted	CPAM-PC		cpamadmin	Browning, Mr. Tho...
8/24/2015 15:40:51	Credential record updated				1234
8/24/2015 15:40:51	Credential record updated				7564
8/24/2015 15:35:28	Personnel record updated	MaryJo-Opti9020		cpamadmin	Mockridge, Dr. Jon...
8/24/2015 15:35:27	Credential record updated	MaryJo-Opti9020		cpamadmin	916346
8/24/2015 15:33:18	Badge design record upda...	MaryJo-Opti9020		cpamadmin	Badge Sample 5
8/24/2015 15:33:03	Badge design record upda...	MaryJo-Opti9020		cpamadmin	Badge Sample 5
8/24/2015 15:26:10	Badge design record upda...	MaryJo-Opti9020		cpamadmin	Badge Sample 5
8/24/2015 15:23:05	Badge design record upda...	MaryJo-Opti9020		cpamadmin	Badge Sample 5
8/24/2015 15:15:27	Badge design record inser...	MaryJo-Opti9020		cpamadmin	Badge Sample 5
8/24/2015 15:12:20	Badge design record upda...	MaryJo-Opti9020		cpamadmin	Badge Sample 4
8/24/2015 15:11:39	Badge design record upda...	MaryJo-Opti9020		cpamadmin	Badge Sample 1
8/24/2015 15:07:03	Credential record inserted	MaryJo-Opti9020		cpamadmin	916346
8/24/2015 15:07:03	Personnel record updated	MaryJo-Opti9020		cpamadmin	Mockridge, Dr. Jon...
8/24/2015 14:40:02	Privilege record inserted	CPAM-PC		cpamadmin	Sales Access Level

Alarms: 5 active 100+ items cpamadmin - SantaAnaCR

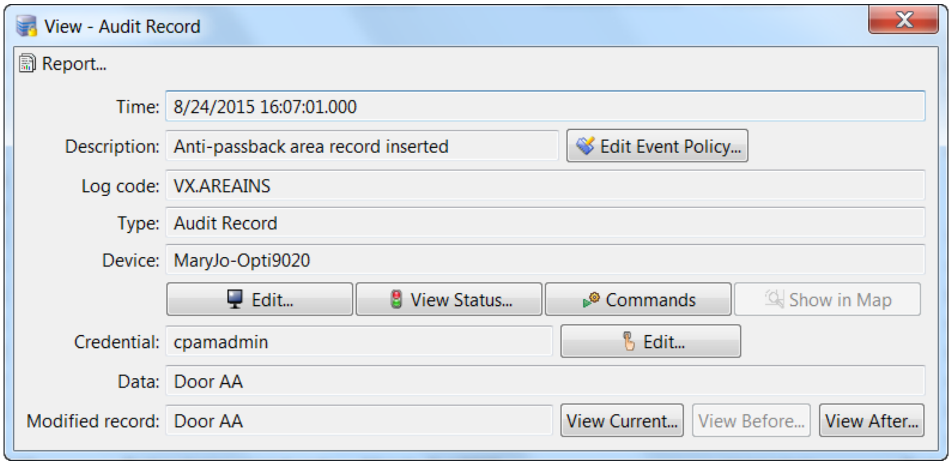
Step 2 Modify the list of records using the following toolbar controls:

- **Scroll Lock:** Disable or enable automatic scrolling of the list as new audit records are inserted.
- **Report...:** See Creating Reports, page 3-10.
- **Columns...:** See Revising the Column Display, page 3-14.
- **Filter:** See Using Filters, page 3-12.

Step 3 Select a record and click **View...** to open the detail window (Figure 12-11). You can also double-click the record.

Step 4 Review the properties and actions for the record. See Table 12-7 for field descriptions.

Figure 12-11 View Audit Trail Detail Window



View - Audit Record

Report...

Time: 8/24/2015 16:07:01.000

Description: Anti-passback area record inserted

Log code: VX.AREAINS

Type: Audit Record

Device: MaryJo-Opti9020

Credential: cpamadmin

Data: Door AA

Modified record: Door AA

Table 12-7 Audit Trail Event Properties

Field	Description
Time	The time the event was received and stored in the database. If the event was processed by an external device such as a controller, this may differ from the time, depending on delays or interruptions in communications between the host and the device.
Description	A description of the event.
Site	A site is a single instance of a ICPAM database.
Log Code	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 12-34.
Type	The type of event. The types of events are: • **Event:** A general occurrence within the system, often from external hardware such as a controller. • **Alarm:** An event configured to be an alarm. • **Alarm Annotation:** An event caused by commenting, clearing, or acknowledging alarms. • **Audit Record:** An event caused by an operator modifying a record, such as a badge or personnel record. • **Device Command:** An event caused by an operator executing a device command. • **Device Command Result:** Notification of a completed device command.
Priority	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 12-43.

Table 12-7 Audit Trail Event Properties (continued)

Field	Description
Device	The device associated with the event, such as a workstation or hardware module. • **Edit...**: Displays information about the device including type, name, and address. Some fields are editable, depending on the type of device. • **View Status...**: Displays the status of the associated device. For example, if the workstation is logged in to the system or if the hardware module is enabled. • **Commands**: lists any available commands for the device. For example, apply a controller configuration, or send a message to a workstation. • **Show in Graphics Map**: see Map Viewer, page 12-47.
Credential	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. • **Edit...**: Revise the credential (badge, login, etc.) record associated with the event.
Watch Level	Displays the Credential Watch Level for the badge associated with the event. See Adding a Color Border to Event Photos (Credential Watch), page 12-24. • **Edit...**: Revise the credential watch level associated with the badge.
Personnel Record	If a personnel record is associated with the event, this field displays the person's name. • **Edit...**: Edit the personnel record associated with the event. • **View Photo...**: Displays the associated personnel record photo, if any.
Data	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.
Modified Record	The item changed by the user. • **View Current...**: Opens a detail window of the modified record, as it exists currently. • **View Before...**: Opens a detail window of the modified record, as it existed before the modification. • **View After...**: Opens a detail window of the modified record, as it existed after the modification.

Viewing Recent Events for a Device, Driver, or Location

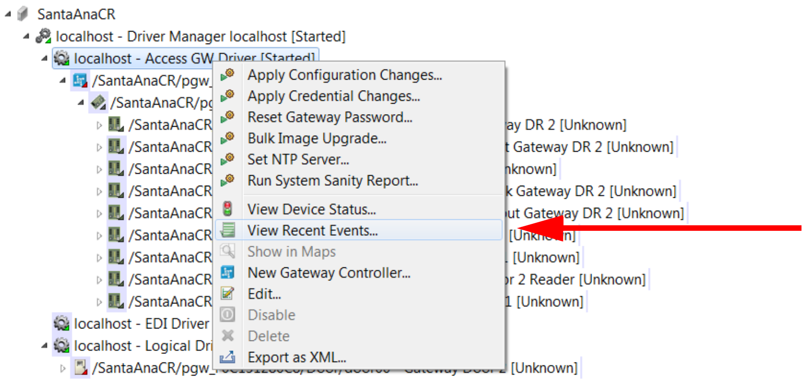
To view a list of recent events for a device or driver, do the following:

Step 1 Select **Hardware - Tree** or **Door/Location-based Hardware** from the **Doors** menu.

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

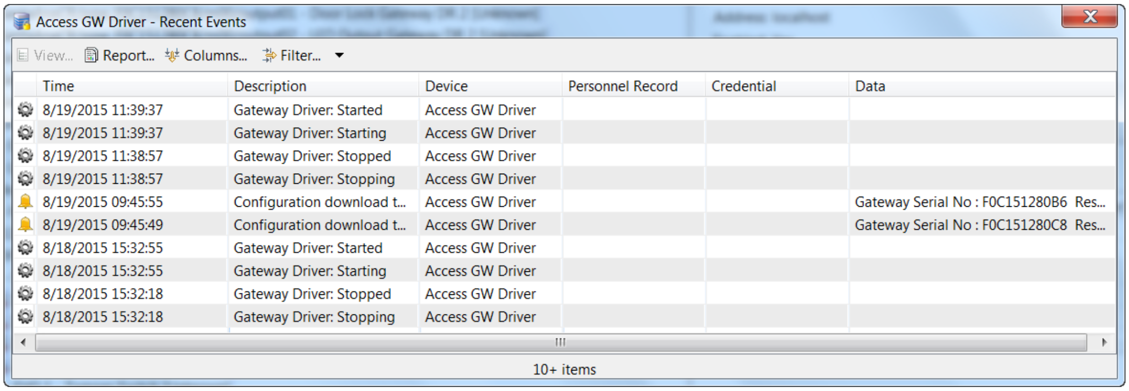
Step 3 Right-click the device or driver, and select **View Recent Events** from the drop-down menu, as shown in Figure 12-12.

Figure 12-12 View Recent Events Menu



Step 4 Double-click an event to view event details, as shown in Figure 12-13.

Figure 12-13 Recent Events



Time	Description	Device	Personnel Record	Credential	Data
8/19/2015 11:39:37	Gateway Driver: Started	Access GW Driver			
8/19/2015 11:39:37	Gateway Driver: Starting	Access GW Driver			
8/19/2015 11:38:57	Gateway Driver: Stopped	Access GW Driver			
8/19/2015 11:38:57	Gateway Driver: Stopping	Access GW Driver			
8/19/2015 09:45:55	Configuration download t...	Access GW Driver			Gateway Serial No : F0C151280B6 Res...
8/19/2015 09:45:49	Configuration download t...	Access GW Driver			Gateway Serial No : F0C151280C8 Res...
8/18/2015 15:32:55	Gateway Driver: Started	Access GW Driver			
8/18/2015 15:32:55	Gateway Driver: Starting	Access GW Driver			
8/18/2015 15:32:18	Gateway Driver: Stopped	Access GW Driver			
8/18/2015 15:32:18	Gateway Driver: Stopping	Access GW Driver			

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 12-23
- Adding a Color Border to Event Photos (Credential Watch), page 12-24
- Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 12-27

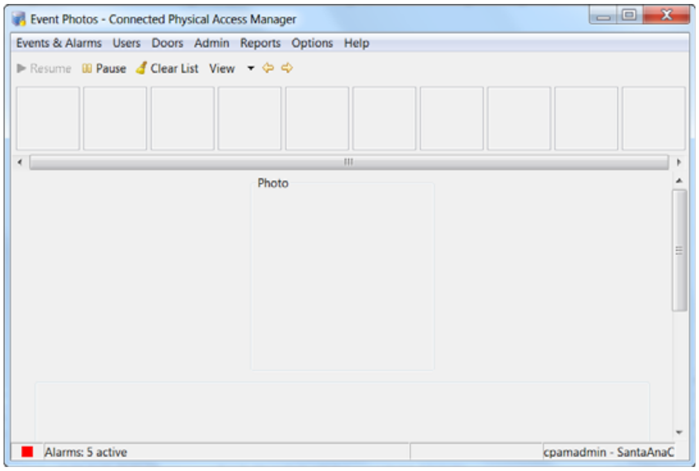
Viewing Event Photos

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** submenu.

Step 2 Select a photo to display the associated event (Figure 12-14).

Figure 12-14 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 3-12 and Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 12-27).
- **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.

Tip

See Viewing Events, Alarms, and Audit Trail Records, page 12-3 for field descriptions. To make the event fields read-only, see Configuring Events and Alarms, page 12-34.

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:

Step 1 Enable Credential Watch Levels menu:

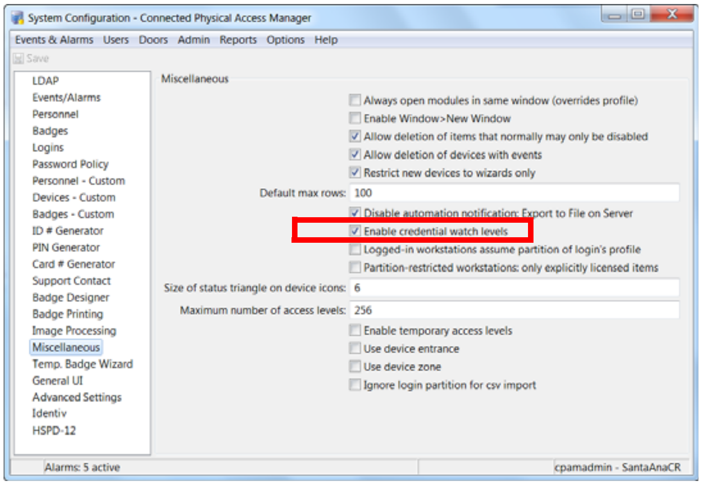
a. Choose **System Configuration** from the Admin menu.

b. Choose the **Miscellaneous** tab.

c. Select the **Enable credential watch levels** check box.

d. Click **Save**.

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



Miscellaneous

☐ Always open modules in same window (overrides profile)
☐ Enable Window>New Window
☑ Allow deletion of items that normally may only be disabled
☑ Allow deletion of devices with events
☑ Restrict new devices to wizards only
Default max rows: 100
☑ Disable automation notification: Export to File on Server
☑ Enable credential watch levels
☐ Logged-in workstations assume partition of login's profile
☐ Partition-restricted workstations: only explicitly licensed items
Size of status triangle on device icons: 6
Maximum number of access levels: 256
☐ Enable temporary access levels
☐ Use device entrance
☐ Use device zone
☐ Ignore login partition for csv import

Step 2 Add credential watch access privileges for user profiles:

a. Select **Profiles** from the **Users** menu.

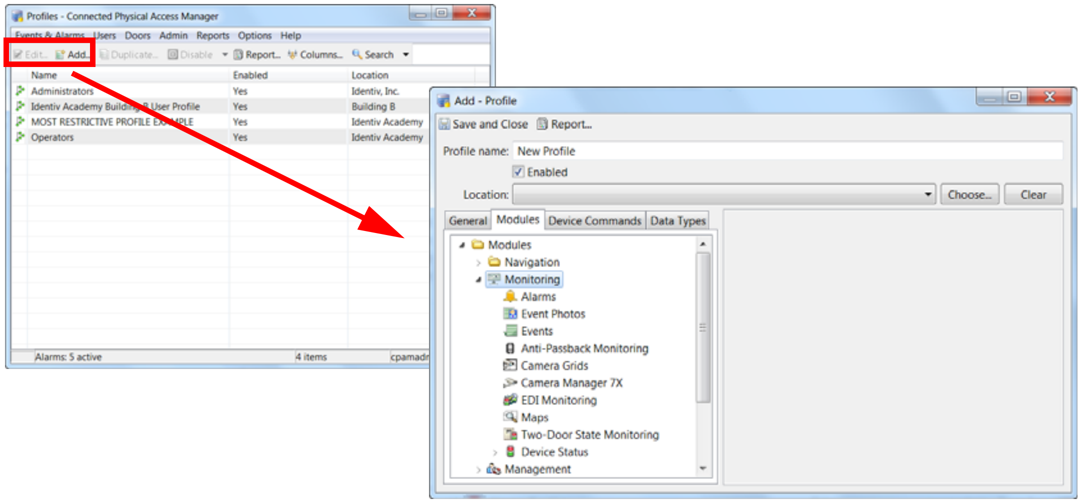
b. Click **Add** or select an existing profile and click **Edit**.

c. Click the **Module** tab.

d. Click the **Quick Launch** module in the left window.

e. Select the options in the panel to the right.

f. Click **Save and Close**.


Profiles - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Duplicate... Disable Report... Columns... Search
Add - Profile
Save and Close Report...
Choose... Clear
General Modules Device Commands Data Types
Modules
Navigation
Monitoring
Alarms
Event Photos
Events
Anti-Passback Monitoring
Camera Grids
Camera Manager 7X
EDI Monitoring
Maps
Two-Door State Monitoring
Device Status
Management

Name	Enabled	Location
Administrators	Yes	Identiv, Inc.
Identiv Academy Building B User Profile	Yes	Building B
MOST RESTRICTIVE PROFILE EXAMPLE	Yes	Identiv Academy
Operators	Yes	Identiv Academy

Alarms: 5 active 4 items cpamadr

Profile name: New Profile

☑ Enabled

Location:

Tip For more information, see Chapter 4, “Configuring User Access for the ICPAM Desktop Client”.

Step 3 (Optional) Assign the profile to the user login, if necessary:

a. Select **Login** from the **Users** menu.

b. Click **Add** or select an existing user and click **Edit**.

c. Select **Profiles**.

d. Select the profile that includes the required access privileges.

e. Click **Save and Close**.

Step 4 (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.

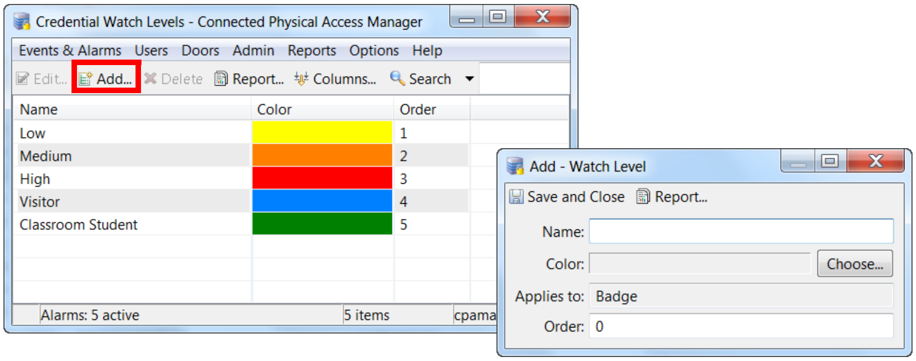
b. Click **Add** or select an existing level and click **Edit**.

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**.



Name	Color	Order
Low	🟨	1
Medium	🟧	2
High	🟥	3
Visitor	🟦	4
Classroom Student	🟩	5

Name:

Color:

Applies to: Badge

Order: 0

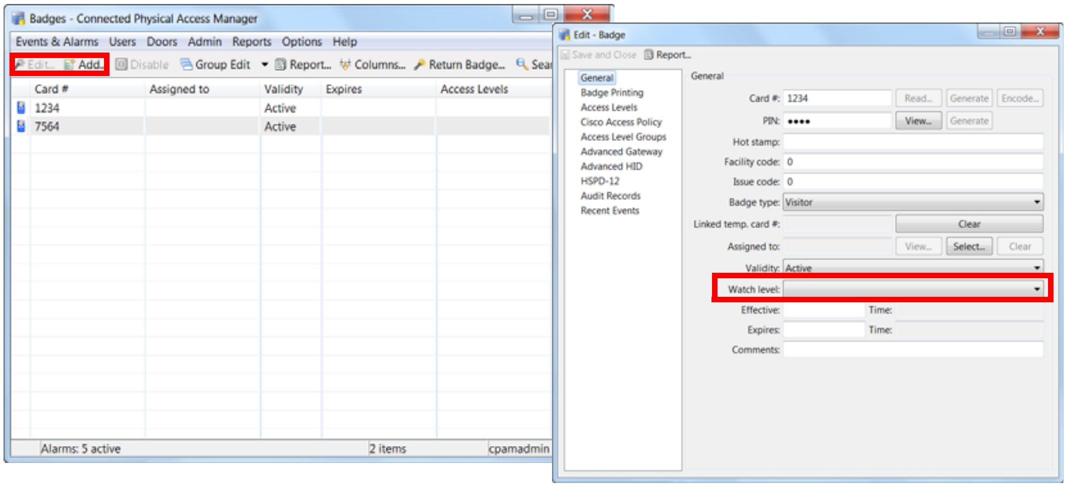
Step 5 Add the credential watch level to a badge configuration:

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**.



Card #	Assigned to	Validity	Expires	Access Levels
1234		Active		
7564		Active		

Card #: 1234

PIN: ●●●●

Hot stamp:

Facility code: 0

Issue code: 0

Badge type: Visitor

Linked temp. card #:

Assigned to:

Validity: Active

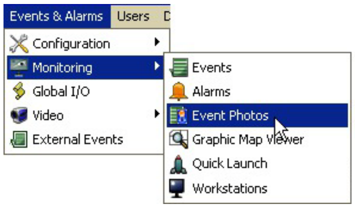
Watch level:

Effective: Time:

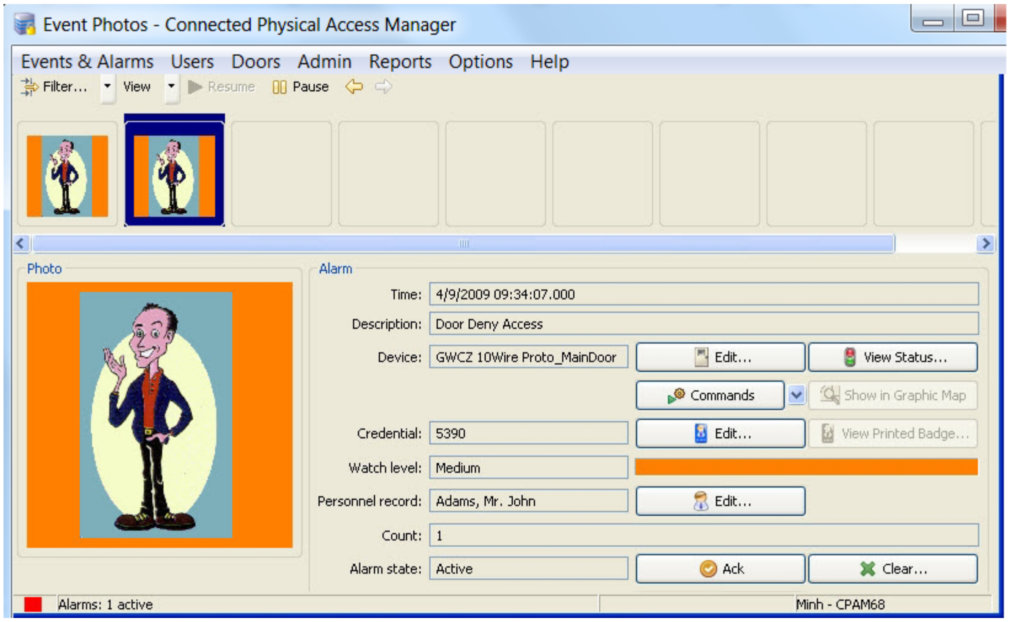
Expires: Time:

Comments:

Step 6 Open the **Event Photos** module: select **Event Photos** from the Events & Alarms menu, in the **Monitoring** submenu.



Step 7 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".



Time: 4/9/2009 09:34:07.000
Description: Door Deny Access
Device: GWCZ 10Wire Proto_MainDoor
Credential: 5390
Watch level: Medium
Personnel record: Adams, Mr. John
Count: 1
Alarm state: Active

Alarms: 1 active
Minh - CPAM68

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.

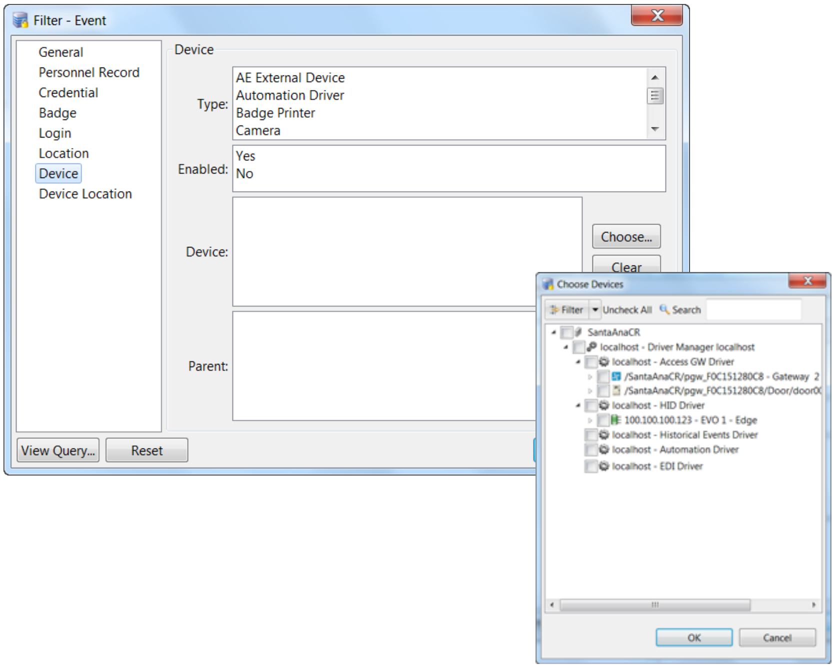
b. In the filter window, select the **Device** tab then select the **Choose** button (see Figure 12-15).

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.

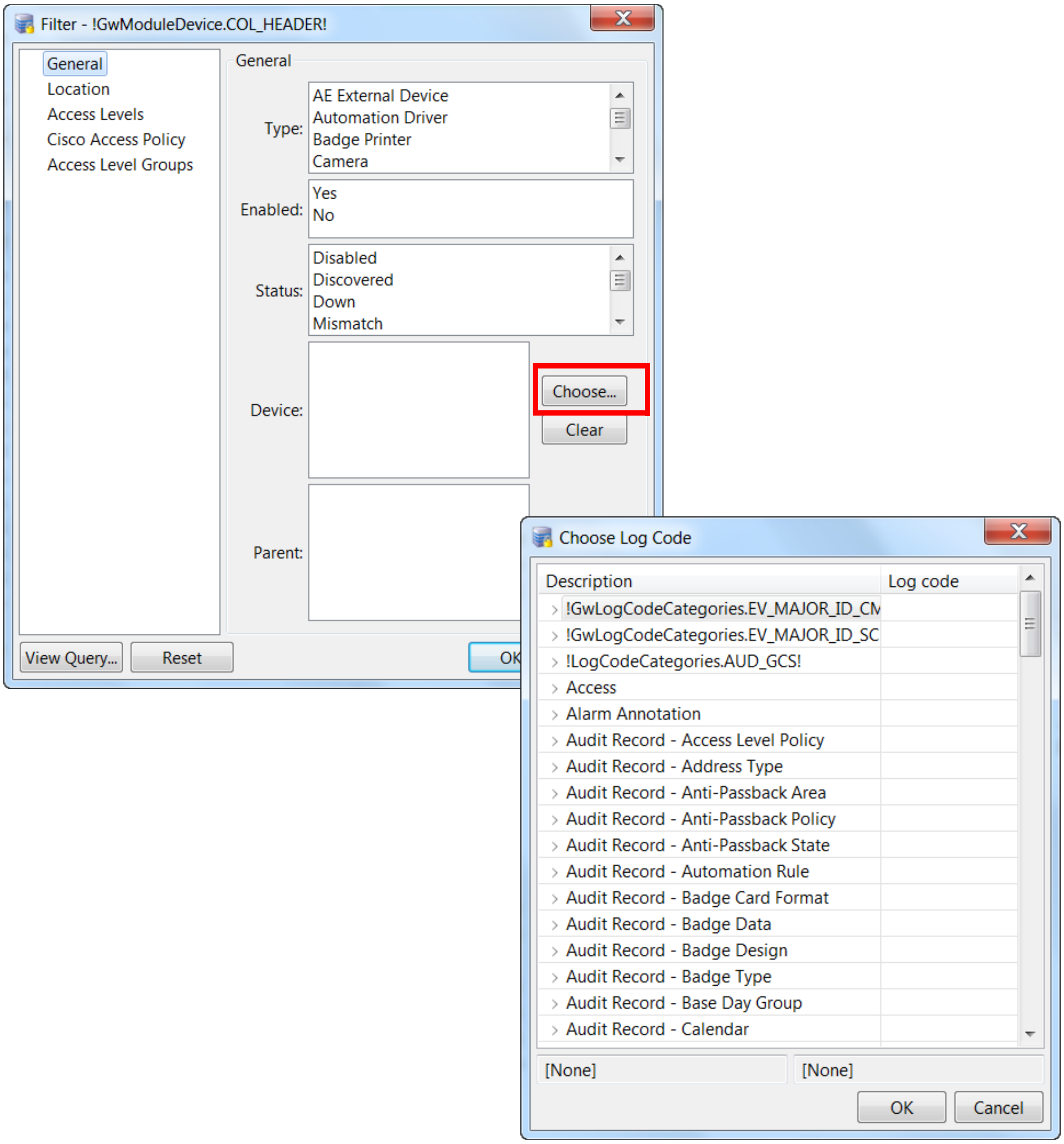
Figure 12-15 Filter Device Window



Step 2 To display the photo once for each badge presentation:

a. In the filter window, select the **General** tab then select the **Choose** button in the Log Code field (see Figure 12-16 on page 12-29).

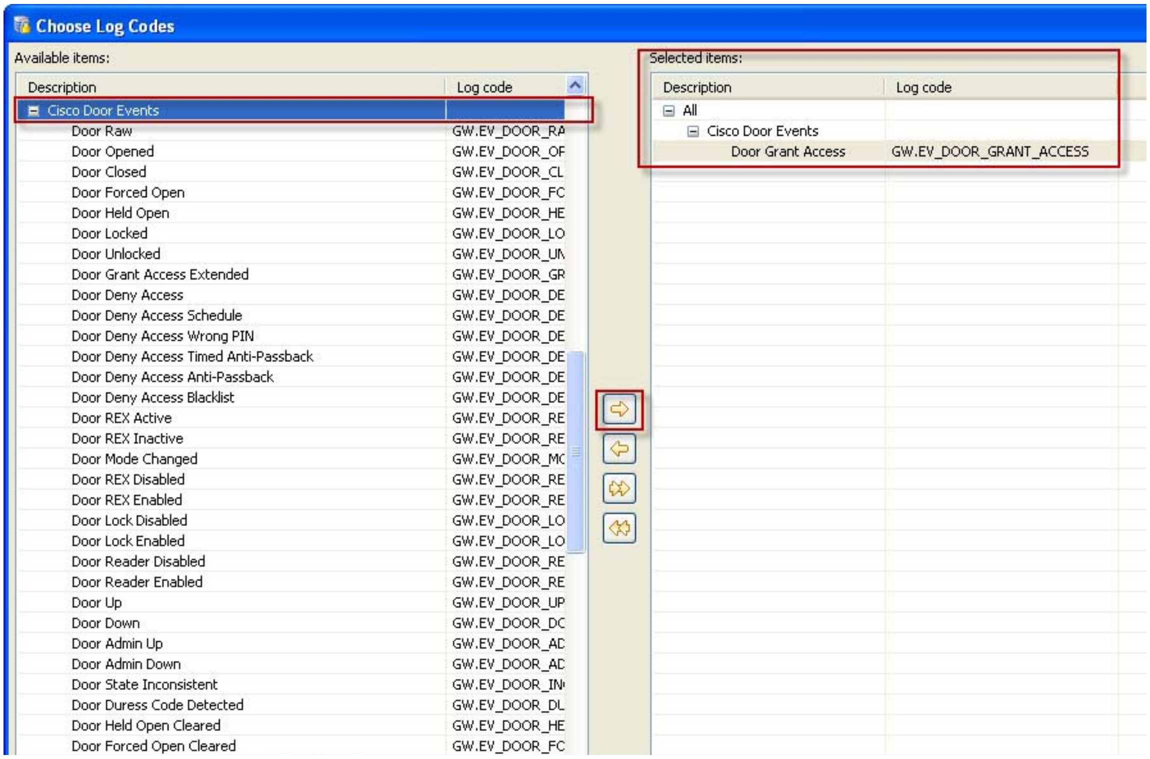
Figure 12-16 Filter Log Code



Description	Log code
!GwLogCodeCategories.EV_MAJOR_ID_CM	
!GwLogCodeCategories.EV_MAJOR_ID_SC	
!LogCodeCategories.AUD_GCS!	
Access	
Alarm Annotation	
Audit Record - Access Level Policy	
Audit Record - Address Type	
Audit Record - Anti-Passback Area	
Audit Record - Anti-Passback Policy	
Audit Record - Anti-Passback State	
Audit Record - Automation Rule	
Audit Record - Badge Card Format	
Audit Record - Badge Data	
Audit Record - Badge Design	
Audit Record - Badge Type	
Audit Record - Base Day Group	
Audit Record - Calendar	

b. Select the events to be displayed in Event Photos, as shown in Figure 12-17. For example, select **Door Grant Access**.

Figure 12-17 Select the Log Code



Available items:

Description	Log code
⊟ Cisco Door Events	
Door Raw	GW.EV_DOOR_RA
Door Opened	GW.EV_DOOR_OF
Door Closed	GW.EV_DOOR_CL
Door Forced Open	GW.EV_DOOR_FC
Door Held Open	GW.EV_DOOR_HE
Door Locked	GW.EV_DOOR_LO
Door Unlocked	GW.EV_DOOR_UN
Door Grant Access Extended	GW.EV_DOOR_GR
Door Deny Access	GW.EV_DOOR_DE
Door Deny Access Schedule	GW.EV_DOOR_DE
Door Deny Access Wrong PIN	GW.EV_DOOR_DE
Door Deny Access Timed Anti-Passback	GW.EV_DOOR_DE
Door Deny Access Anti-Passback	GW.EV_DOOR_DE
Door Deny Access Blacklist	GW.EV_DOOR_DE
Door REX Active	GW.EV_DOOR_RE
Door REX Inactive	GW.EV_DOOR_RE
Door Mode Changed	GW.EV_DOOR_MC
Door REX Disabled	GW.EV_DOOR_RE
Door REX Enabled	GW.EV_DOOR_RE
Door Lock Disabled	GW.EV_DOOR_LO
Door Lock Enabled	GW.EV_DOOR_LO
Door Reader Disabled	GW.EV_DOOR_RE
Door Reader Enabled	GW.EV_DOOR_RE
Door Up	GW.EV_DOOR_UP
Door Down	GW.EV_DOOR_DC
Door Admin Up	GW.EV_DOOR_AD
Door Admin Down	GW.EV_DOOR_AD
Door State Inconsistent	GW.EV_DOOR_IN
Door Duress Code Detected	GW.EV_DOOR_DL
Door Held Open Cleared	GW.EV_DOOR_HE
Door Forced Open Cleared	GW.EV_DOOR_FC

Selected items:

Description	Log code
⊟ All	
⊟ Cisco Door Events	
Door Grant Access	GW.EV_DOOR_GRANT_ACCESS

c. Click **OK** to close the windows and save the changes.

Recording External Events

External applications can record events in ICPAM 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 12-31. This file also defines the categories for the log codes.
2. Create a Text File to Define the Event Names in ICPAM, page 12-31.
3. Import the Files into ICPAM, page 12-32.
4. Add external events and alarms to ICPAM using the **recordExtEvent** API, as described in the *Identiv 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 ICPAM. This file also defines the category for the events and is imported into ICPAM 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

```
<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 ICPAM

To define the log code names displayed in ICPAM, 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

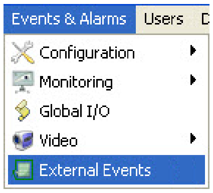
Cisco_VSM=Cisco Video Surveillance Manager

The file is saved with the `.properties` extension. For example: `AppExtMessages.properties`.

Import the Files into ICPAM

Once the XML and properties files are created, import the files into the ICPAM External Events module.

Step 1 Select **External Events** from the **Events & Alarms** menu.



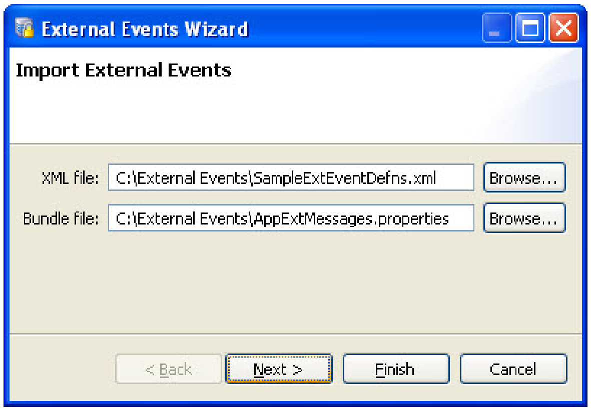
Step 2 Click **Import**.

Step 3 Do the following:

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 ICPAM.

b. Click **Next** to preview the settings, or click **Finish** to save the changes.



XML file: C:\External Events\SampleExtEventDefns.xml

Bundle file: C:\External Events\AppExtMessages.properties

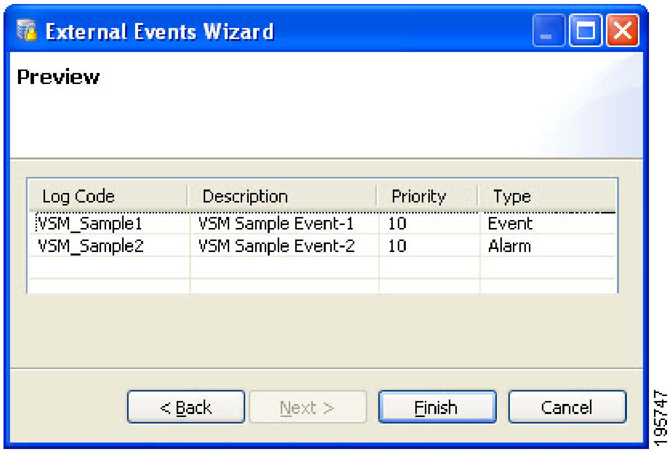
For instructions to create these files, see:

- Define External Event Types Using the Event Definition Format, page 12-31
- Create a Text File to Define the Event Names in ICPAM, page 12-31

Step 4 (Optional) Preview the settings.

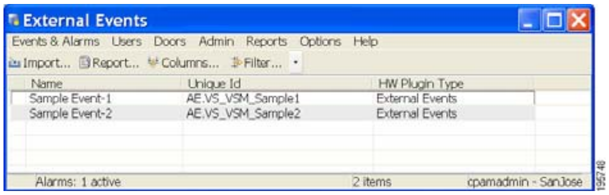
Step 5 Click **Finish** to save the changes

Step 6 Click **Back** to select a different file.



Log Code	Description	Priority	Type
VSM_Sample1	VSM Sample Event-1	10	Event
VSM_Sample2	VSM Sample Event-2	10	Alarm

Step 7 The new log codes are displayed in the main External Events window.



Name	Unique Id	HW Plugin Type
Sample Event-1	AE.VS_VSM_Sample1	External Events
Sample Event-2	AE.VS_VSM_Sample2	External Events

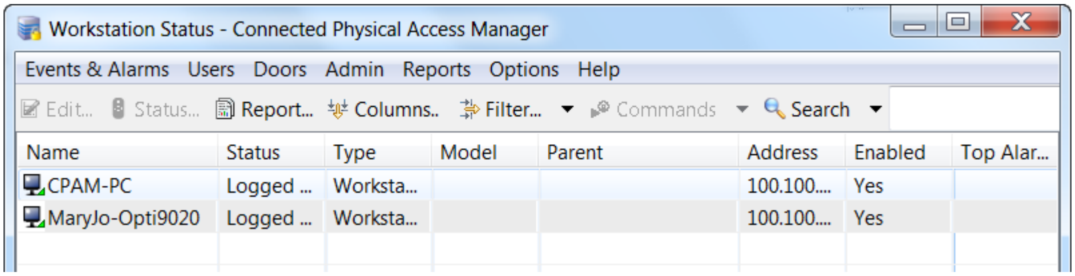
Alarms: 1 active 2 items cpamadmin - SanJose

Step 8 Add external events and alarms to ICPAM using the **recordExtEvent** API, as described in the *Identiv Physical Access Control API Reference Guide*.

Viewing Workstation Activity

To view a summary of the users who access the system, select **Workstations** from the **Events & Alarms** menu, under the **Monitoring** submenu. The Workstations window (see Figure 12-18) shows the most recent events in the access-control system.

Figure 12-18 Workstations Main Window



Name	Status	Type	Model	Parent	Address	Enabled	Top Alar...
CPAM-PC	Logged ...	Worksta...			100.100....	Yes	
MaryJo-Opti9020	Logged ...	Worksta...			100.100....	Yes	

Tip 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 ICPAM 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

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):
  - **a.** Log code
  - **b.** Log code category
  - **c.** Device instance
  - **d.** Device group
  - **e.** Partition
  - **f.** Hierarchical location (Building, Area, etc.)
  - **g.** Device type
  - **h.** Time schedule
  - **i.** 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 ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (see Logins Settings, page 17-10 for more information on this), 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.

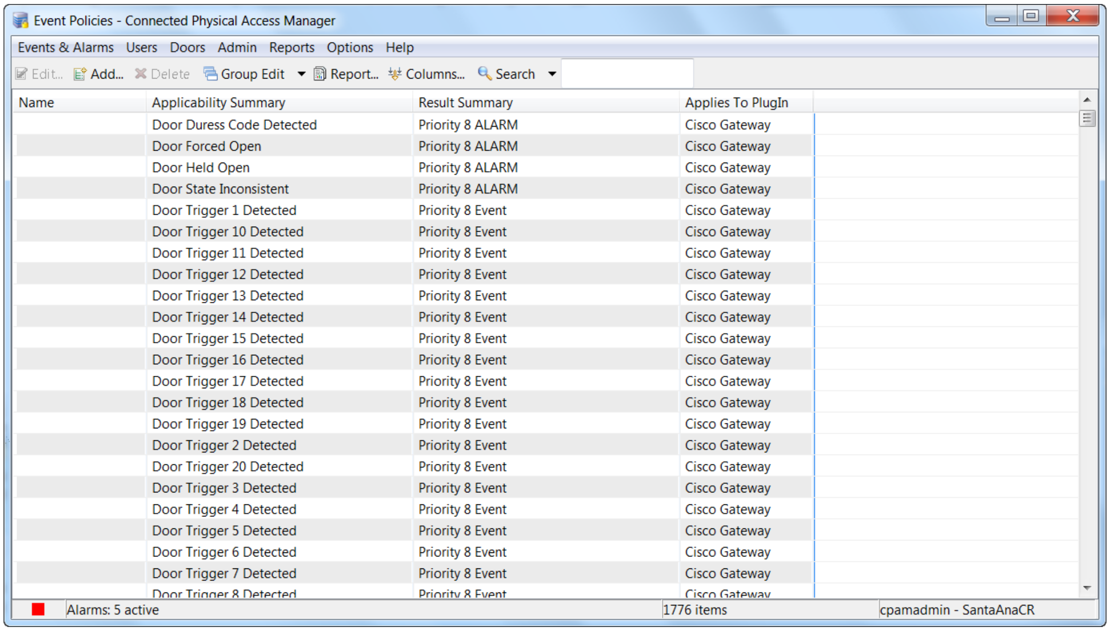
Note These points are applicable only when the profile enhancement feature is set in the System Configuration of the ICPAM. Otherwise the ICPAM appliance retains its behavior as in the previous version(1.3).

To modify event policies, do the following:

Step 1 Select **Event Policy Manager** from the **Events & Alarms** menu, in the **Configuration** submenu.

Step 2 The main window (Figure 12-19) shows all event policies defined within the system.

Figure 12-19 Event Policy Manager Module Main Window



Name	Applicability Summary	Result Summary	Applies To PlugIn
	Door Duress Code Detected	Priority 8 ALARM	Cisco Gateway
	Door Forced Open	Priority 8 ALARM	Cisco Gateway
	Door Held Open	Priority 8 ALARM	Cisco Gateway
	Door State Inconsistent	Priority 8 ALARM	Cisco Gateway
	Door Trigger 1 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 10 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 11 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 12 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 13 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 14 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 15 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 16 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 17 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 18 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 19 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 2 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 20 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 3 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 4 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 5 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 6 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 7 Detected	Priority 8 Event	Cisco Gateway
	Door Trigger 8 Detected	Priority 8 Event	Cisco Gateway

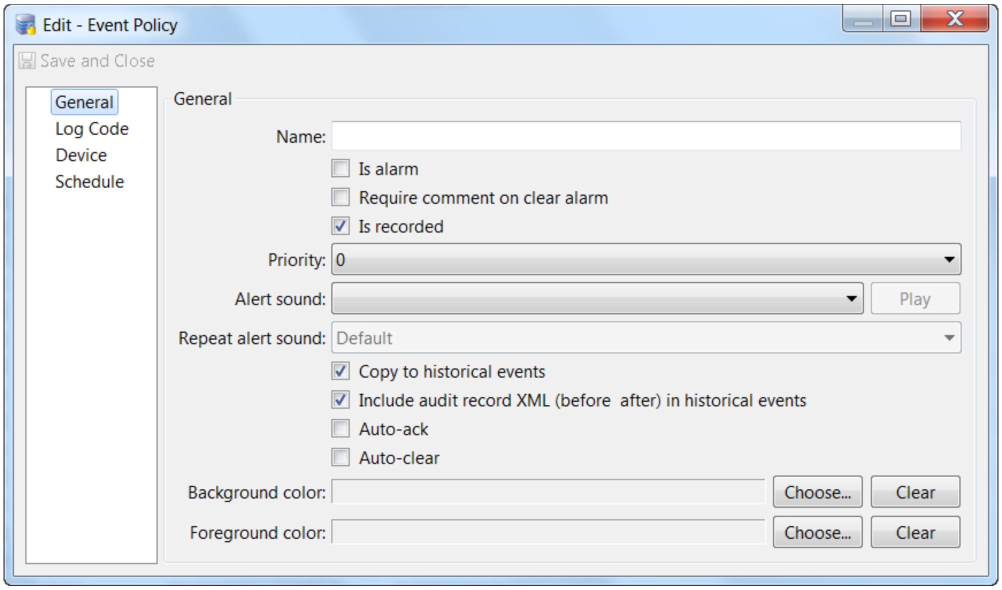
🟥 Alarms: 5 active | 1776 items | cpamadmin - SantaAnaCR

Step 3 Modify the events, if necessary:

- Select an existing entry and click **Edit**. The detail window opens, as shown in Figure 12-20. You can also double-click the entry.
- Click **Add...** to open the detail window (Figure 12-20) and add a new event policy.
- Select an entry and click **Delete** to delete the selected event policy.

Each field is described in Table 12-8 on page 12-37

Figure 12-20 Event Policy Manager Detail Window



Edit - Event Policy

Save and Close

General
Log Code
Device
Schedule

General

Name:

□ Is alarm
□ Require comment on clear alarm
☑ Is recorded

Priority: 0

Alert sound: Play

Repeat alert sound: Default

☑ Copy to historical events
☑ Include audit record XML (before after) in historical events
□ Auto-ack
□ Auto-clear

Background color: Choose... Clear

Foreground color: Choose... Clear

Event Policy Properties

An event policy has the following properties:

Table 12-8 Event Policy Properties

Field	Description
Log Code	
Log Code	An abbreviated code uniquely identifying the event.
Log code description	The description associated with the log code.
Applies To	The type of event this log code applies to.
Log code category	The category associated with the log code.
Device	
Device	If specified, the policy only applies to the device. Click **Choose** to select the device. Click **Clear** to remove the device. If no device is specified, the event applies to all devices.
Device Group	If specified, the policy only applies to the device group (for example: `Door`, `Gateway`, or `Reader`). Click **Choose** to select the group. Click **Clear** to remove the group. If no device group is specified, the event applies to all device groups. See also Configuring Device Groups, page 7-22.
Partition	If present, the policy only applies to this partition.
Classification	If present, the policy only applies to this classification.
Anti-passback area	If present, the policy only applies to this anti-passback area.
Anti-passback area (exit)	If present, the policy only applies to this anti-passback area exit.

Table 12-8 Event Policy Properties (continued)

Field	Description
Entrance	If present, the policy only applies to this entrance.
Zone	If present, the policy only applies to this zone.
Hierarchical location	If present, the policy only applies to the doors in this location.
Device type	If present, the policy only applies to devices of this type.
Time Schedule	
Any time	Generate events at all times and dates.
During time schedule	Generate events only during the specified **Time schedule**.
Not during time schedule	Do not generate events during the specified **Time schedule**. Generate events at all times outside the specified **Time schedule**.
Time schedule	Specifies the time schedule used for event policies. See Configuring Time Schedules, page 12-39 for more information.
Other	
Is Alarm	Specifies if events with this log code will be recorded as an alarm. Alarms are shown in the **Alarms** module.
Is Recorded	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 Identiv technical support.
Priority	A priority used for sorting events and alarms. Positive priorities are above normal priority, while negative priorities are below normal priority. Zero is normal.
Alert Sound	The sound to be played, if **Is Alarm** is checked. Available alert sounds are managed in Configuring Alert Sounds, page 12-42. Click **Play** to preview the alarm sound.
Background color	The color of the event entry. Click **Choose** to select a color. Click **Clear** to restore the default white background.
Foreground color	The color of the event text. Click **Choose** to select a color. Click **Clear** to restore the default black text.

Automatically Open the Alarm Window

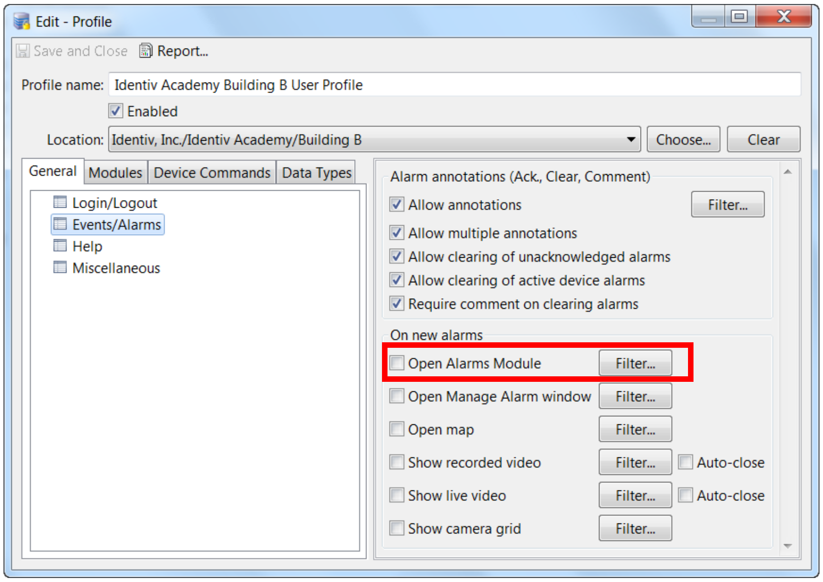
To automatically open the alarm window when an alarm occurs, do the following:

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 submenu **Events/Alarms** (Figure 12-21).

Figure 12-21 Profile: General Tab



Edit - Profile

Save and Close | Report...

Profile name: Identiv Academy Building B User Profile

☑ Enabled

Location: Identiv, Inc./Identiv Academy/Building B

General | Modules | Device Commands | Data Types

- Login/Logout
- Events/Alarms
- Help
- Miscellaneous

Alarm annotations (Ack, Clear, Comment)

☑ Allow annotations

☑ Allow multiple annotations

☑ Allow clearing of unacknowledged alarms

☑ Allow clearing of active device alarms

☑ Require comment on clearing alarms

On new alarms

□ Open Alarms Module

□ Open Manage Alarm window

□ Open map

□ Show recorded video □ Auto-close

□ Show live video □ Auto-close

□ Show camera grid

Step 4 Select the check-box for **Open Alarms Module**.

Step 5 Click **Save and Close**.

Tip Be sure that the user has access to the Alarms module. Click the **Modules** tab, select **Alarms** from the module list, and select the check box for **Allow access to module**. For more information, see Defining User Profiles for Desktop Application Access, page 4-1.

Configuring Time Schedules

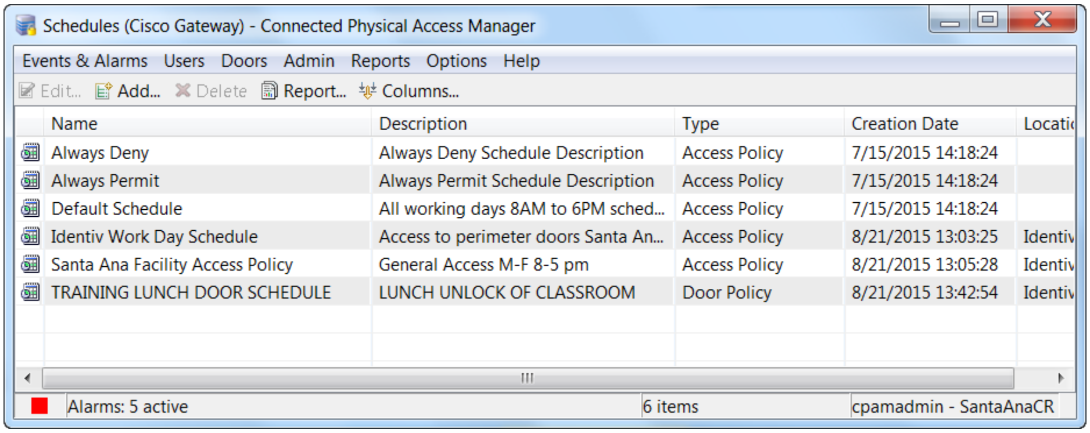
Time schedules define when events and automated rules will run. See Configuring Events and Alarms, page 12-34 and Configuring Global I/O Automated Rules, page 13-16 for more information.

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 12-22.

Figure 12-22 Schedules: Main Window


Schedules (Cisco Gateway) - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Delete Report... Columns...

Name	Description	Type	Creation Date	Locati
Always Deny	Always Deny Schedule Description	Access Policy	7/15/2015 14:18:24	
Always Permit	Always Permit Schedule Description	Access Policy	7/15/2015 14:18:24	
Default Schedule	All working days 8AM to 6PM sched...	Access Policy	7/15/2015 14:18:24	
Identiv Work Day Schedule	Access to perimeter doors Santa An...	Access Policy	8/21/2015 13:03:25	Identiv
Santa Ana Facility Access Policy	General Access M-F 8-5 pm	Access Policy	8/21/2015 13:05:28	Identiv
TRAINING LUNCH DOOR SCHEDULE	LUNCH UNLOCK OF CLASSROOM	Door Policy	8/21/2015 13:42:54	Identiv

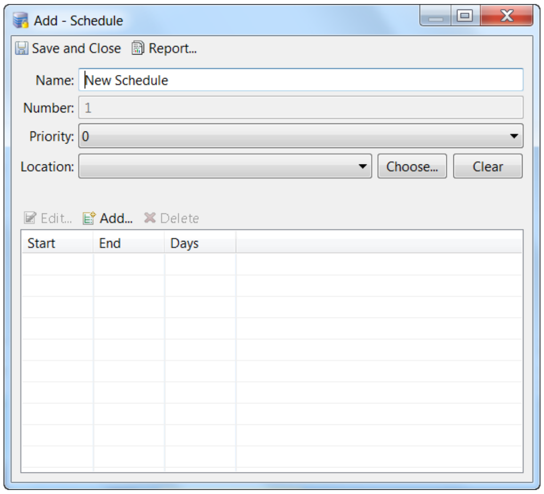
🟥 Alarms: 5 active 6 items cpamadmin - SantaAnaCR

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 12-23.

Figure 12-23 Schedule: Detail Window



Name: New Schedule
Number: 1
Priority: 0
Location:

Start	End	Days

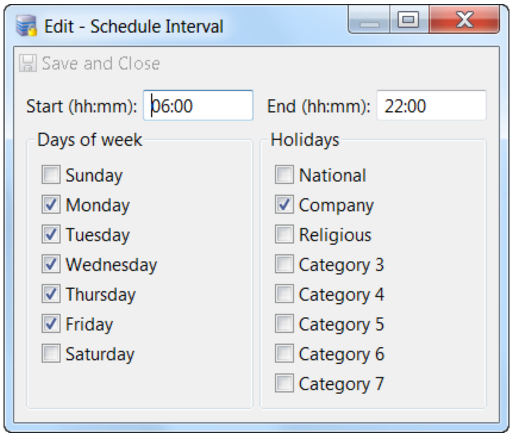
Step 4 Select a **Priority**.

Step 5 Define the schedule times:

a. Click **Add**, or select an existing entry and click **Edit** or **Delete**.

b. For Add or Edit only, specify the time interval for the schedule, as shown in Figure 12-23.

Figure 12-24 Time Schedule Interval



Start (hh:mm): 06:00 End (hh:mm): 22:00

Days of week

- □ Sunday
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- □ Saturday

Holidays

- □ National
- ☑ Company
- □ Religious
- □ Category 3
- □ Category 4
- □ Category 5
- □ Category 6
- □ Category 7

c. Enter the **Start** and **End** time in hour and minute format (`hh:mm`)

d. Select the **Days of Week** for the schedule.

e. Select additional **Holidays** for the schedule.

f. Click **Save and Close**.

g. Repeat step a to step f Define additional time intervals, if necessary.

Step 6 Click **Save and Close** to save the changes in the detail window (Figure 12-23).

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 12-34.

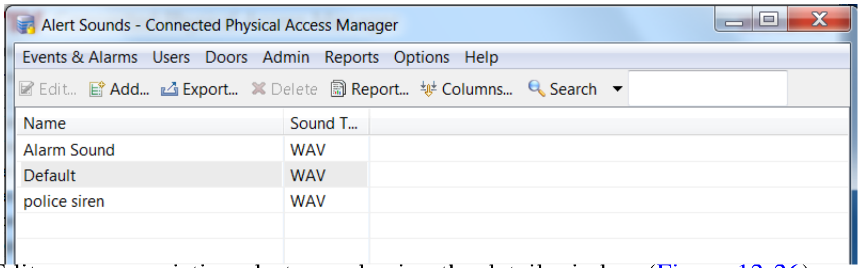
To add or modify alert sounds, do the following:

Step 1 Select **Alert Sounds** module from the **Events & Alarms** menu, in the **Configuration** submenu.

Step 2 The main window (Figure 12-25) 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.

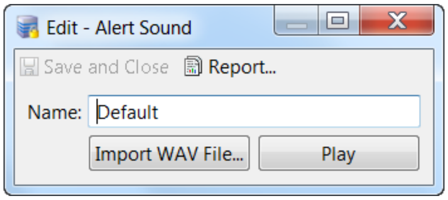
Figure 12-25 Alert Sound Module Main Window



Name	Sound T...
Alarm Sound	WAV
Default	WAV
police siren	WAV

Step 3 Edit a new or existing alert sound using the detail window (Figure 12-26):

Figure 12-26 Alert Sounds Module Detail Window



Name: Default

a. Click **Import WAV File** and select a sound file from a local drive. Click **Play WAV File...** to preview the alert sound.

b. Enter a name for the alert sound.

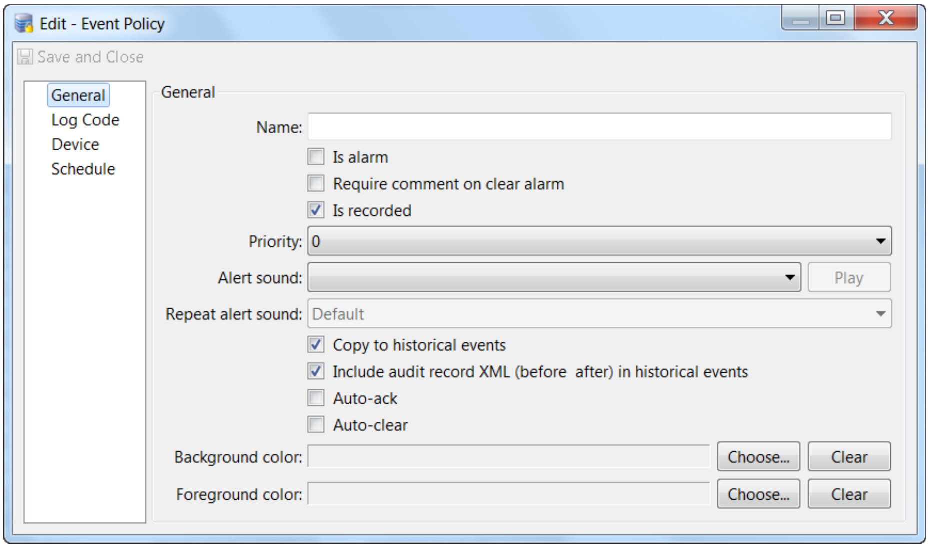
c. Click **Save & Close**.

Setting Event and Alarm Priorities

Priorities are used to sort or filter events and alarms. To define the priorities for an event or alarm log code, edit the Priority setting for the Log Code using the Event Policy Manager:

Step 1 Open the **Event Policy Manager** module in the **Events & Alarms**: **Configuration** menu. Edit an event policy by selecting it and clicking the **Edit...** button in the tool bar. This opens the **Event Policy** window (Figure 12-27).

Figure 12-27 Event Policy Window



Edit - Event Policy

Save and Close

General
Log Code
Device
Schedule

General

Name:

☐ Is alarm
☐ Require comment on clear alarm
☑ Is recorded

Priority: 0

Alert sound: Play

Repeat alert sound: Default

☑ Copy to historical events
☑ Include audit record XML (before after) in historical events
☐ Auto-ack
☐ Auto-clear

Background color: Choose... Clear

Foreground color: Choose... Clear

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 12-34.

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 12-28).

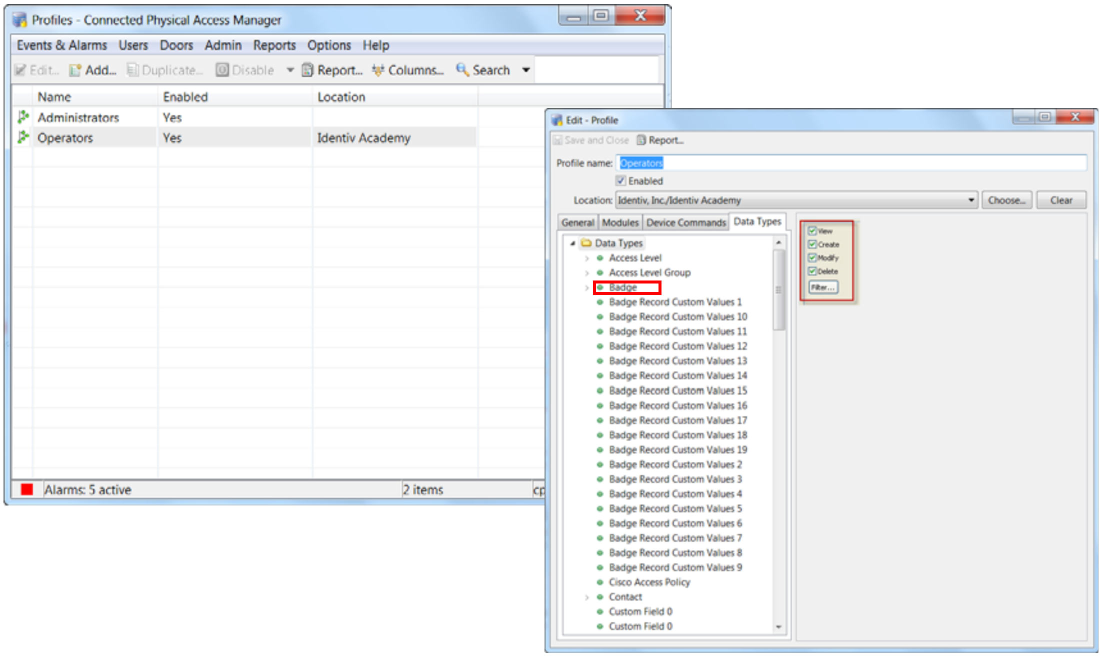
Step 3 Click the **Data Types** tab.

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 12-28 Selecting Editable Fields in the Profiles Module


Profiles - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Duplicate... Disable Report... Columns... Search
Edit - Profile
Save and Close Report...
Choose... Clear
General Modules Device Commands Data Types

Name	Enabled	Location
Administrators	Yes	
Operators	Yes	Identiv Academy

Alarms: 5 active 2 items

Profile name: Operators

☑ Enabled

Location: Identiv, Inc./Identiv Academy

- Data Types
  - Access Level
  - Access Level Group
  - Badge
  - Badge Record Custom Values 1
  - Badge Record Custom Values 10
  - Badge Record Custom Values 11
  - Badge Record Custom Values 12
  - Badge Record Custom Values 13
  - Badge Record Custom Values 14
  - Badge Record Custom Values 15
  - Badge Record Custom Values 16
  - Badge Record Custom Values 17
  - Badge Record Custom Values 18
  - Badge Record Custom Values 19
  - Badge Record Custom Values 2
  - Badge Record Custom Values 3
  - Badge Record Custom Values 4
  - Badge Record Custom Values 5
  - Badge Record Custom Values 6
  - Badge Record Custom Values 7
  - Badge Record Custom Values 8
  - Badge Record Custom Values 9
  - Cisco Access Policy
  - Contact
  - Custom Field 0
  - Custom Field 0

☑ View
☑ Create
☑ Modify
☑ Delete
Filter...

Using Graphic Maps

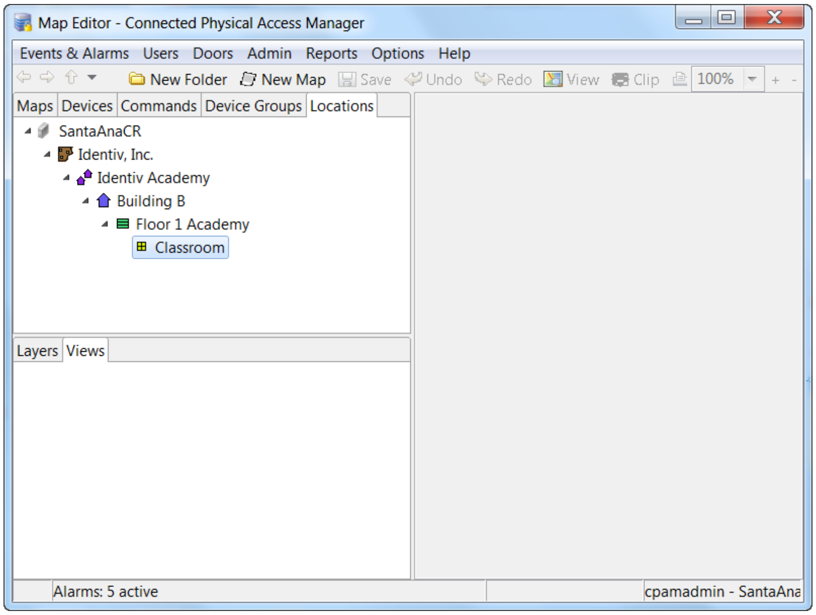
Graphic maps provide a visual representation of the devices available in a location. Icons representing the devices provide real-time status and alarms information, and allow the user to trigger actions such as viewing live video or denying access to a door. Automated rules can also be invoked, and icons representing a location provide status and alarm summary for all the devices assigned to that location.

Graphic Maps in ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), 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 12-29.

Figure 12-29 Location-specific Graphic



- 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 ICPAM's System Configuration; otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

The followings sections describes the map viewer, and the used to create the maps:

- Maps Viewer
- Map Editor

Map Viewer

Select **Maps** from the **Monitoring** submenu under the Events & Alarms menu.

Figure 12-30 Selecting Graphic Maps Viewer in Events & Alarms menu

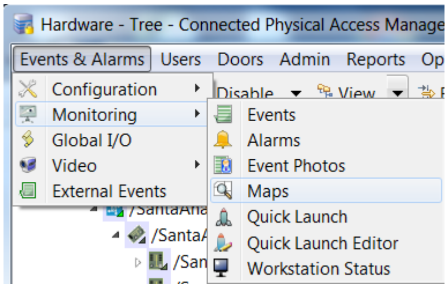
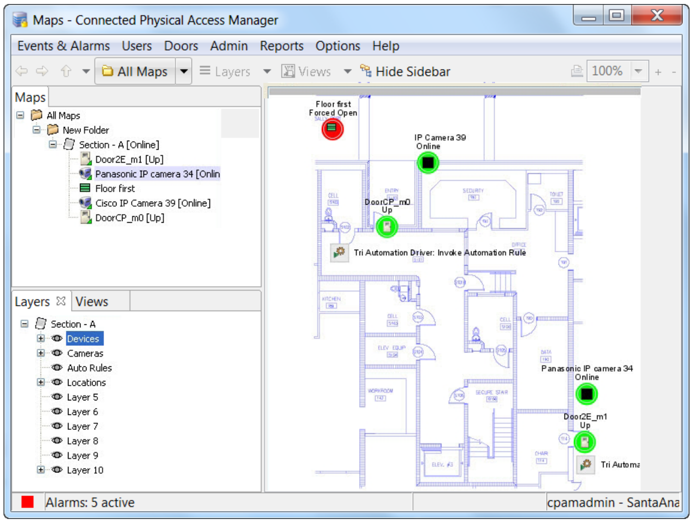


Figure 12-31 shows a sample map. In the top left frame, click + and - to expand and collapse the map folders and view associated devices. Right-click a device to view the actions and commands available for that device.

Figure 12-31 Maps Viewers Main Window



Icon Colors and Status

On the map, icons representing devices, automated rules, and locations provide status information using two colors: the inside fill color and the outside ring color.

Inside Fill Color

The inside color represents the device state.

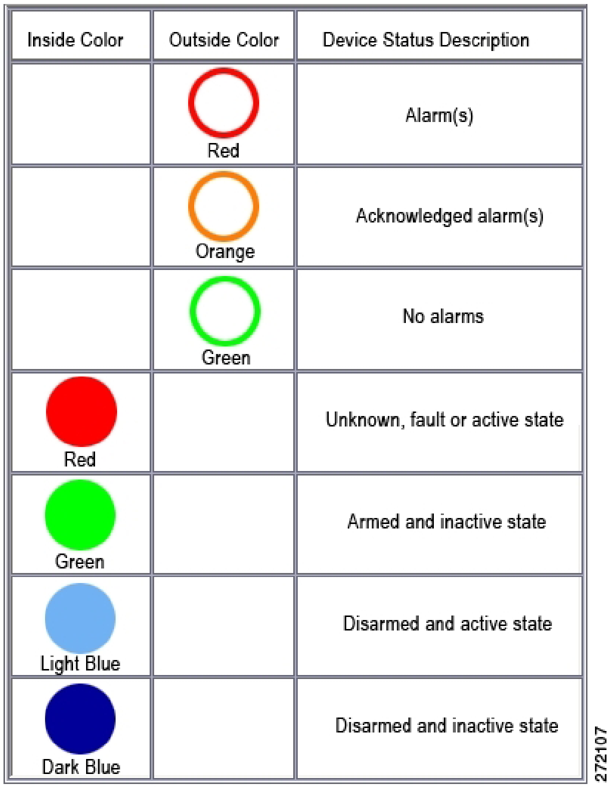
- *Light Green:* Represents armed, secure, online states.
- *Red:* Represents unknown, active, offline states.
- *Dark Blue:* Represents disarmed, inactive states.
- *Light Blue:* Represents disarmed, active.

Outer Ring Color

The outer ring color represents the alarm state.

- *Green:* Represents a normally operating device free of any alarms.
- *Orange:* Represents a device in an acknowledged alarm or alarms state.
- *Red:* Represents a device in an alarm state.

Figure 12-32 Icon Colors and Status



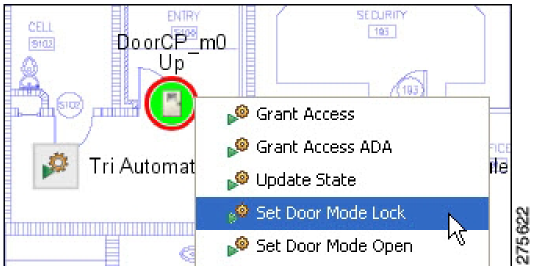
Inside Color	Outside Color	Device Status Description
	○ Red	Alarm(s)
	○ Orange	Acknowledged alarm(s)
	○ Green	No alarms
● Red		Unknown, fault or active state
● Green		Armed and inactive state
● Light Blue		Disarmed and active state
● Dark Blue		Disarmed and inactive state

Device Commands

Right-click an icon to view the available commands for that device. For example, you can view live video for a camera, or deny access for a door, depending on your access privileges.

Tip To trigger an automated rule, click the icon.

Figure 12-33 Viewing Available Commands



Layers and Views

Layers

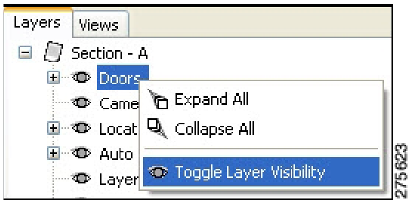
Layers allow you to hide or display categories of icons, depending on the map configuration.

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.

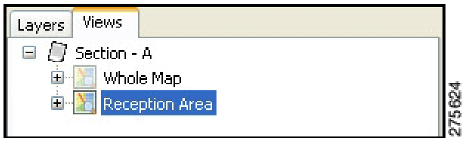
Figure 12-34 Layers



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.

Figure 12-35 Views



Toolbar and Navigation Controls

Use the following menu controls to select maps and adjust the map display.

Figure 12-36 Toolbar and Navigation Controls

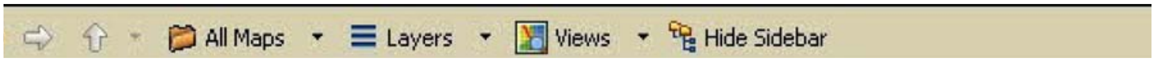


Table 12-9 Toolbar and Navigation Controls

Control	Description
Back Arrow	Navigates backwards in the viewed maps history.
Forward Arrow	Navigates forward in the viewed maps history.
Up Arrow	Navigates to maps linked to the displayed map.
All Maps	Opens a menu containing all maps for easy navigation regardless of whether the sidebar is shown.
Layers	Displays all layers in the open map, and allows you to show and hide layers, regardless of whether the sidebar is shown.
Views	Displays a selected view, regardless of whether the sidebar is shown.
Hide/Show Sidebar	Hides or shows the sidebar in the Layers and Views tabs in the sidebar.
Print	Prints the currently displayed map.
Zoom	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 click **Reset View**.
Zoom Marquee	To zoom into a specific map area; hold down the Control button, click and drag the dotted rectangle on the map. Release the mouse button and the view zooms to fit the rectangle. To scroll the screen, hold down the Shift button, click the left mouse button while dragging to a desired location.

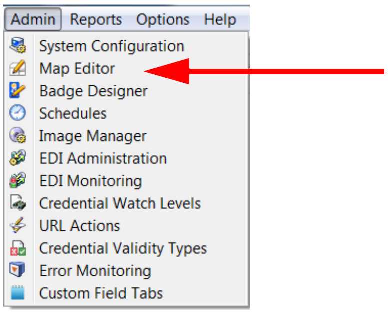
Map Editor

Use the **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 **Map Viewer**.

Caution Do not use the **Maps Editor** while other client workstations have the **Map Viewer or Maps Editor** open. Use of the **Graphic Map Editor** while any other client workstations have the **Graphic Maps Viewer or Graphic Map Editor** opened may result in system errors.

To create or modify graphic maps, do the following:

Step 1 Select **Map Editor** from the **Admin** menu.



Step 2 (Optional) Add a folder for map organization:

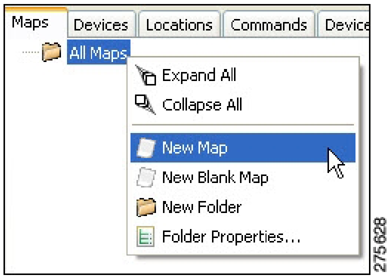
a. Click **New Folder**.

b. To rename the folder, right click the folder and select **Folder Properties** from the command menu.

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.

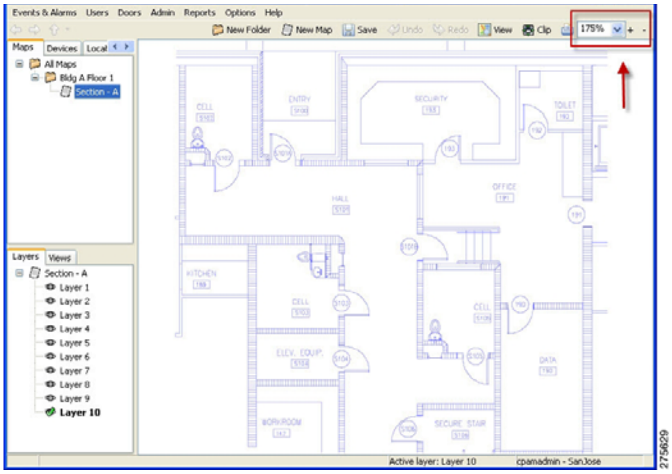


Tip You can also select options to create folders and maps by right-clicking a folder.

Step 4 (Optional) Use the clip and zoom controls to adjust the image:

- **Clip**: use the **Clip** button to crop an image. To clip an image, click the **Clip** button, click and drag a rectangle on the image, and then click **Clip** again to crop the image.
- **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.

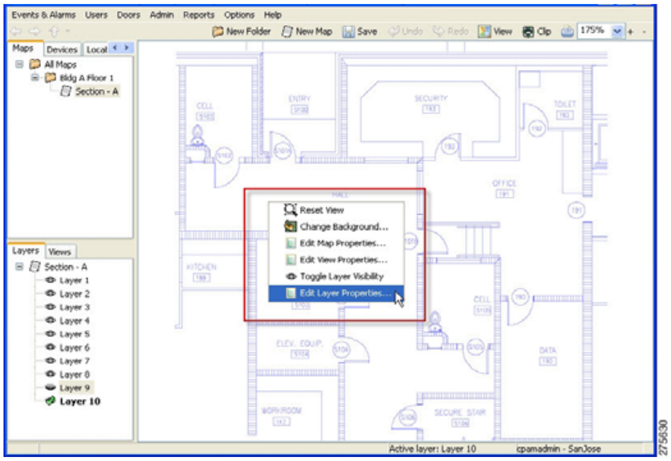
  To cancel the zoom and reset the view, select **Reset** from the drop-down menu, or right-click the image and click **Reset View**.
- **Zoom Marquee**: to zoom an image using the zoom marquee feature, hold down the Control button, click and drag a rectangle on the image. Release the mouse button and the image will zoom to fit the rectangle.



Tip To move an image, hold down the Shift button, click the image and drag to a desired location. Navigate between modifications by using the **Undo** and **Redo** buttons.

Step 5 (Optional) Right-click the image to access the following functions:

- **Reset View**: cancel a zoom view and return to 100%.
- **Change Background**: selects a new background image for the image.
- **Edit Properties**: defines the properties of the image, such as the icon scale.
- **Edit View Properties**: defines layout properties.
- **Toggle Layer Visibilit**y: turns layer visibility on or off.
- **Edit Layer Properties**: edits the layer name.

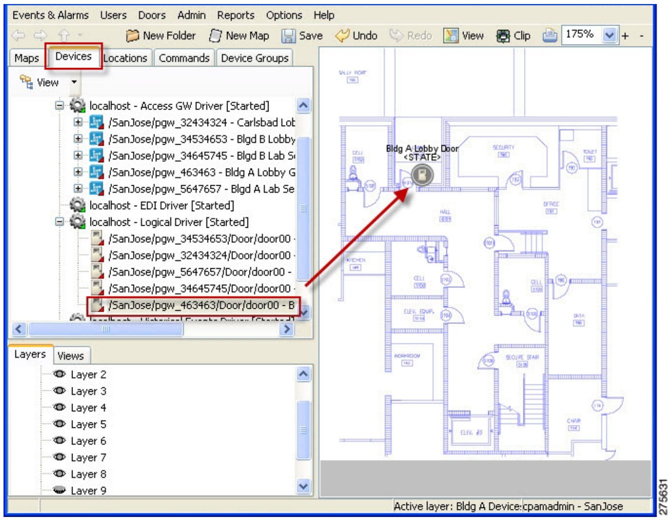


Step 6 Add a devices or doors to the appropriate location on the image.

The device will report real-time status in the Graphic Maps Viewer.

a. Click the **Devices** tab to view the controllers, doors and drivers.

b. Drag a device to an appropriate place on the image.


Events & Alarms Users Doors Admin Reports Options Help
New Folder New Map Save Undo Redo View Clip 175%
Maps Devices Locations Commands Device Groups
View
localhost - Access GW Driver [Started]
/SanJose/pgw_32434324 - Carlsbad Lob
/SanJose/pgw_34534653 - Blgd B Lobby
/SanJose/pgw_34645745 - Blgd B Lab S
/SanJose/pgw_463463 - Bldg A Lobby G
/SanJose/pgw_5647657 - Blgd A Lab Se
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
/SanJose/pgw_34534653/Door/door00 -
/SanJose/pgw_32434324/Door/door00 -
/SanJose/pgw_5647657/Door/door00 -
/SanJose/pgw_34645745/Door/door00 -
/SanJose/pgw_463463/Door/door00 - B
Bldg A Lobby Door
<STATE>
Layers Views
Layer 2
Layer 3
Layer 4
Layer 5
Layer 6
Layer 7
Layer 8
Layer 9
Active layer: Bldg A Device
cpamadmin - SanJose
275631

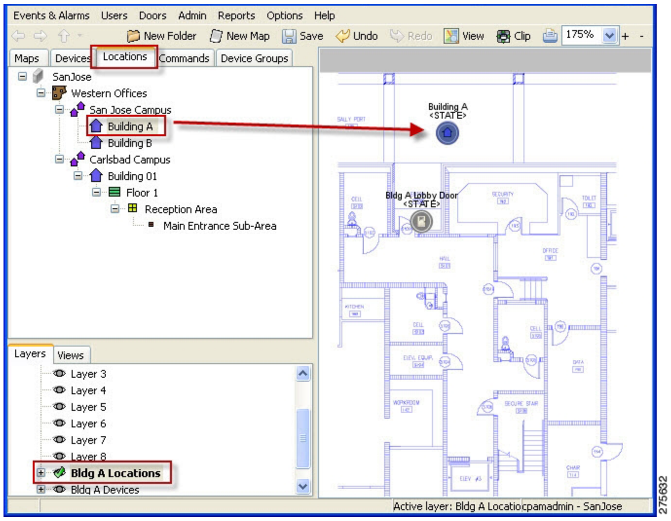
Tip To add Door Groups, click the **Device Groups** tab and drag the group to the image. See Configuring Device Groups, page 7-22 for more information.

Step 7 Add locations to the map.

The device will report real-time status in the Map Viewer.

a. Click the **Locations** tab.

b. Drag a location to an appropriate place on the map.



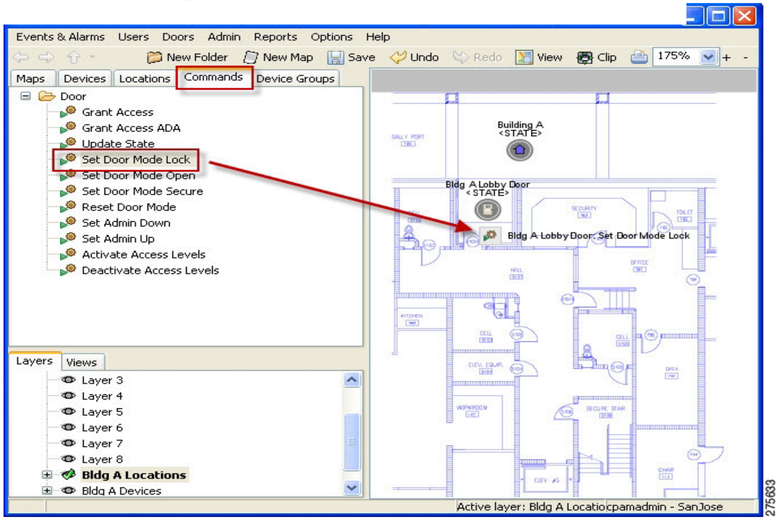
Tip Click a Layer icon in the bottom left window to organize the image elements into different layers. For example, click a layer and add the devices, then click another layer and add locations or commands. You can turn layers on or off by right-clicking the layer and selecting **Toggle Layer Visibility**. 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 Map 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.



Step 9 (Optional) To select a different device and command combination using the Device Command window, do the following:

a. Select the device(s)

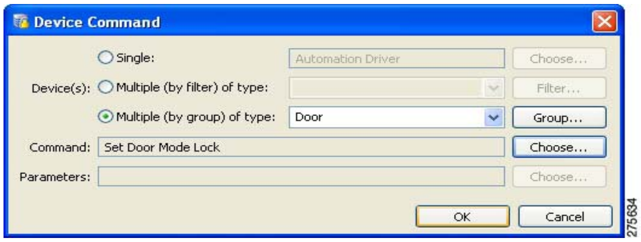
– **Single**: click **Choose** and select a single device or door from the Hardware - Tree view, as shown in the example to the right.

– **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

Device(s): ○ Single: Automation Driver

○ Multiple (by filter) of type:

● Multiple (by group) of type: Door

Command: Set Door Mode Lock

Parameters:

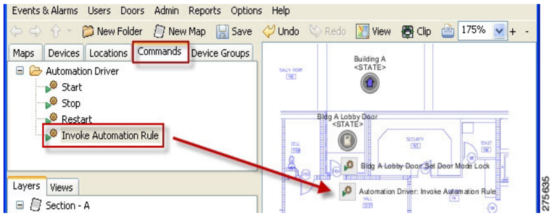
Note If **Choose** is shown in black, you must click the button to continue. Select a parameter from the list. If the message "*Are you sure you want to continue?*" appears, click **OK**. This message indicates that a parameter is not required.

d. Click **OK**.

Step 10 (Optional) Add automated rules to the image.

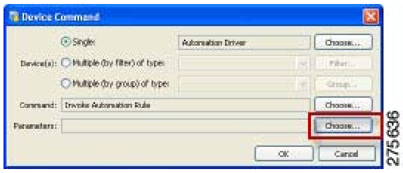
a. Click the **Devices** tab and select the **Automation Driver**.

b. Click the **Command** stab and drag the icon for **Invoke Automation Rule** to the image. The Device Command window appears.



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

Device(s): ● Single: Automation Driver [Choose...]
○ Multiple (by filter) of type: [Filter...]
○ Multiple (by group) of type: [Group...]

Command: Invoke Automation Rule [Choose...]

Parameters: [Choose...]

[OK] [Cancel]

d. To define rules, see Configuring Automated Tasks Using Global I/O, page 13-18.

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.

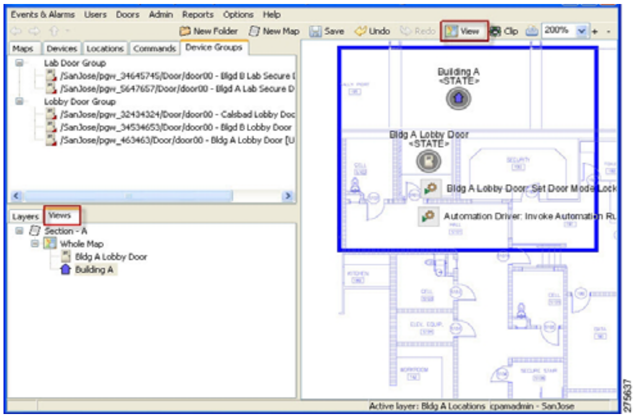
b. Click **View** in the top menu bar.

c. Use your mouse to click and drag a border within the map.

d. Release the mouse button to select the area. The 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 **Map Viewer**.

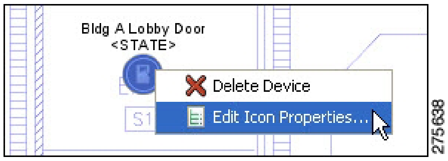
f. Click **OK** to save the changes and create the new view.


Events & Alarms
Users
Doors
Admin
Reports
Options
Help
New Folder
New Map
Save
Undo
Redo
View
Clip
200%
Maps
Devices
Locations
Commands
Device Groups
Lab Door Group
/SanJose/pgw_34645745/Door/door00 - Bldg B Lab Secure I
/SanJose/pgw_5647657/Door/door00 - Bldg A Lab Secure D
Lobby Door Group
/SanJose/pgw_32434324/Door/door00 - Calebad Lobby Doc
/SanJose/pgw_34534653/Door/door00 - Bldg B Lobby Door
/SanJose/pgw_463463/Door/door00 - Bldg A Lobby Door [U
Layers
Views
Section - A
Whole Map
Bldg A Lobby Door
Building A
Building A <STATE>
Bldg A Lobby Door <STATE>
Bldg A Lobby Door: Set Door Mode Lock
Automation Driver: Invoke Automation Ru
Active layer: Bldg A Locations cpamadmin - SanJose
275637

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 an 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.

Backing 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 12-57
- "Pruning and Archiving Old Events" section on page 12-57
- Creating Reports from Pruned Events, page 12-58

Including Events In System Backups

Events can either be included or excluded from system backups, as described in the "Backing up the ICPAM 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 ICPAM 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 ICPAM 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.

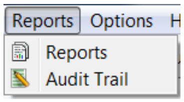
  Archived event files can be restored to the ICPAM database, if necessary, or used by other applications to view old events or run reports. See the "Creating Reports from Pruned Events" section on page 12-58.

See the "Archiving Historical Events" section on page 2-25 for more information.

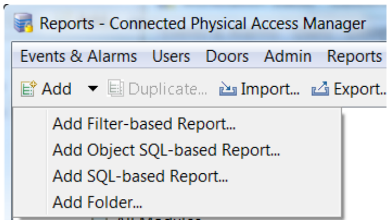
Creating Reports from Pruned Events

To run reports on historical events that were copied to the historical events database, create a filter-based report in the Report Manager.

Step 1 Select **Reports** from the Reports menu.

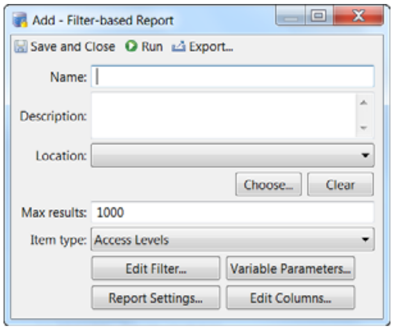


Step 2 Click **Add** and select **Add Filter-based Report Template**.



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 3-12.
- **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 3-10.
- **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.


Add - Filter-based Report

Name:

Description:

Location:

Max results: 1000

Item type: Access Levels

Step 4 Click **Save and Close**.

CHAPTER 13

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

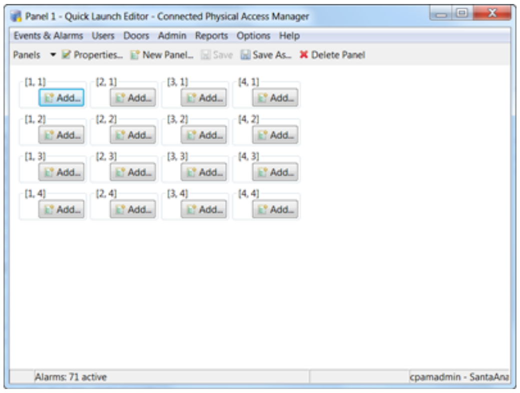
Quick Launch buttons provide one-click access to commonly used actions. For example, you can create buttons to unlock a door or open a ICPAM module. Complete the following instructions to create or modify buttons, and organize them into different panels (windows).

- Creating a Button, page 13-2
- Creating a Button That Runs An Automated Rule, page 13-6
- Creating Panels (Windows) of Related Buttons, page 13-7
- Restricting User Access to Button Panels, page 13-8

Creating a Button

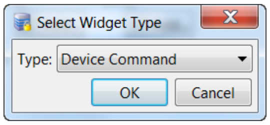
To create a button, perform the following procedure.

Step 1 Select **Quick Launch Editor** from the **Events & Alarms** menu in the **Monitoring** submenu. The Quick Launch Editor window opens.



Step 2 Press **Add** to select the row and column where the button will appear in the Quick Launch window.

The Select Widget type dialog appears.



Type: Device Command

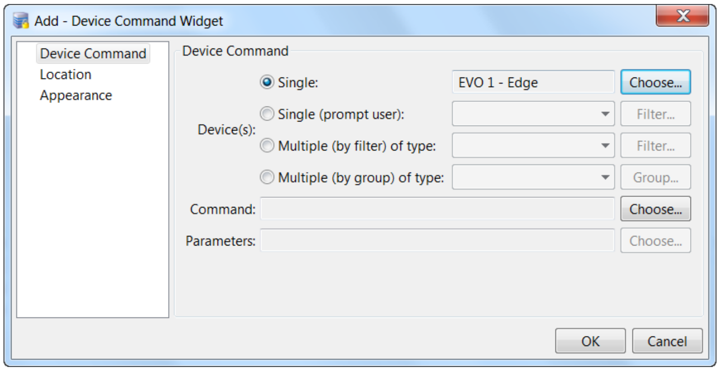
Step 3 Select a widget type to create a Quick Launch button then click **OK**.

The widget types include:

- **Device Command**: creates a button that executes a command for a door or device. For example, grant access to a door.
- **Open Module**: creates a button that opens a ICPAM module window.
- **Label**: Creates a text label used to organize Quick Launch buttons into rows and columns.

The Device Command Widget screen appears.

Step 4 At the Device Command Widget screen, select the required values.



Add - Device Command Widget

Device Command

Device(s):

● Single: EVO 1 - Edge

○ Single (prompt user):

○ Multiple (by filter) of type:

○ Multiple (by group) of type:

Command:

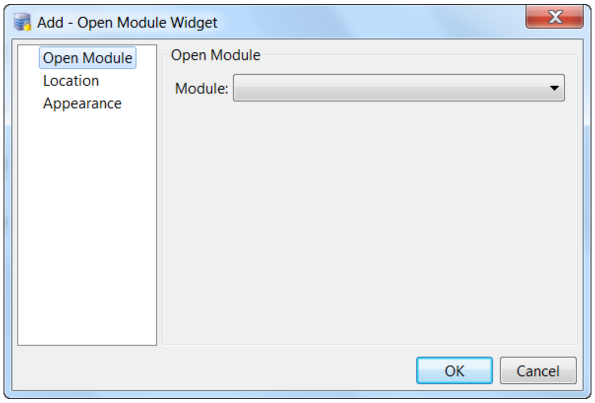
Parameters:

Step 5 If the widget type is **Open Module**, select a module:

a. Click the **Open Module** tab.

b. Select the ICPAM module that will open when the Quick Button is clicked.

c. Click **OK**.



Add - Open Module Widget

Open Module

Module:

d. Skip to Step 10b.

Step 6 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):

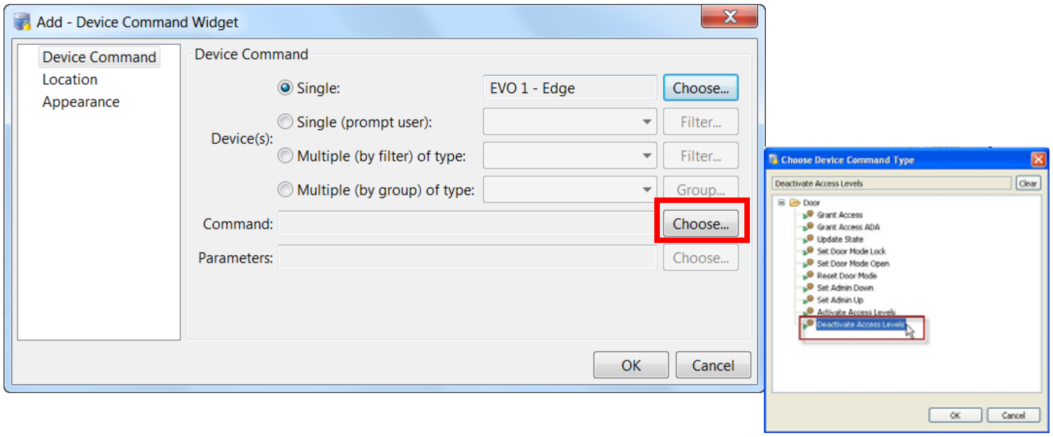
- **Single**: click **Choose** and select a single device or door from the Hardware - Tree view, as shown in the example to the right.
- **Multiple (by filter) of type**: select a device type from the drop-down menu. For example, select *deadbolt* to select all deadbolt devices in all doors. To refine 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 7-22.
  - **Monitor Point**
  - **Monitor Point Group**

Step 7 Select a command for the door or device(s):

a. Select **Choose**.

b. Select a command from the list. For example, **Deactivate Access Policies**.

c. Click **OK**.



Device Command

Device(s):
● Single: EVO 1 - Edge
○ Single (prompt user):
○ Multiple (by filter) of type:
○ Multiple (by group) of type:

Command:

Parameters:

Deactivate Access Levels

- Door
  - Grant Access
  - Grant Access ADA
  - Update State
  - Set Door Mode Lock
  - Set Door Mode Open
  - Reset Door Mode
  - Set Admin Down
  - Set Admin Up
  - Activate Access Levels
  - Deactivate Access Levels

Tip See Device Commands, page 7-39 and Door Modes and Commands, page 7-40 for command descriptions.

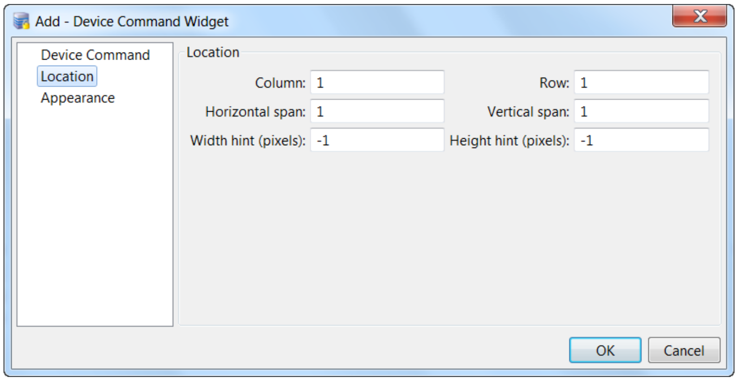
Step 8 Do the following:

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.

Step 9 Select the **Locations** tab and enter the row and column number.



Location

Column: 1 Row: 1
Horizontal span: 1 Vertical span: 1
Width hint (pixels): -1 Height hint (pixels): -1

Note If another button already exists in that location, the existing button location automatically shifts to the right.

Step 10 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 –.

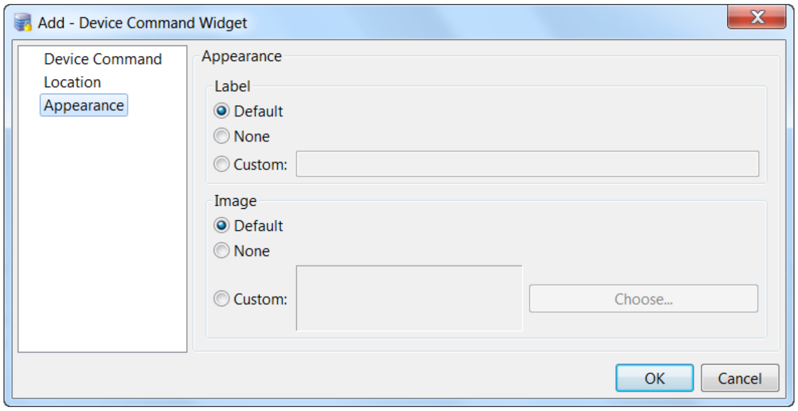
a. Click the **Appearance** tab.

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.


Add - Device Command Widget

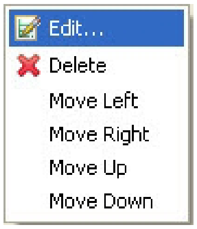
Appearance

Label
● Default
○ None
○ Custom:

Image
● Default
○ None
○ Custom:

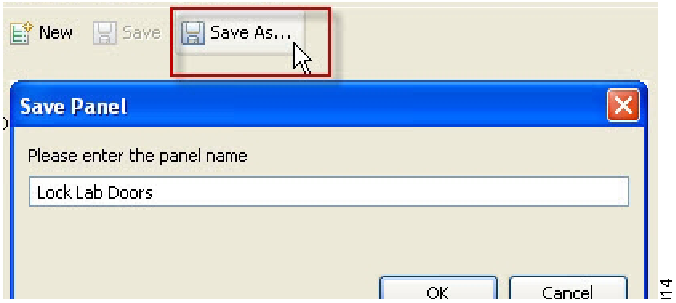
Step 11 (Optional) Repeat these steps to create additional quick launch buttons, or organize the buttons in the current panel (window).

- 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 12 (Optional) Create panels (windows) of related buttons.



Save Panel

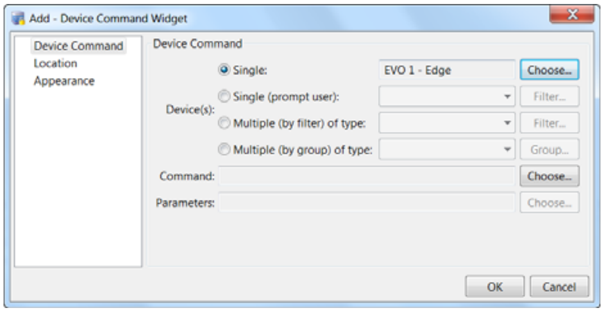
Please enter the panel name

Lock Lab Doors

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**.



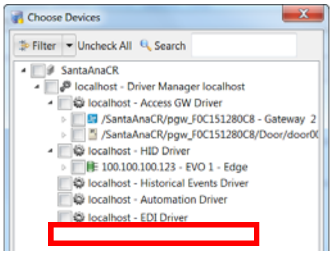
Add - Device Command Widget

Device Command

Device(s):
● Single: EVO 1 - Edge
○ Single (prompt user):
○ Multiple (by filter) of type:
○ Multiple (by group) of type:

Command:

Parameters:



Choose Devices

- □ SantaAnaCR
  - □ localhost - Driver Manager localhost
    - □ localhost - Access GW Driver
      - □ /SantaAnaCR/pgw_F0C151280C8 - Gateway 2
      - □ /SantaAnaCR/pgw_F0C151280C8/Door/door0(
    - □ localhost - HID Driver
      - □ 100.100.100.123 - EVO 1 - Edge
    - □ localhost - Historical Events Driver
    - □ localhost - Automation Driver
    - □ localhost - EDI Driver

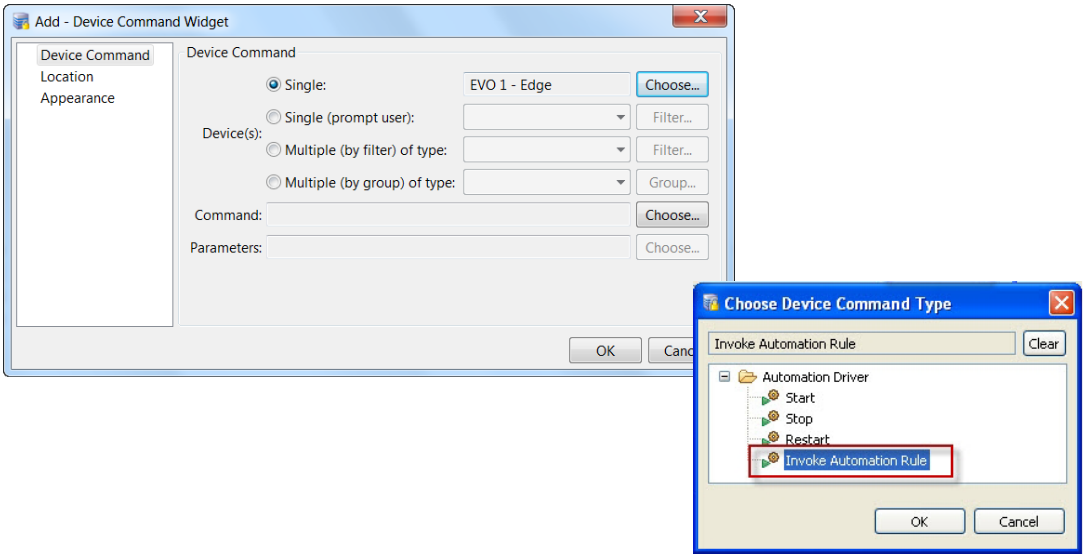
Step 2 Click **Choose** to select a single device.

Step 3 In the Hardware - Tree 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**.



● Single: EVO 1 - Edge

Invoke Automation Rule

Step 7 Click **OK** to save the changes and close the window.

See Configuring Global I/O Automated Rules, page 13-16 for more information.

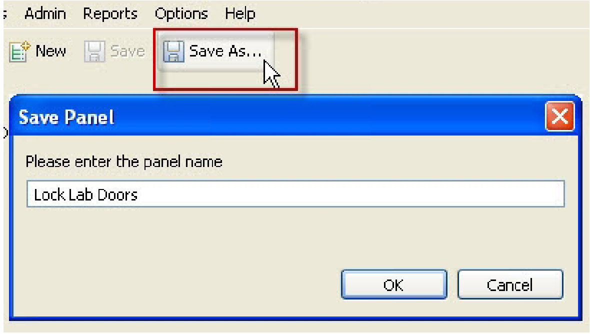
Creating Panels (Windows) of Related Buttons

Step 1 Create one or more Quick Launch buttons.

Step 2 Select **Save** or **Save As** to save the current Quick Launch window as a panel.

Step 3 Enter the panel name.

Step 4 Click **OK**.



Please enter the panel name

Lock Lab Doors

Tip To toggle between the panels, select **Panels** from the menu bar and select a panel.

Restricting User Access to Button Panels

Restrict user access to the button panels using the Profiles and Login modules, as described in the following instructions.

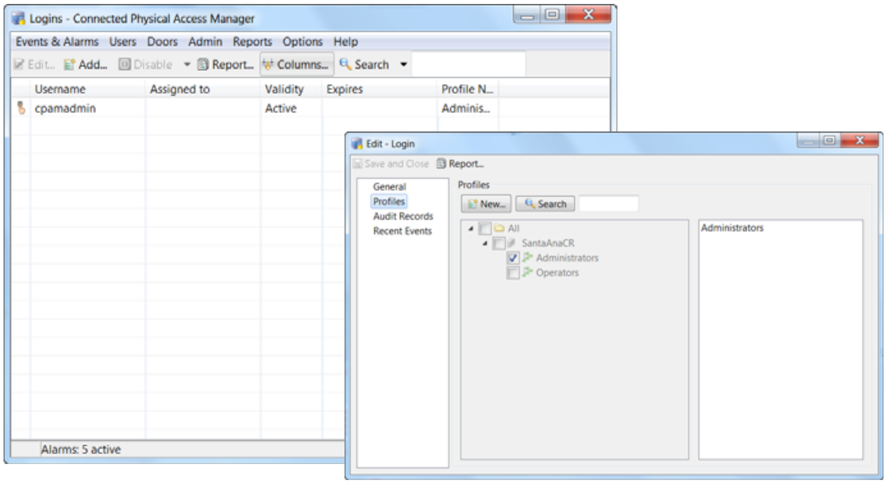
Step 1 Create or modify profiles to include the required Quick Launch access privileges. Profiles are sets of access privileges that are assigned to individual user logins.

- **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 4, "Configuring User Access for the ICPAM 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.
- **e.** Click **Save and Close**.


Logins - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Disable Report... Columns... Search
Alarms: 5 active
Edit - Login
Save and Close Report...
General
Profiles
Audit Records
Recent Events
Profiles
New... Search

Username	Assigned to	Validity	Expires	Profile N...
cpamadmin		Active		Adminis...

- □ All
  - □ SantaAnaCR
    - ☑ Administrators
    - □ Operators

Administrators

Using Quick Launch Buttons

To use a quick launch button to execute one or more actions:

Step 1 From the **Events & Alarms** menu, select **Monitoring** > **Quick Launch**.

The Quick Launch window appears with all of the currently defined Quick Launch buttons listed by panel. For more on defining these buttons, refer to Creating a Button, page 13-2.

Step 2 Double-click the widget you require and the action defined by that widget is triggered for the specified panel.

Configuring Edge Policies

Use **Edge Policies** to create event-based actions that are stored and executed on specific controllers. 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 controller, and are triggered immediately when an event occurs, even if network communication with the ICPAM server is delayed or lost.
- Global I/O rules may not execute immediately due to network delays, rules processing, communication between ICPAM and the controllers, 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 controller.

See Configuring Global I/O Automated Rules, page 13-16 instructions to create global automation rules.

Procedure

Complete the following instructions to create or modify edge policies:

Note This example assumes that the controllers, 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, “Adding New Doors” and Chapter 9, “Configuring Personnel and Badges”.

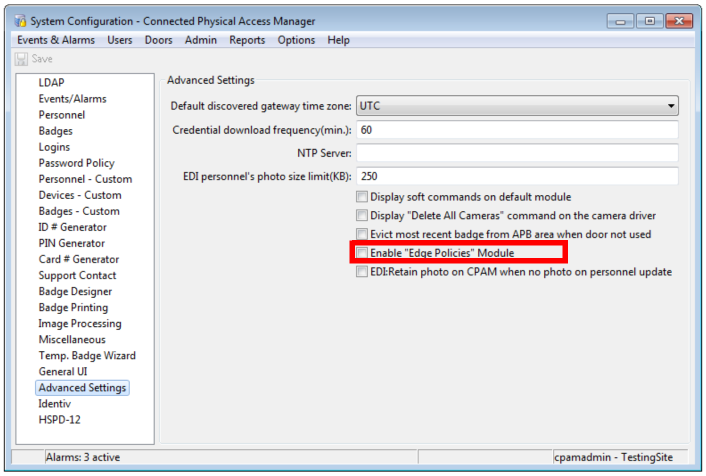
Step 1 Enable the Edge Policy menu.

a. Select **System Configuration** from the Admin menu.

b. Select the **Advanced Setting** tab.

c. Select the check box **Enable “Edge Policies” Module**.

d. Click **Save**.



Advanced Settings

Default discovered gateway time zone: UTC

Credential download frequency(min.): 60

NTP Server:

EDI personnel's photo size limit(KB): 250

□ Display soft commands on default module

□ Display "Delete All Cameras" command on the camera driver

□ Evict most recent badge from APB area when door not used

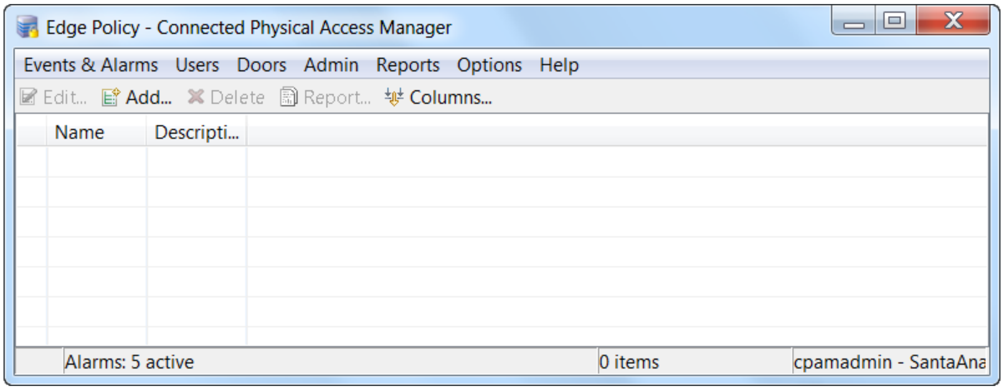
□ Enable "Edge Policies" Module

□ EDI:Retain photo on CPAM when no photo on personnel update

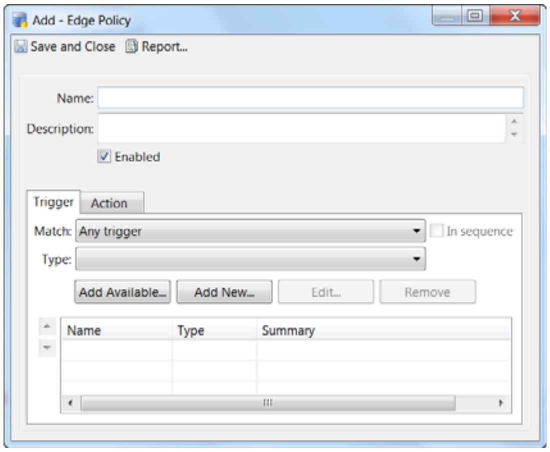
e. Log out and log back in to the ICPAM application to activate the changes (select Logout from the Options menu).

Step 2 Select **Doors** > **Edge Policies** > **Edge Policy**.

Step 3 Click **Add**, or select an existing rule and click **Edit**.



Step 4 Enter a name and description for the rule.



Name:

Description:

☑ Enabled

Match: Any trigger

□ In sequence

Type:

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 controller) for the trigger. When the specified event occurs on the specified device, the Edge Policy *action* is triggered.

Release 1.3 and later support event triggers.

a. Match – Select **Any trigger**.

b. Type – Select **Event**.

Step 6 Define the **Trigger**.

The *trigger* defines an event that occurs on a device. When this triggers 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.

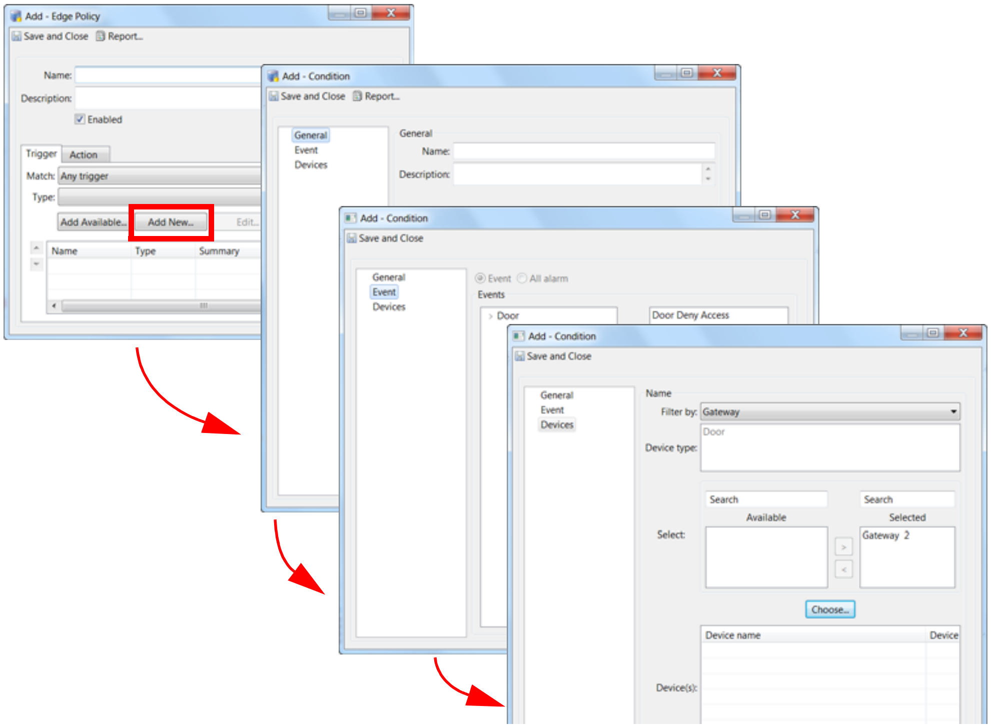
- Select an available event from the left column.
- Click the arrow to move the event to the right column.

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)—*lick Choose* and select an available device (such as a Door) and move it to the *Selected* field.

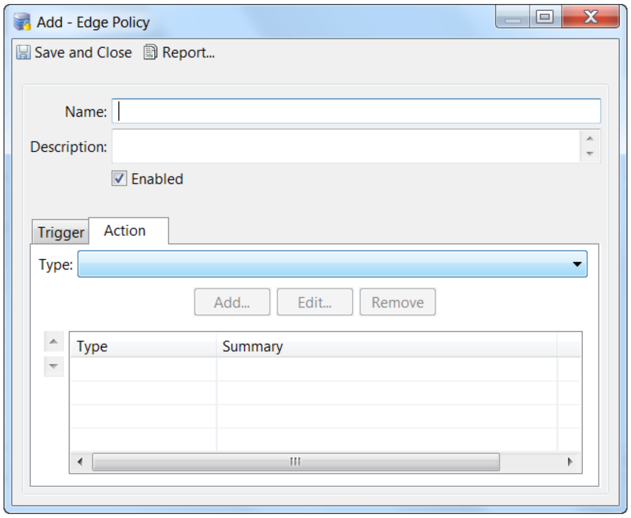
e. Verify that the selected device name appears in the Devices field.

f. Select **Save and Close**.



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.

Step 9 Select **Apply Configuration Changes** on the affected controller to activate the rule.

See Applying Configuration Changes, page 7-12 for more information.

Note Controllers 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.

Configuring Device I/O Rules

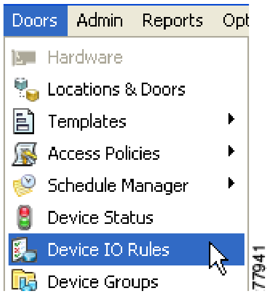
Use the **Device I/O Rules** module to create event based rules for a specific controller and the doors and devices configured on the controller. For example, when a door is forced open, a rule can activate a generic output device to sound an alarm. Since device rules are implemented for a single controller, the action is triggered immediately.

Device automation rules differ from global automation rules (global I/O) in the following ways:

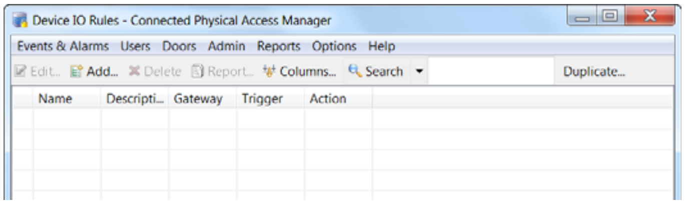
- Device rules affect a single controller. Global I/O rules can affect multiple controllers.
- Device rules trigger actions immediately since they are executed on the controller and not subject to system or network delays. Global I/O rules may not execute immediately due to network delays, rules processing, communication between ICPAM and the controllers, or other factors. See Configuring Global I/O Automated Rules, page 13-16 instructions to create global rules.

Complete the following instructions to create or modify device I/O rules:

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.

Step 3 Enter the rule settings:

- **Name**: enter the name of the rule.
- **Description**: enter a short description of the rule.
- **Gateway**: select the controller or gateway where the device is installed.

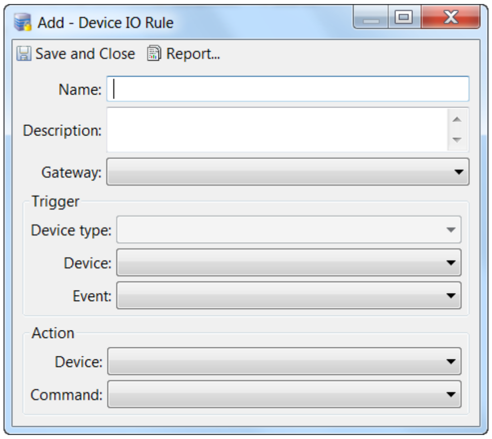
Trigger:

- **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 Commands, page 7-39.



Step 4 Click **Save and Close** to save the changes. The new or revised rule is displayed in the main window.

Step 5 Select **Apply Configuration Changes** on the affected controller to activate the rule.

See Applying Configuration Changes, page 7-12 for more information.

Note Controllers 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.

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 Maps Editor.

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.

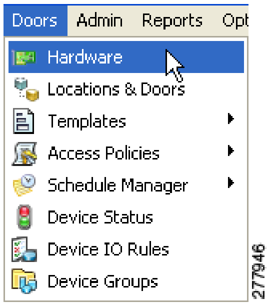
- Enabling the Automation Driver, page 13-16
- Configuring Automated Tasks Using Global I/O, page 13-18
- Example: Automated Weekly Report, page 13-25

Enabling the Automation Driver

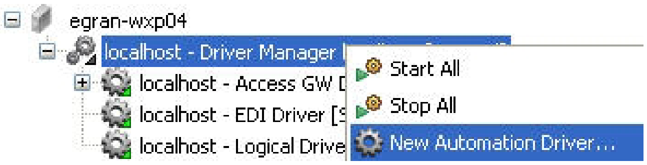
To enable automated tasks, the Automation Driver must be created and configured in the Hardware - Tree window. The driver is created once and remains active unless deactivated.

Tip The Automation Driver is a system component that executes automation policy actions. See Viewing Doors and Devices in the Hardware Tree View, page 5-4 for a description of the various system drivers.

Step 1 Select **Hardware - Tree** from the **Doors** menu.



Step 2 Right-click the **Driver Manager** and select **New Automation Driver...**.

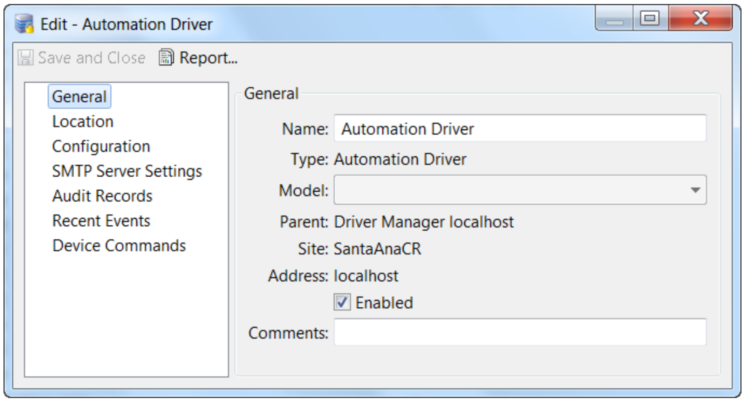

egran-wxp04
localhost - Driver Manager l
localhost - Access GW D
localhost - EDI Driver [S
localhost - Logical Drive
Start All
Stop All
New Automation Driver...

Step 3 Enter the driver settings:

a. Click the **General** tab and enter a **Name** for the **Automation Driver**.

b. If e-mail notification is needed, click the **SMTP Server Settings** tab and enter the SMTP server settings.

c. Click **Save and Close** to close the configuration window and create the Automation Driver.



General

Name: Automation Driver

Type: Automation Driver

Model:

Parent: Driver Manager localhost

Site: SantaAnaCR

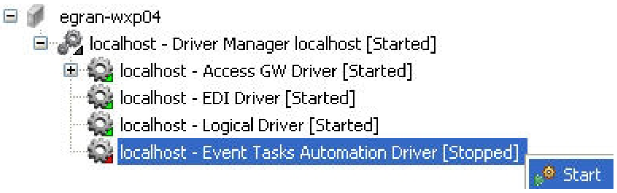
Address: localhost

☑ Enabled

Comments:

Step 4 Right-click the **Automation Driver** and select **Start**.

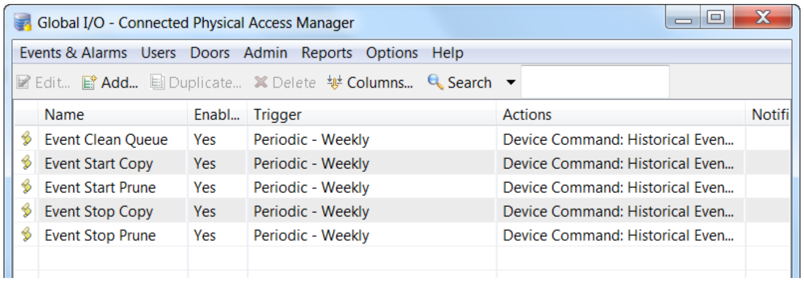
This enables the driver and activates any automated rules.


egran-wxp04
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - Event Tasks Automation Driver [Stopped]
Start

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.

Step 1 Select **Global I/O** from the **Events & Alarms** menu. The Automates Rules window lists the currently defined rules.


Global I/O - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Duplicate... Delete Columns... Search

Name	Enabl...	Trigger	Actions	Notifi
Event Clean Queue	Yes	Periodic - Weekly	Device Command: Historical Even...	
Event Start Copy	Yes	Periodic - Weekly	Device Command: Historical Even...	
Event Start Prune	Yes	Periodic - Weekly	Device Command: Historical Even...	
Event Stop Copy	Yes	Periodic - Weekly	Device Command: Historical Even...	
Event Stop Prune	Yes	Periodic - Weekly	Device Command: Historical Even...	

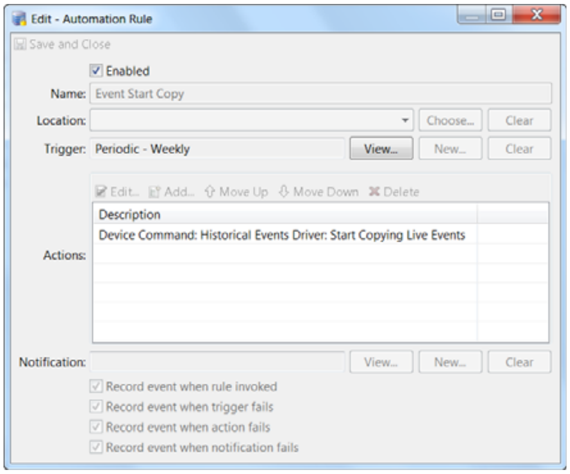
The main window includes the following columns.

- **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** check box.



☑ Enabled
Name: Event Start Copy
Location:
Trigger: Periodic - Weekly
Actions:

Description
Device Command: Historical Events Driver: Start Copying Live Events

Notification:
☑ Record event when rule invoked
☑ Record event when trigger fails
☑ Record event when action fails
☑ Record event when notification fails

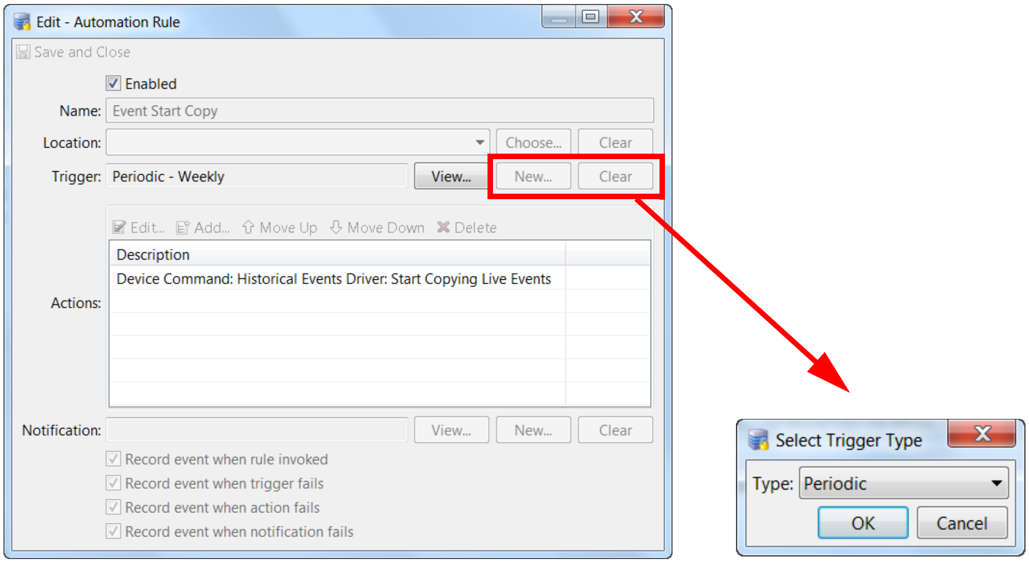
Step 4 Enter a **Trigger** type for the rule.

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 12-39 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



☑ Enabled

Name: Event Start Copy

Location:

Trigger: Periodic - Weekly

Actions:

Description
Device Command: Historical Events Driver: Start Copying Live Events

Notification:

☑ Record event when rule invoked

☑ Record event when trigger fails

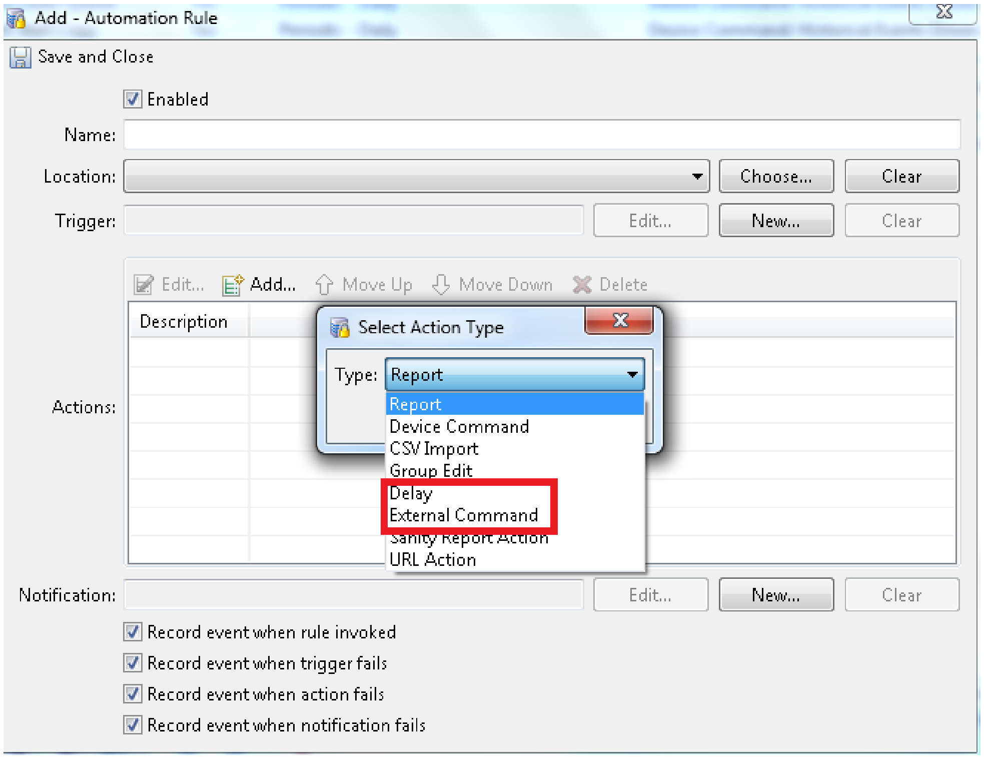
☑ Record event when action fails

☑ Record event when notification fails

Type: Periodic

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 a ICPAM server.
- **Group Edit**: Edits multiple personnel or badge records.
- Delay: Shows the time of delay between two actions performed in the Global I/O.
- **External Command**: An External command is used to run a exe file or application on server from Global I/O.
- **Sanity Report Action**: Provides a snapshot of the system status.
- **URL Action**: performs a pre-defined URL action.



☑ Enabled

☑ Record event when rule invoked

☑ Record event when trigger fails

☑ Record event when action fails

☑ Record event when notification fails

Tip See Understanding Automated Rule Actions, page 13-21 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 Step 3 in Enabling the Automation Driver, page 13-16.
- **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. ICPAM does not verify the Host server availability.
  - **Facility**: The log facility to use when recording the information to the Syslog.

Step 7 Select the event options. These events occur when the rule is successfully invoked, or when rule options fail.

Click the check boxes to activate or deactivate the options:

- **Record event when rule invoked:** Each time the rule is invoked, record an event.
- **Record event when trigger fails:** Each time the trigger fails, record an event.

- **Record event when action fails:** Each time the action fails, record an event
- **Record event when notification fails:** Each time the notification fails, record an event.

Step 8 Click **Save and Close**.

Understanding Automated Rule Actions

Automated rule actions define what occurs when the rule is triggered. Actions are defined when creating or editing a rule, as described in 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 ICPAM 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 13-18. 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:

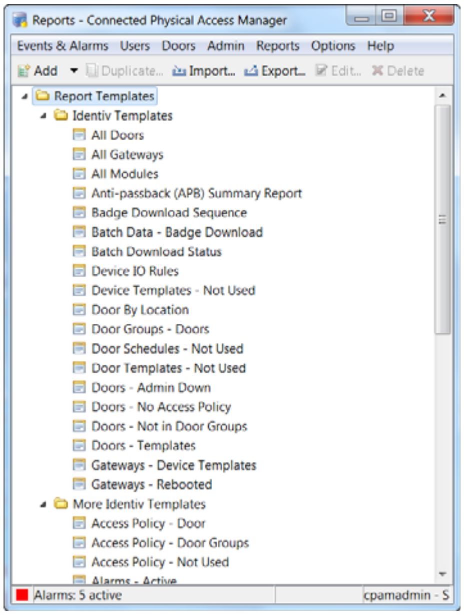
a. Select the Action type **Report**.

b. Click **Choose** to select a predefined report template. To create or modify reports, see Defining Reports (Report Manager), page 13-33.

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**.

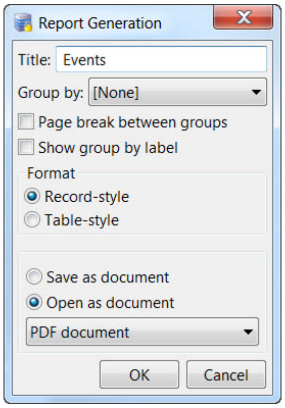


Reports - Connected Physical Access Manager

Events & Alarms Users Doors Admin Reports Options Help
Add Duplicate... Import... Export... Edit... Delete

- Report Templates
  - Identiv Templates
    - All Doors
    - All Gateways
    - All Modules
    - Anti-passback (APB) Summary Report
    - Badge Download Sequence
    - Batch Data - Badge Download
    - Batch Download Status
    - Device IO Rules
    - Device Templates - Not Used
    - Door By Location
    - Door Groups - Doors
    - Door Schedules - Not Used
    - Door Templates - Not Used
    - Doors - Admin Down
    - Doors - No Access Policy
    - Doors - Not in Door Groups
    - Doors - Templates
    - Gateways - Device Templates
    - Gateways - Rebooted
  - More Identiv Templates
    - Access Policy - Door
    - Access Policy - Door Groups
    - Access Policy - Not Used
    - Alarms - Active

Alarms: 5 active cpamadmin - S



Report Generation

Title: Events

Group by: [None]

☐ Page break between groups

☐ Show group by label

Format

● Record-style

○ Table-style

○ Save as document

● Open as document

PDF document

Device Command

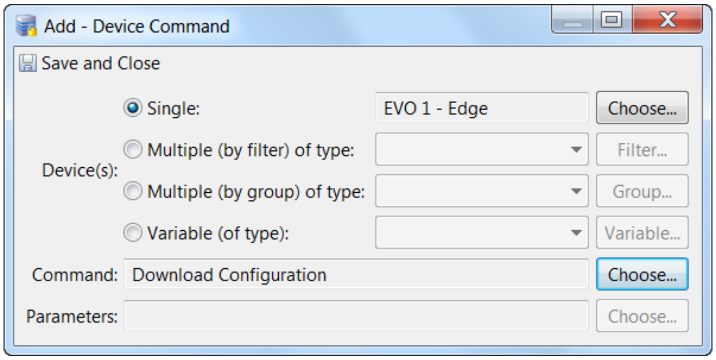
Executes a command on one or more devices:

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 - Tree 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 7-22.
- **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 the previous Step 3 is caused by a door, then the action is initiated.



Add - Device Command

Device(s):

● Single: EVO 1 - Edge

○ Multiple (by filter) of type:

○ Multiple (by group) of type:

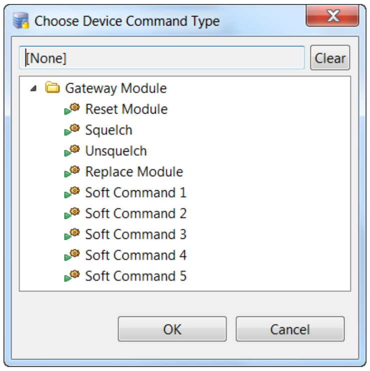
○ Variable (of type):

Command: Download Configuration

Parameters:

c. **Command**: Click **Choose** to select the Command for the device(s). See Device Commands, page 7-39 and Door Modes and Commands, page 7-40 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 ICPAM 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 ICPAM server** enter the file settings as:

- Directory Path: The directory path of the CSV file location in ICPAM 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 ICPAM 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 9-12.

Group Edit

Edits multiple personnel or badge records.

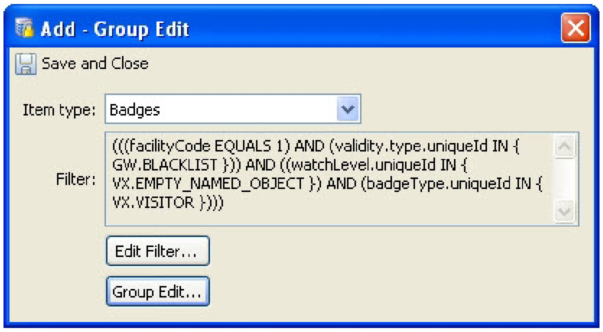
a. Select the Action type **Group Edit**.

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**.



Item type: Badges

Filter: (((facilityCode EQUALS 1) AND (validity.type.uniqueId IN { GW.BLACKLIST })) AND ((watchLevel.uniqueId IN { VX.EMPTY_NAMED_OBJECT }) AND (badgeType.uniqueId IN { VX.VISITOR })))

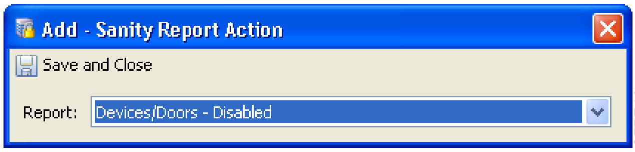
Sanity Report Action

System sanity reports provide information about potential system inconsistencies or issues in the access control system. See Generating a Gateway Driver System Sanity Report, page 5-16 for more information.

a. Select the Action type **Sanity Report Action**.

b. Select the Report type:
for example, **Devices/Doors - Disabled**.

c. Click **Save and Close**.



Report: Devices/Doors - Disabled

277746

URL Action

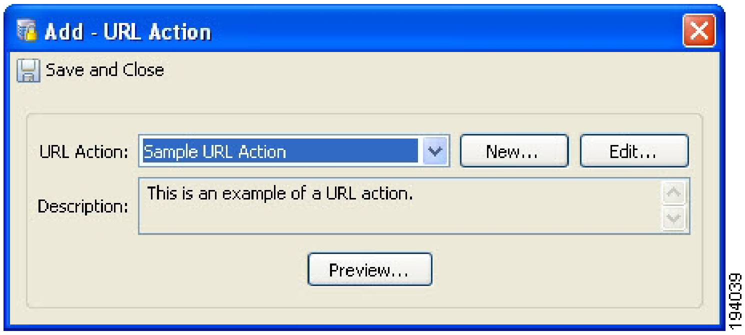
Performs a pre-defined URL action.

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**.



URL Action: Sample URL Action

Description: This is an example of a URL action.

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 - Tree module and selecting **Invoke Automation Rule**. You can also create a Quick Launch button to invoke the rule (see Creating 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.

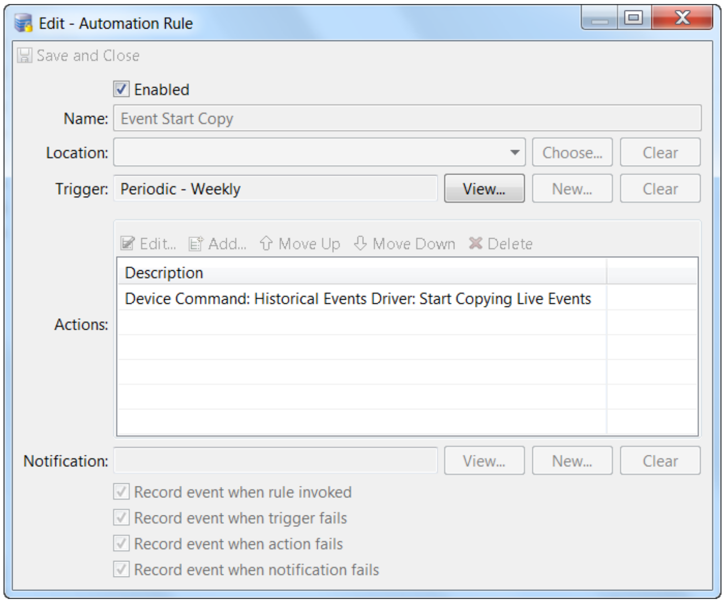
Step 1 Select **Global I/O** in the Events & Alarms menu.

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** check box is selected.



☑ Enabled
Name: Event Start Copy
Location:
Trigger: Periodic - Weekly
Actions:

Description
Device Command: Historical Events Driver: Start Copying Live Events

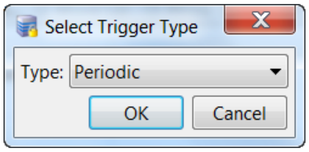
Notification:
☑ Record event when rule invoked
☑ Record event when trigger fails
☑ Record event when action fails
☑ Record event when notification fails

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**.



Type: Periodic

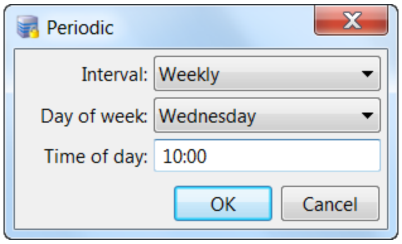
Step 4 Select the days and times for the periodic Trigger:

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**.

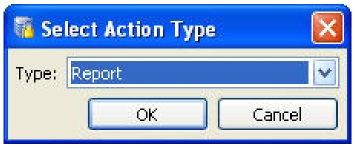


Interval: Weekly
Day of week: Wednesday
Time of day: 10:00

Step 5 Select the action to generate a report file:

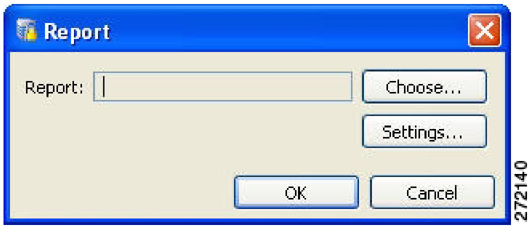
a. In the **Action** section, click the **Add**... button.

b. Select **Report** from the drop-down menu.



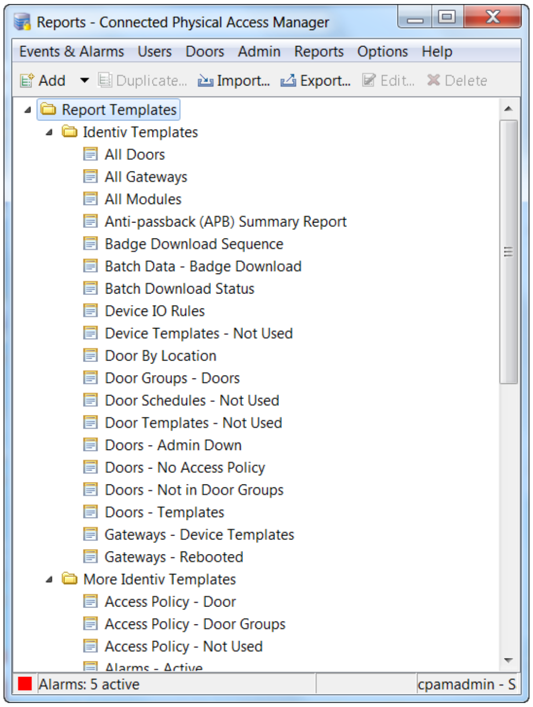
Step 6 Define the type of report and the format of the output:

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.



Report Templates
- Identiv Templates
  - All Doors
  - All Gateways
  - All Modules
  - Anti-passback (APB) Summary Report
  - Badge Download Sequence
  - Batch Data - Badge Download
  - Batch Download Status
  - Device IO Rules
  - Device Templates - Not Used
  - Door By Location
  - Door Groups - Doors
  - Door Schedules - Not Used
  - Door Templates - Not Used
  - Doors - Admin Down
  - Doors - No Access Policy
  - Doors - Not in Door Groups
  - Doors - Templates
  - Gateways - Device Templates
  - Gateways - Rebooted
- More Identiv Templates
  - Access Policy - Door
  - Access Policy - Door Groups
  - Access Policy - Not Used
  - Alarms - Active

Alarms: 5 active
cpamadmin - S

Tip To create or edit reports, see Defining Reports (Report Manager), page 13-33.

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.

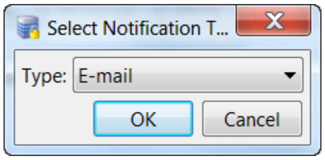
d. Repeat these steps to create additional **Actions** for the automated rule, if necessary.

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.

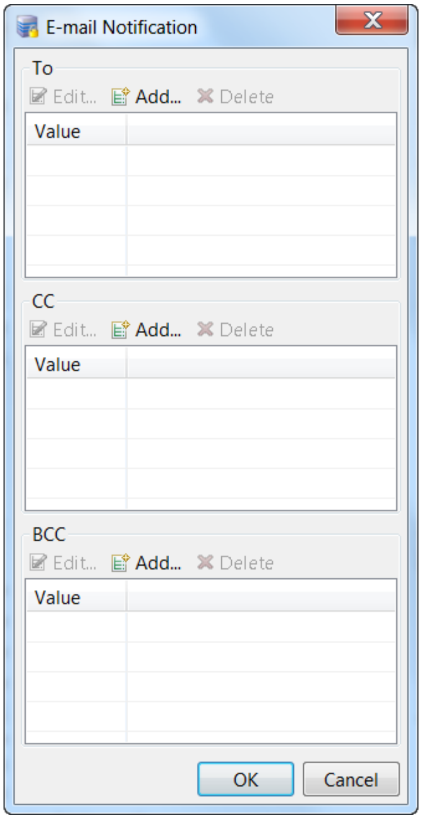
c. Click **OK**.



Type: E-mail

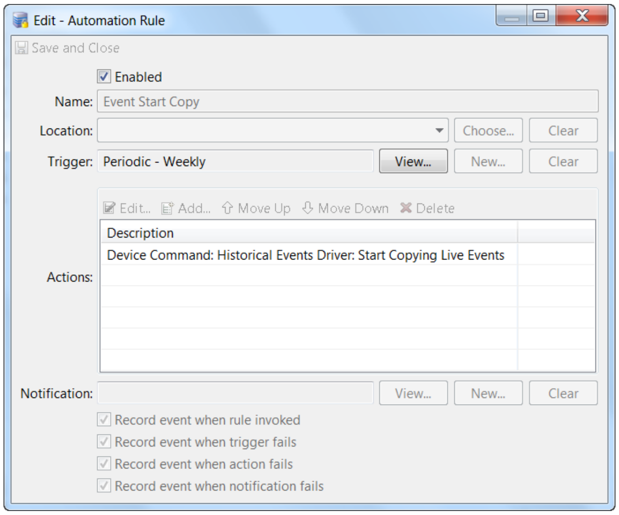
Step 8 Add e-mail addresses for the **To**, **CC**, and or **BCC** fields. You can enter specific e-mail addresses, or select addresses from the Personnel records configured in ICPAM.

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



Step 9 Verify that all configurations are correct.

Step 10 Click **Save and Close** to save the Automated Rule and close the window.



☑ Enabled

Name: Event Start Copy

Location:

Trigger: Periodic - Weekly

Actions:

Description
Device Command: Historical Events Driver: Start Copying Live Events

Notification:

☑ Record event when rule invoked

☑ Record event when trigger fails

☑ Record event when action fails

☑ Record event when notification fails

Step 11 Add the Automation driver as described in Enabling the Automation Driver, page 13-16.

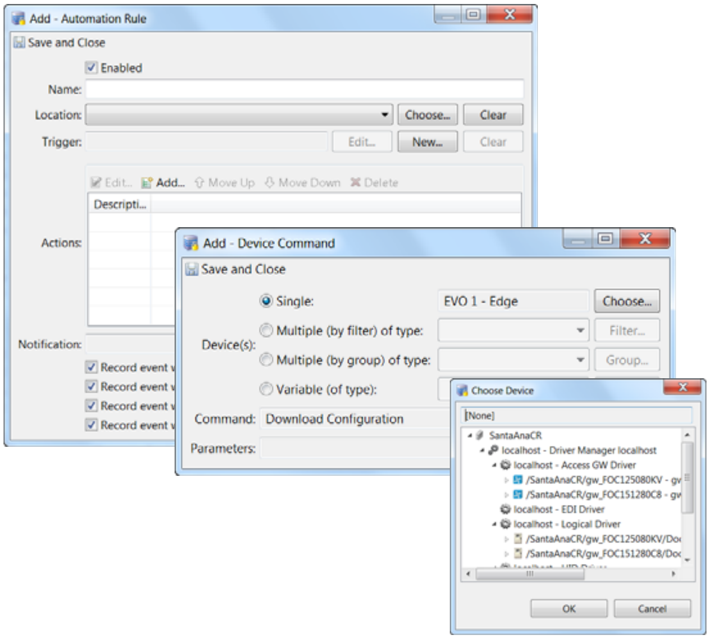
Note This step is only necessary if the Automation Driver is not already added.

Automation Rules in ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (see Logins Settings, page 17-10), 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 as shown in Figure 13-1 on page 13-30.

Figure 13-1 Add Automation Rule



● Single: EVO 1 - Edge

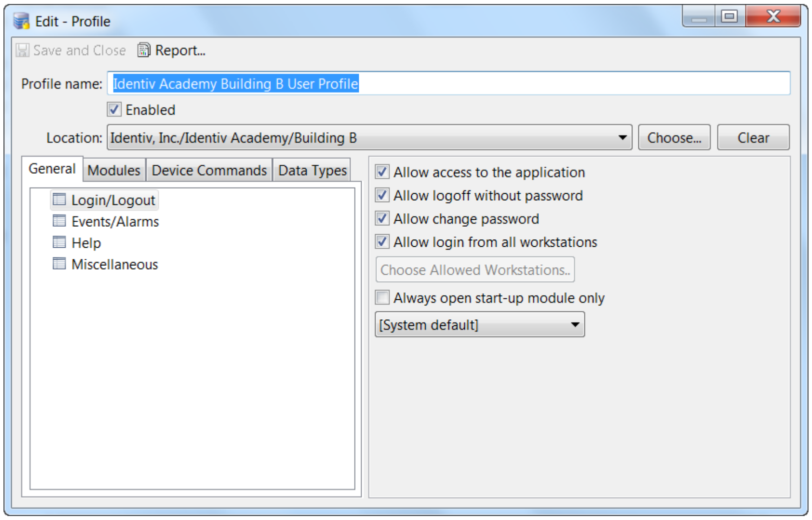
Command: Download Configuration

- 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 > Login/Logout.**

Figure 13-2 Assign to Login



Edit - Profile

Save and Close | Report...

Profile name: Identiv Academy Building B User Profile

☑ Enabled

Location: Identiv, Inc./Identiv Academy/Building B | Choose... | Clear

General | Modules | Device Commands | Data Types

□ Login/Logout
□ Events/Alarms
□ Help
□ Miscellaneous

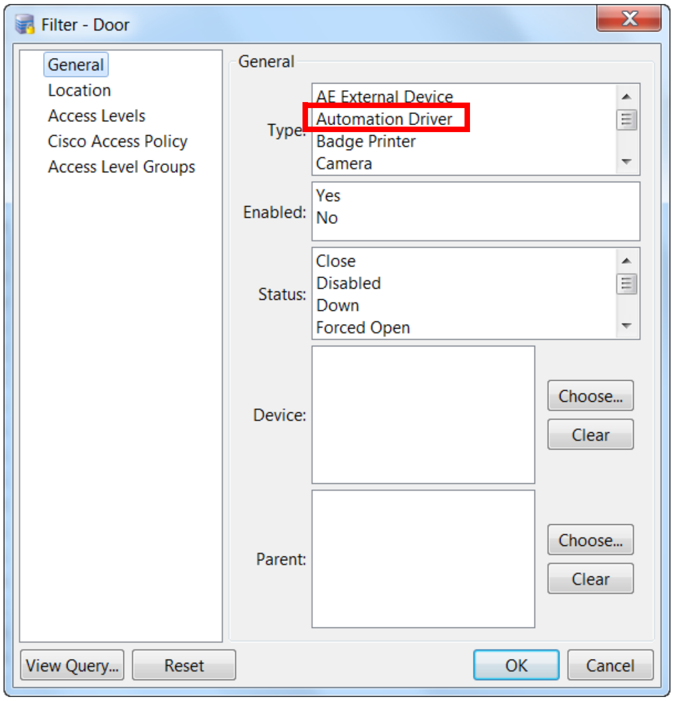
☑ Allow access to the application
☑ Allow logoff without password
☑ Allow change password
☑ Allow login from all workstations
Choose Allowed Workstations..
□ Always open start-up module only
[System default]

Step 2 Select the **Ignore hierarchical location restriction for device matching filter** check box.

Step 3 Click **Filter**. The Filter Device window appears.

Step 4 Select Automation Driver from the Type drop down list.

Figure 13-3 Select Automation Driver



Filter - Door

General
Location
Access Levels
Cisco Access Policy
Access Level Groups

General

Type: AE External Device / Automation Driver / Badge Printer / Camera

Enabled: Yes / No

Status: Close / Disabled / Down / Forced Open

Device: | Choose... | Clear

Parent: | Choose... | Clear

View Query... | Reset | OK | Cancel

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 ICPAM system configuration; otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

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. 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 13-16 for instructions to assign reports to automated tasks.

This section includes the following information:

- Report Manager in ICPAM 2.1, page 13-33
- Using the Report Manager, page 13-34
- Filter-based Report Template, page 13-35
- Object SQL-based Report Template, page 13-36
- SQL-Based Report Template, page 13-37

Report Manager in ICPAM 2.1

If the profile enhancement feature is set in the system configuration settings (see Logins Settings, page 17-10), 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.

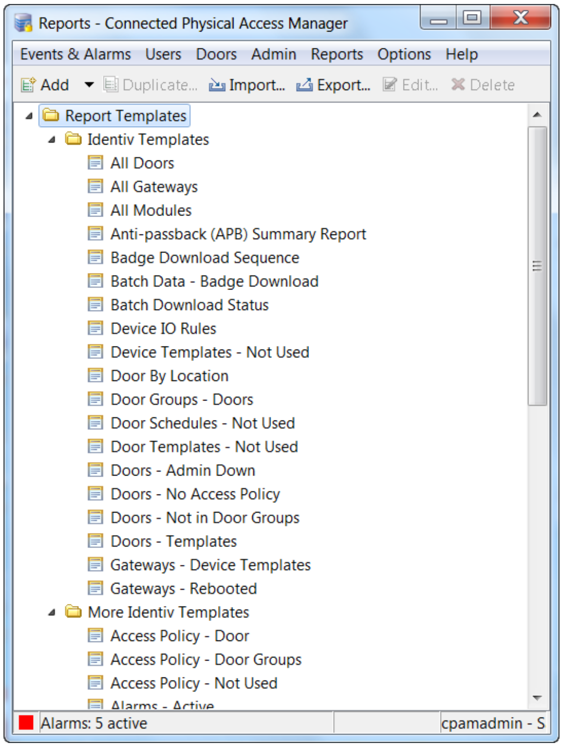
Note These points are applicable only when the profile enhancement feature is set in the ICPAM system configuration; otherwise the ICPAM appliance retains its behavior as in the previous version (1.5.1).

Using the Report Manager

To use the report manager, follow this procedure.

Step 1 Select **Report Manager** from the Reports menu. The main window appears, as shown in Figure 13-4.

Figure 13-4 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 Filter-based Report Template...**: See Filter-based Report Template, page 13-35.
  - **Add Object SQL-based Report Template... See** Object SQL-based Report Template, page 13-36.
  - **Add SQL-based Report Template...**: See SQL-Based Report Template, page 13-37.
  - **Add Folder...**: Adds a new folder for report organization.
- **Import...**: Import a previously exported report or set of reports from XML.
- **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 13-35
- SQL-Based Report Template, page 13-37

Filter-based Report Template

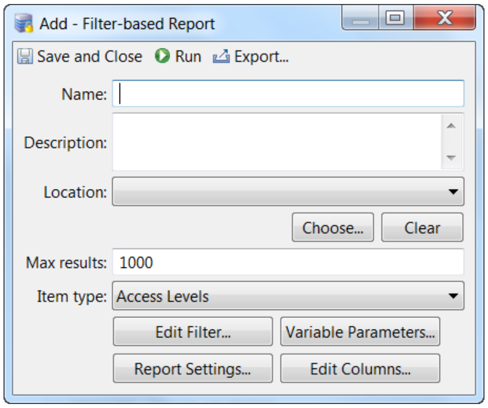
When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

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 13-5 shows the detail window for a Filter-based Report Template. Complete the fields according to the descriptions in Table 13-1.

Figure 13-5 Filter-based Report Template


Add - Filter-based Report

Name:

Description:

Location:

Max results: 1000

Item type: Access Levels

Table 13-1 Filter-based Report Template Settings

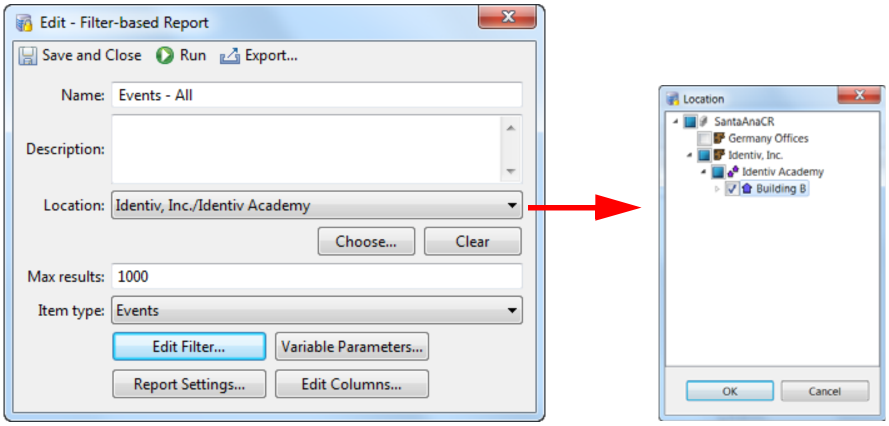
Field	Description
Name	Enter a unique name for the report.
Max results	The number of results displayed in the report. "-1" retrieves unlimited results.
Item type	The type of category to build the filter based report on.
Edit Filter...	Defines the filter, similar to filters available in the toolbar. See Using Filters, page 3-12.
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 3-10.

Table 13-1 Filter-based Report Template Settings (continued)

Field	Description
Variable Parameters...	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.
Edit Columns...	Select the columns used in the report. Use the **Up** and **Down** buttons to reorder the columns for the report.

Note The filter based reports have an additional field, **Location** that allows the user to retrieve reports on the devices or events in the user's assigned location only.See (Figure 13-6). This is based on the system configuration settings. For more on this, see Logins Settings, page 17-10.

Figure 13-6 Filter based Report with Location



Name: Events - All

Description:

Location: Identiv, Inc./Identiv Academy

Max results: 1000

Item type: Events

- SantaAnaCR
  - □ Germany Offices
  - Identiv, Inc.
    - Identiv Academy
      - ☑ Building B

Object SQL-based Report Template

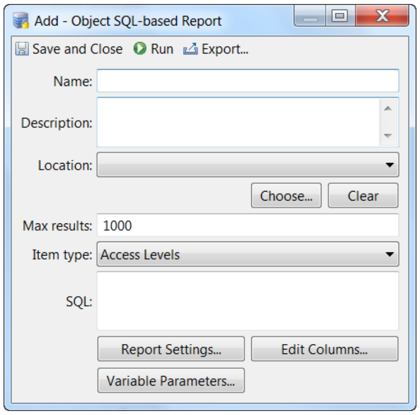
When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

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 13-7 shows the detail window for a Object SQL-based Report Template. Complete the fields according to the descriptions in Table 13-2.

Figure 13-7 Object SQL-based Report Template


Add - Object SQL-based Report

Name:
Description:
Location:
Max results: 1000
Item type: Access Levels
SQL:

Table 13-2 Object SQL-based Report Template Settings

Field	Description
Name	Enter a unique name for the report.
Max results	The number of results displayed in the report. `"-1"` retrieves unlimited results.
Item type	The type of category to build the object SQL-based report on.
SQL	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.
Report Settings...	Report generation options. For more information on report settings see Creating Reports, page 3-10).
Variable Parameters...	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.

SQL-Based Report Template

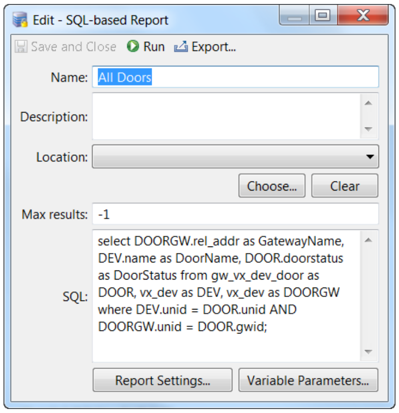
When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

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 SQL-based report template. Complete the fields according to the descriptions in Table 13-2.

Figure 13-8 SQL-based Report Template



Name: All Doors

Description:

Location:

Max results: -1

SQL:

```
select DOORGW.rel_addr as GatewayName,
DEV.name as DoorName, DOOR.doorstatus
as DoorStatus from gw_vx_dev_door as
DOOR, vx_dev as DEV, vx_dev as DOORGW
where DEV.unid = DOOR.unid AND
DOORGW.unid = DOOR.gwid;
```

SQL-Based Report Template Settings

Field	Description
Name	Enter a unique name for the report.
Max results	The number of results displayed in the report. `"-1"` retrieves unlimited results.
SQL	The SQL query to be executed. It returns all the column data defined in the SQL.
Report Settings...	Report generation options. For more information on report settings see Creating Reports, page 3-10.
Variable Parameters...	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 "select evt_time from vx_evt where evt_time < (?) ;"

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 policies, unselect the ‘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.

CHAPTER 14

System Integration

This chapter describes how to integrate the ICPAM data and actions with enterprise or third-party systems.

Contents

Note See also the *Cisco Physical Access Control API Reference Guide* and http://www.identiv.com/support-icpam for information on web services support.

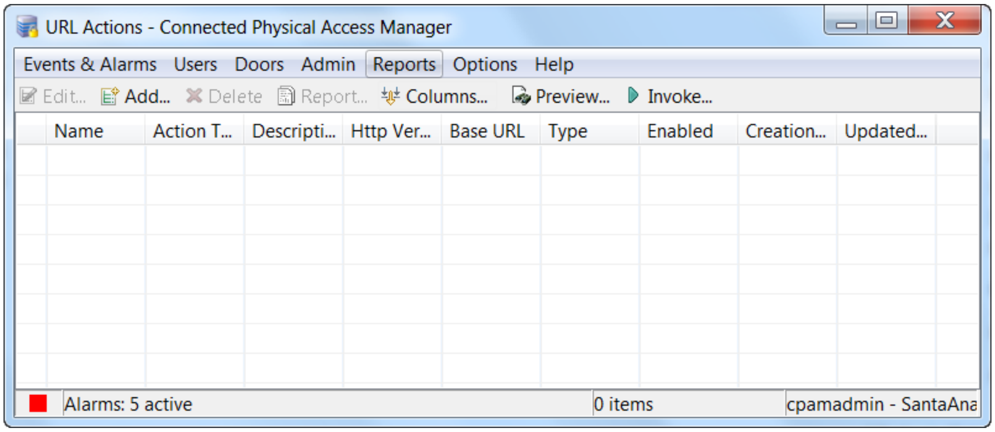
Configuring URL Actions

URL actions allow you to trigger actions in external systems when alarms or events occur in ICPAM. For example, URL actions can trigger the following in other systems:

- Identiv 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 Identiv 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



Name	Action T...	Descripti...	Http Ver...	Base URL	Type	Enabled	Creation...	Updated...

🟥 Alarms: 5 active | 0 items | cpamadmin - SantaAna

- 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).

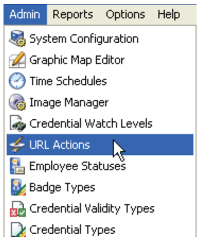
See the following sections for instructions to create and automate URL actions:

- Creating or Modifying URL Actions, page 14-3
- Creating Automated Rules for URL Actions, page 14-5
- Viewing URL Events, Alarms, and Logs, page 14-7

Creating or Modifying URL Actions

To add or modify URL actions, complete the following instructions:

Step 1 Select **URL Actions** from the **Admin** menu.



Step 2 Click **Add** to create a new action, or select an existing action and click **Edit**.

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.

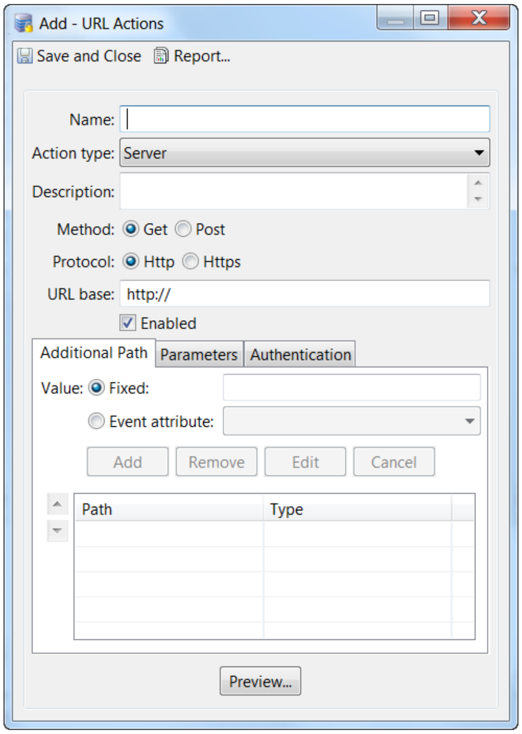
d. **Http / Https**: Select the connection method. The ICPAM default for secure connections is to present a client certificate, and accept all secure certificates.

e. Enter the **URL base**.

This is the URL of the system that will be triggered.

For example: http://www.identiv.com

f. Select **Enabled** to enable or disable the action.



Name:

Action type: Server

Description:

Method: ● Get ○ Post

Protocol: ● Http ○ Https

URL base: http://

☑ Enabled

Value: ● Fixed:

○ Event attribute:

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.

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>*

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.identiv.com/sample_value/ <Device Type>?Fixed_Text=text_sample&Event_Attr=*
<Device Address>

Step 6 (Optional) Enter the username and password required to access the URL.

Note The username and password is used for servers requiring authentication. If authentication is unsuccessful, the server returns a response code: *401*: *Unauthorized*. This code is placed in the data field of the event generated from executing the URL action.

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.

Step 1 Select **Global I/O** from the **Events & Alarms** menu.

Step 2 Click **Add**.

Step 3 Enter a Name for the rule and select or deselect the Enabled check box.

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** 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.

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**.

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 the "Enabling the Automation Driver" section on page 13-16.
- **FTP**: Sends the file to the specified FTP server.
  - **Host**: The FTP server IP address or name.
  - **Username**: Log in username required by the FTP server.
  - **Password**: Password to log in to the FTP server.
  - **Path**: Path on the FTP server where files should be uploaded.
- **Syslog**: Sends the notification or report to a syslog.
  - **Host**: The Syslog server IP address or name.
  - **Facility**: The facility to use when recording the information to the syslog.

Step 7 Select the event options. These events occur when the rule is successfully invoked, or when rule options fail.

Click the check boxes to activate or deactivate the options:

- **Record event when rule invoked:** Each time the rule is invoked, record an event.
- **Record event when trigger fails:** Each time the trigger fails, record an event.
- **Record event when action fails:** Each time the action fails, record an event
- **Record event when notification fails:** Each time the notification fails, record an event.

Step 8 Click **Save and Close**.

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 ICPAM 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 14-7
- Viewing Alarms for Failed URL Action, page 14-8
- Event and Alarm Response Codes for URL Actions, page 14-8
- Viewing Logs for URL Action Output, page 14-9
- URL Action Failure Due to Invalid Security Certificate, page 14-10

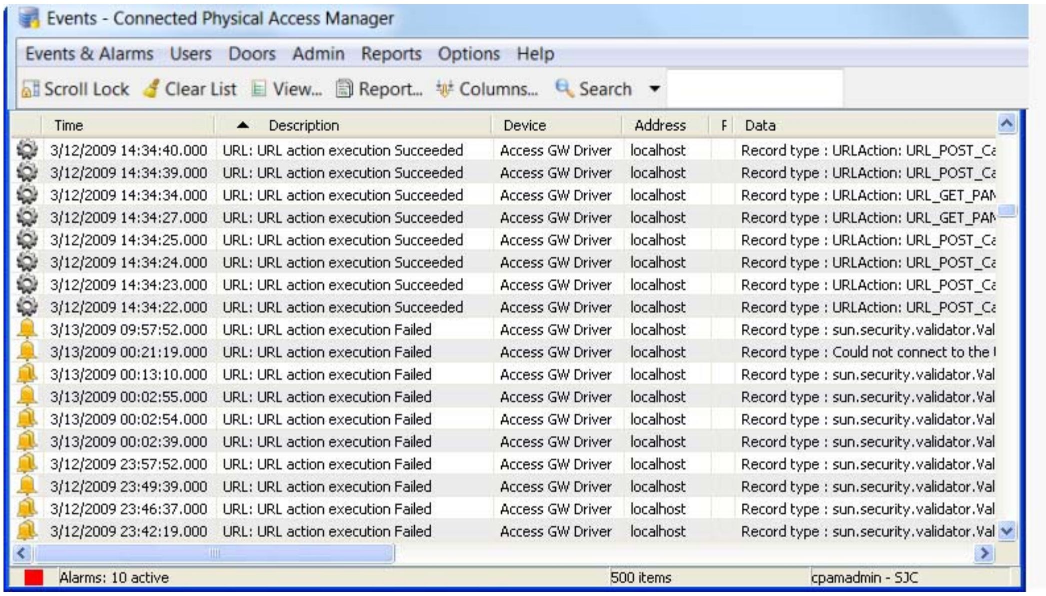
Viewing URL Action Events

To view events, select **Events** from the **Events & Alarms** menu, under the **Monitoring** submenu.

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



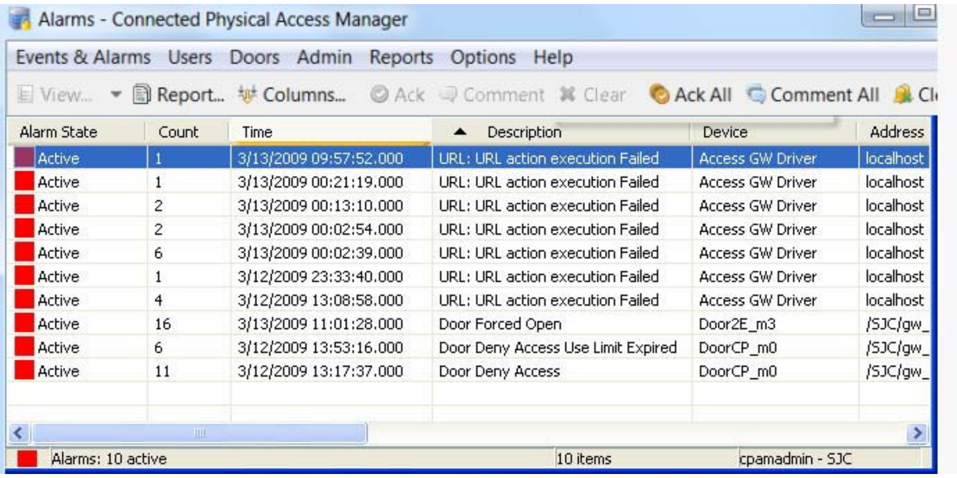
Time	▲ Description	Device	Address	F	Data
3/12/2009 14:34:40.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_POST_Ca
3/12/2009 14:34:39.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_POST_Ca
3/12/2009 14:34:34.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_GET_PAN
3/12/2009 14:34:27.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_GET_PAN
3/12/2009 14:34:25.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_POST_Ca
3/12/2009 14:34:24.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_POST_Ca
3/12/2009 14:34:23.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_POST_Ca
3/12/2009 14:34:22.000	URL: URL action execution Succeeded	Access GW Driver	localhost		Record type : URLAction: URL_POST_Ca
3/13/2009 09:57:52.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/13/2009 00:21:19.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : Could not connect to the
3/13/2009 00:13:10.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/13/2009 00:02:55.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/13/2009 00:02:54.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/13/2009 00:02:39.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/12/2009 23:57:52.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/12/2009 23:49:39.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/12/2009 23:46:37.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val
3/12/2009 23:42:19.000	URL: URL action execution Failed	Access GW Driver	localhost		Record type : sun.security.validator.Val

Viewing Alarms for Failed URL Action

To view only failed URL actions, select **Alarms** from the **Events & Alarms** menu, under the **Monitoring** submenu. 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.

Figure 14-3 URL Action Alarms



Alarm State	Count	Time	Description	Device	Address
🟥 Active	1	3/13/2009 09:57:52.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	1	3/13/2009 00:21:19.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	2	3/13/2009 00:13:10.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	2	3/13/2009 00:02:54.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	6	3/13/2009 00:02:39.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	1	3/12/2009 23:33:40.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	4	3/12/2009 13:08:58.000	URL: URL action execution Failed	Access GW Driver	localhost
🟥 Active	16	3/13/2009 11:01:28.000	Door Forced Open	Door2E_m3	/SJC/gw_
🟥 Active	6	3/12/2009 13:53:16.000	Door Deny Access Use Limit Expired	DoorCP_m0	/SJC/gw_
🟥 Active	11	3/12/2009 13:17:37.000	Door Deny Access	DoorCP_m0	/SJC/gw_

🟥 Alarms: 10 active 10 items cpamadmin - SJC

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

- 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

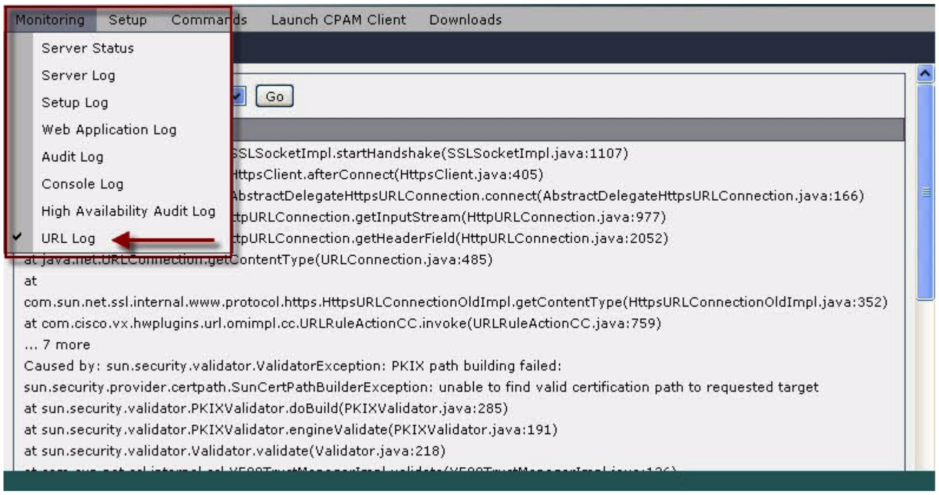
Viewing Logs for URL Action Output

To display the output (HTTP response) from URL actions, open the URL Log in the ICPAM Server Administration utility.

Step 1 Log onto the ICPAM appliance as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

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



```
SSLSocketImpl.startHandshake(SSLSocketImpl.java:1107)
HttpsClient.afterConnect(HttpsClient.java:405)
AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.java:166)
tpURLConnection.getInputStream(HttpURLConnection.java:977)
tpURLConnection.getHeaderField(HttpURLConnection.java:2052)
at java.net.URLConnection.getContentType(URLConnection.java:485)
at
com.sun.net.ssl.internal.www.protocol.https.HttpsURLConnectionOldImpl.getContentType(HttpsURLConnectionOldImpl.java:352)
at com.cisco.vx.hwplugins.url.omimpl.cc.URLRuleActionCC.invoke(URLRuleActionCC.java:759)
... 7 more
Caused by: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:285)
at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:191)
at sun.security.validator.Validator.validate(Validator.java:218)
```

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 ICPAM Server Administration utility (see Viewing Logs for URL Action Output, page 14-9):

```
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 ICPAM client and try again.
- When the URL Action was invoked by an automated rule, stop and start the ICPAM server and try again. See Using the Web Admin Menus, Commands and Options, page 2-18 for instructions to restart the server.
- When the URL Action was invoked by a Quick Launch button, stop and start the ICPAM server and try again. See Using the Web Admin Menus, Commands and Options, page 2-18 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 ICPAM database. This section includes instructions to do the following:

- Install the **EDI license** on the ICPAM server.
- Download and install the **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 ICPAM 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

Review the following notes before creating EDI projects:

- This feature requires an optional Identiv license. The **EDI** menu appears only after the license is installed on the ICPAM server. See Obtaining and Installing Optional Feature Licenses, page 2-44 for instructions.
- The source database records are the master version: imported records cannot be deleted in ICPAM.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 - Tree** 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 ICPAM is synchronized with the Video Surveillance Manager (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 Identiv VSM server. Restart the EDI project after the actions are complete. For more information, see Summary of EDI Administration Functions, page 14-44 and Managing the Camera Inventory, page 15-28.
- Stop any running EDI projects before upgrading the ICPAM appliance software. After the upgrade, you can restart the projects. See Importing and Starting EDI Projects, page 14-37 for instructions to stop, start and import EDI projects. If EDI projects are not stopped before a ICPAM upgrade, the project execution (or run) will not be successful. If this occurs, contact your Identiv 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

- 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.
- For importing EDI personnel data from Active directory, users should not make major modifications to the AD schema and the User object should contain the field name **when changed**.

Understanding Photo File Compression When Importing Personnel Records

Photo files that are imported into the ICPAM 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 ICPAM.

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.

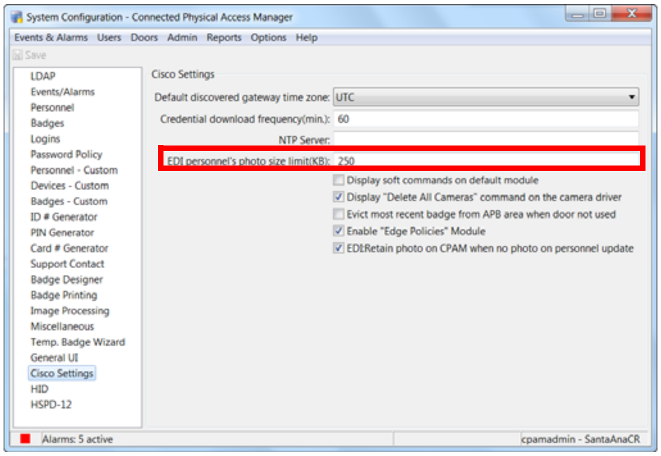
Step 2 Select **Cisco Settings** on the left (Figure 14-5).

Step 3 In the field *EDI personnel's photo size limit*, ***e**nter 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.

Figure 14-5 ICPAM Settings



Cisco Settings

Default discovered gateway time zone: UTC

Credential download frequency(min.): 60

NTP Server:

EDI personnel's photo size limit(KB): 250

□ Display soft commands on default module

☑ Display "Delete All Cameras" command on the camera driver

□ Evict most recent badge from APB area when door not used

☑ Enable "Edge Policies" Module

☑ EDI:Retain photo on CPAM when no photo on personnel update

Step 4 Click **Save** to save the changes.

Step 5 Log out and log back into the ICPAM application to activate the changes (select **Logout** from the **Options** menu).

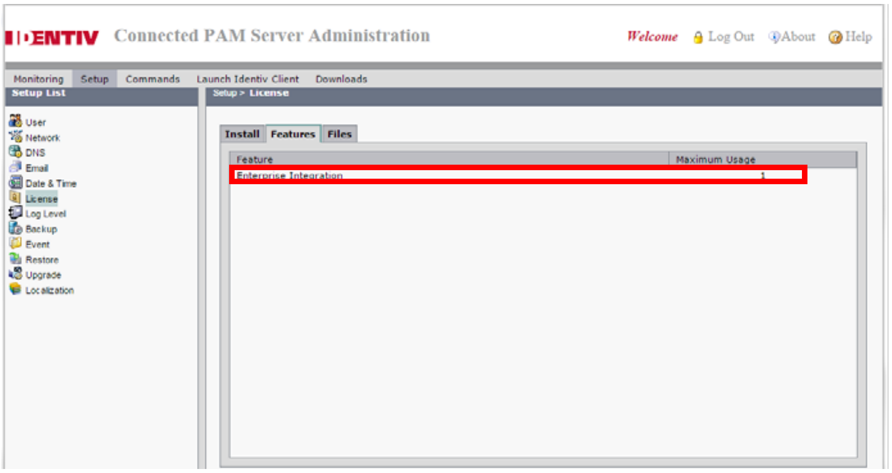
Installing the EDI Licence and Desktop Application

To enable EDI database integration, complete the following tasks:

1. Install the EDI license on the ICPAM server.
2. Start the EDI driver in the ICPAM hardware module.
3. Install the EDI Studio desktop software on your PC.

Step 1 Install the EDI license on the ICPAM server. Figure 14-6 shows the EDI license installed on a ICPAM server. See Using the Web Admin Menus, Commands and Options, page 2-18 for information to view the installed licenses or purchase and install new licenses.

Figure 14-6 ICPAM Licenses



Feature	Maximum Usage
Enterprise Integration	1

Step 2 Create and start the EDI driver, if necessary.

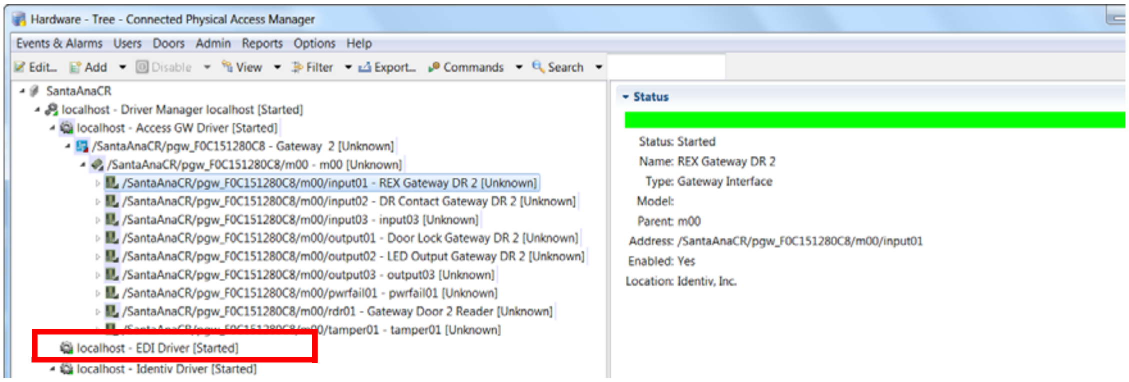
a. Select **Hardware - Tree** from the **Doors** menu.

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).

Figure 14-7 EDI Driver



SantaAnaCR
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/SantaAnaCR/pgw_F0C151280C8 - Gateway 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00 - m00 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/input01 - REX Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/input02 - DR Contact Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/input03 - input03 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/output01 - Door Lock Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/output02 - LED Output Gateway DR 2 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/output03 - output03 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/pwrfail01 - pwrfail01 [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/rdr01 - Gateway Door 2 Reader [Unknown]
/SantaAnaCR/pgw_F0C151280C8/m00/tamper01 - tamper01 [Unknown]
localhost - EDI Driver [Started]
localhost - Identiv Driver [Started]

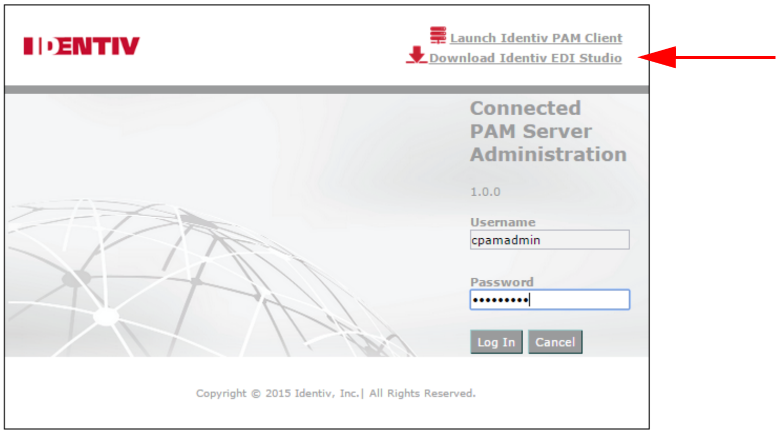
Status: Started
Name: REX Gateway DR 2
Type: Gateway Interface
Model:
Parent: m00
Address: /SantaAnaCR/pgw_F0C151280C8/m00/input01
Enabled: Yes
Location: Identiv, Inc.

Step 3 Download and install the EDI Studio desktop software.

a. Open a Web browser and enter the IP address for the ICPAM Server Administration utility.

b. Click **Download Identiv 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.

Figure 14-8 Download EDI Studio


IDENTIV
Launch Identiv PAM Client
Download Identiv EDI Studio
Connected PAM Server Administration
1.0.0
Log In
Cancel

Username
cpamadmin

Password
•••••••••

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Tip You can also log into the ICPAM Server Administration utility and select **Download Identiv EDI Studio (JRE Required)** from the **Downloads** menu. See Using the Web Admin Menus, Commands and Options, page 2-18.

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 **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 ICPAM to begin data synchronization.

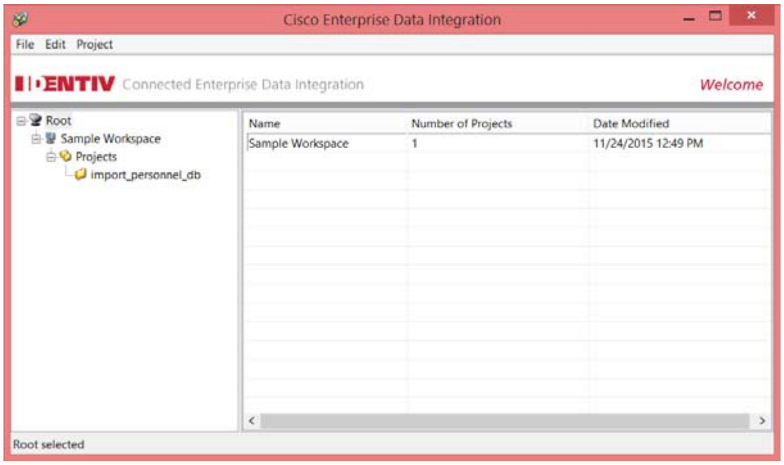
This section provides an example to import personnel records from a Microsoft Active Directory database into the ICPAM database. This example does not cover every possible scenario, and the specific records, fields and other data may not match the details for your site. Contact your Active Directory administrator for assistance when performing this process.

Review the following notes before creating and running an Active Directory project:

- ICPAM supports a single Active Directory project in EDI. You can create multiple Active Directory projects, but only one can run.
- The 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.

Step 1 Select **EDI Studio** on your Windows PC. The EDI main window opens.


Cisco Enterprise Data Integration
File
Edit
Project
IDENTIV Connected Enterprise Data Integration
Welcome
Root
Sample Workspace
Projects
import_personnel_db

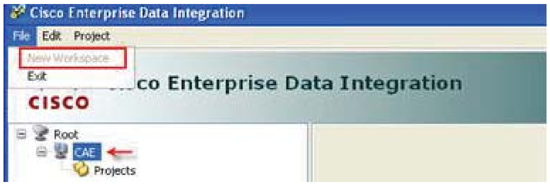
Name	Number of Projects	Date Modified
Sample Workspace	1	11/24/2015 12:49 PM

Root selected

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.


Cisco Enterprise Data Integration
File Edit Project
New Workspace
Exit
...co Enterprise Data Integration
cisco
Root
CAE
Projects

Tip **Root** and **Workspace** help organize your projects. They do not serve any other purpose.

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:

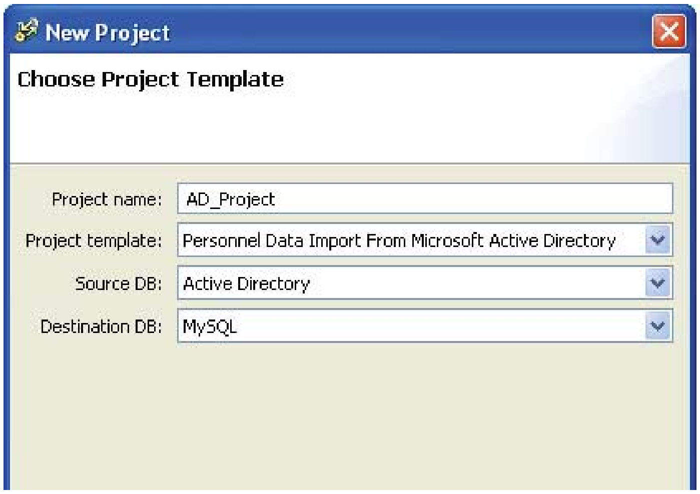
a. **Project name**: enter the name of the project.

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**.



Choose Project Template

Project name: AD_Project
Project template: Personnel Data Import From Microsoft Active Directory
Source DB: Active Directory
Destination DB: MySQL

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 ICPAM appliance network. For example, both systems should be on the same network.

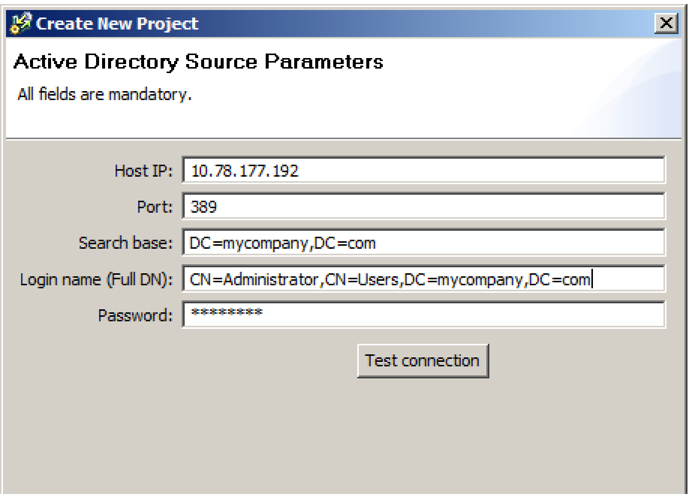
b. **Port**: enter the TCP port for the database server. Port 389 is the default for LDAP.

c. **Search base**: the Distinguished Name (DN) to use as a base for queries. For example: `dc=foobar`.

Note ICPAM 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.



Create New Project

Active Directory Source Parameters

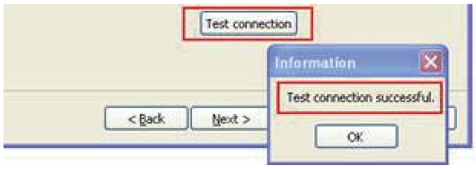
All fields are mandatory.

Host IP: 10.78.177.192
Port: 389
Search base: DC=mycompany,DC=com
Login name (Full DN): CN=Administrator,CN=Users,DC=mycompany,DC=com
Password: *********

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.

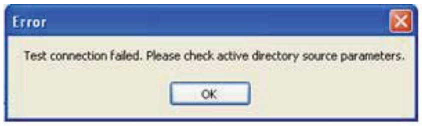
- If the settings are valid, **Test connection successful** appears.



Information

Test connection successful.

- 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.



Error

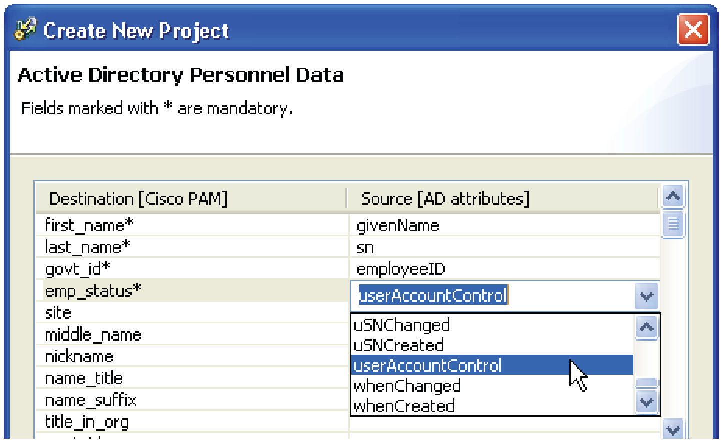
Test connection failed. Please check active directory source parameters.

Tip To verify the Active Directory user account attribute for the ICPAM login, use the tools described in the following step. ICPAM 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* ICPAM 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.



Create New Project

Active Directory Personnel Data

Fields marked with * are mandatory.

Destination [Cisco PAM]	Source [AD attributes]
first_name*	givenName
last_name*	sn
govt_id*	employeeID
emp_status*	userAccountControl
site	
middle_name	
nickname	
name_title	
name_suffix	
title_in_org	

- See also Notes for Mapping the AD and ICPAM User Attribute Names, page

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 e.Click Next..

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 e.Click Next.).

Notes for Mapping the AD and ICPAM User Attribute Names

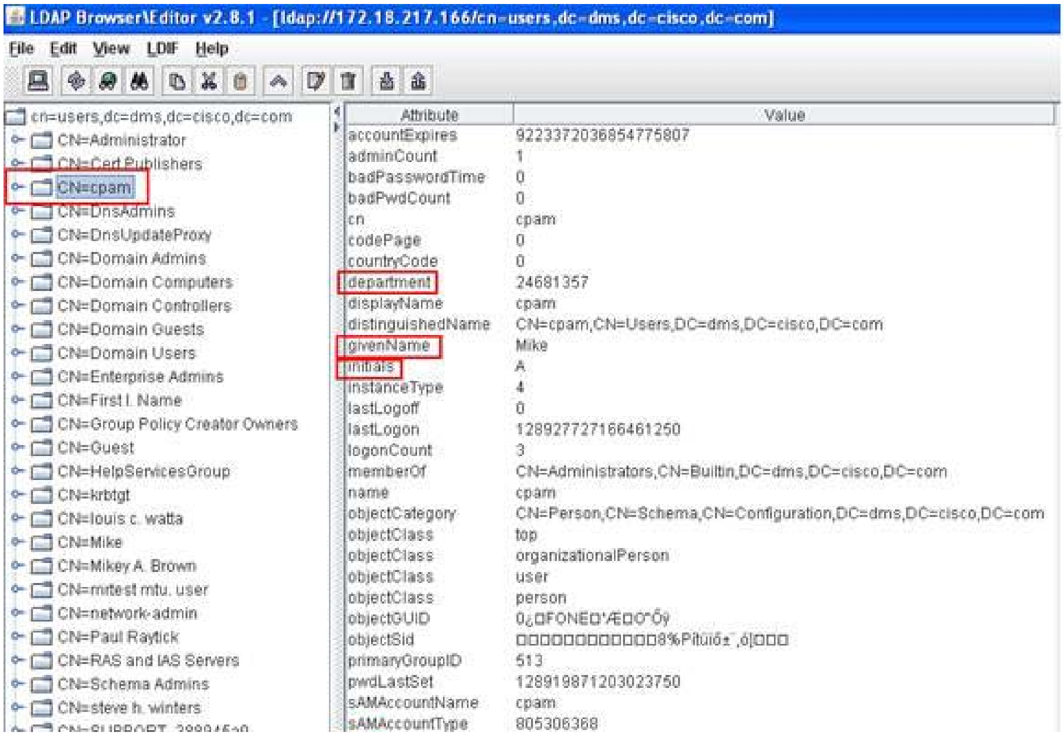
In the AD structure, a user's name includes an attribute `sn` for the last name, and another attribute `givenName` for the first name. For example: of Mike Smith would include:

- sn=Smith
- givenName=Mike

When you create an AD user log in for the ICPAM 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 ICPAM record. The first is called **LDAP Browser/**. Although Identiv does not provide this tool and does not document the tool usage, the sample output to the right shows the information you need to obtain for use with the EDI project. In this sample, the `cpam` user allows the ICPAM server to log in to the AD database. The sn attribute defines the lastname, and the givenName attribute defines the first name.

In addition, the Active Directory attribute `department` is defined. This attribute is mapped to the ICPAM field `govt_id`.



LDAP Browser\Editor v2.8.1 - [ldap://172.18.217.166/cn=users,dc=dms,dc=cisco,dc=com]

cn=users,dc=dms,dc=cisco,dc=com
CN=Administrator
CN=Cert Publishers
CN=cpam
CN=DnsAdmins
CN=DnsUpdateProxy
CN=Domain Admins
CN=Domain Computers
CN=Domain Controllers
CN=Domain Guests
CN=Domain Users
CN=Enterprise Admins
CN=First I. Name
CN=Group Policy Creator Owners
CN=Guest
CN=HelpServicesGroup
CN=krbtgt
CN=louis c. watta
CN=Mike
CN=Mikey A. Brown
CN=mitest mtu. user
CN=network-admin
CN=Paul Raytick
CN=RAS and IAS Servers
CN=Schema Admins
CN=steve h. winters

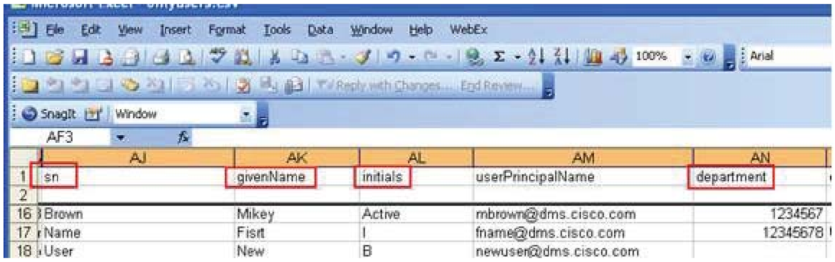
Attribute	Value
accountExpires	9223372036854775807
adminCount	1
badPasswordTime	0
badPwdCount	0
cn	cpam
codePage	0
countryCode	0
department	24681357
displayName	cpam
distinguishedName	CN=cpam,CN=Users,DC=dms,DC=cisco,DC=com
givenName	Mike
initials	A
instanceType	4
lastLogoff	0
lastLogon	128927727166461250
logonCount	3
memberOf	CN=Administrators,CN=Builtin,DC=dms,DC=cisco,DC=com
name	cpam
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=dms,DC=cisco,DC=com
objectClass	top
objectClass	organizationalPerson
objectClass	user
objectClass	person
objectGUID	0¿□FONE□'Æ□□"Õÿ
objectSid	□□□□□□□□□□□□8%Pitúió±¨,ó|□□□
primaryGroupID	513
pwdLastSet	128919871203023750
sAMAccountName	cpam
sAMAccountType	805306368

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.



	AJ	AK	AL	AM	AN
1	sn	givenName	initials	userPrincipalName	department
2					
16	Brown	Mikey	Active	mbrown@dms.cisco.com	1234567
17	Name	Fisrt	I	fname@dms.cisco.com	12345678
18	User	New	B	newuser@dms.cisco.com	

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 ICPAM personnel records fields.

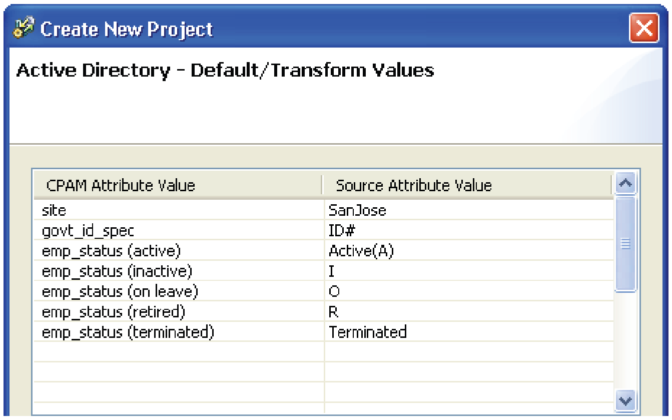
The ICPAM Active Directory Personnel Data window is shown with the correct field mappings. Click **Next** to validate the attribute mappings.

Step 8 Define the Active Directory default database values.

For example, enter the following in the in the **Source Attribute Value** column:

a. Enter a **site**. The **site** must match the ICPAM site name. The site name is shown in the bottom right corner of all ICPAM client windows. The site name is also displayed at the top of the Hardware tree.

b. Enter the **govt_id_spec** value.

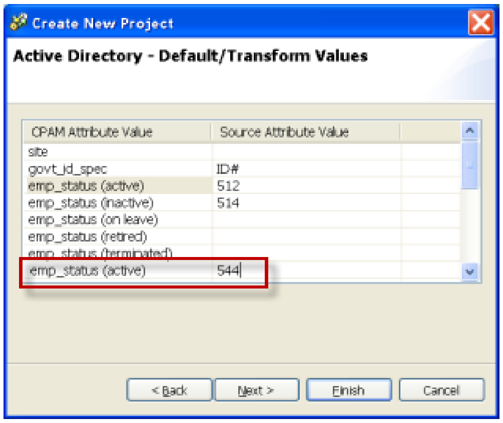


Active Directory - Default/Transform Values

CPAM Attribute Value	Source Attribute Value
site	SanJose
govt_id_spec	ID#
emp_status (active)	Active(A)
emp_status (inactive)	I
emp_status (on leave)	O
emp_status (retired)	R
emp_status (terminated)	Terminated

Note The entries are ignored if values are also entered in the previous **Personnel Data** window. You must enter values for these fields in one of the windows.

c. Enter the AD attribute 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. ICPAM supports status for active, inactive, on leave, retired, and terminated.



Active Directory - Default/Transform Values

CPAM Attribute Value	Source Attribute Value
site	
govt_id_spec	ID#
emp_status (active)	512
emp_status (inactive)	514
emp_status (on leave)	
emp_status (retired)	
emp_status (terminated)	
emp_status (active)	544

Tip If your organization has additional employee status codes, such as 544 to indicate that a user is active, but their password is expired, you can manually add those codes to the bottom of the list (as shown in the screen to the right). In the *ICPAM Attribute Value* column, manually enter an existing ICPAM value, such as **emp_status (active)**. In the *Source Attribute Value column*, enter your organization's code. You can also create new employee status attributes, if necessary. See the Creating Custom Employee Status Values, page 14-23.

d. Click **Next** to continue.

Step 9 (Optional) Select an EDI Extension file, if necessary.

EDI Extension files use API classes used to extend EDI functionality, including the following:

- Transform badge and personnel data received from an AD database. For example, remove the leading **1** from the Badge ID.
- Define default mapping. For example, assign Badge Templates based on the badge type.
- Provide cross field validation (such as dependency fields, correlation across different attributes or between badge and personnel data).

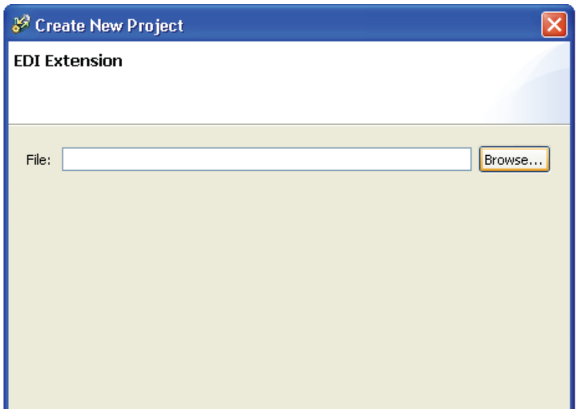
Extensions are built using an Identiv Systems framework and validated by the EDI Studio. Identiv also provides developer support.

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.

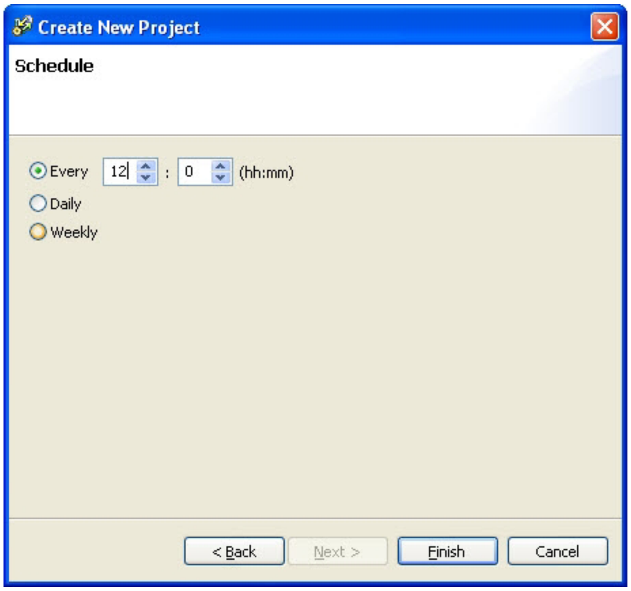
c. Click **Next** to continue.



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.



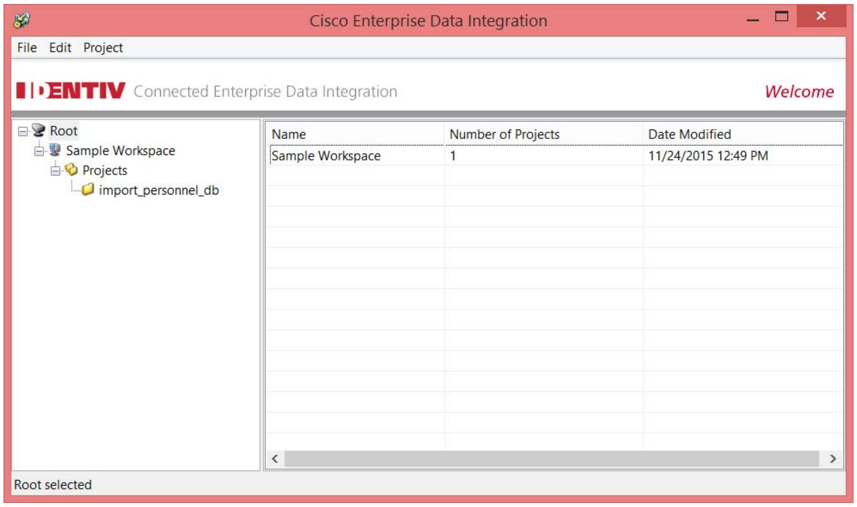
Scheduling Notes:

- Schedules are based on the ICPAM 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.
- ICPAM retrieves records with a 15 minute overlap from the previous run to prevent loss of data; all records will be included even if the ICPAM and Active Directory server time settings are a few minutes apart.

Step 11 Click **Finish** to create the new database project and return to the main window.

The project is shown in the main window. A `.jar` file is saved to the following directory on your PC:

`C:\Program Files\EDI Studio\workspaces\<`*`Project_Folder`*`>\`*`projects`*`\`



Name	Number of Projects	Date Modified
Sample Workspace	1	11/24/2015 12:49 PM

Tip An error message appears if any fields are incorrect or missing. Use the **Back** button to navigate to the screen and correct the entry. When you are done, click **Finish** from the window the correction was made. You do not need to return to the last window. The entries in all windows are preserved.

Step 12 (Optional) To change the data import rules or settings, select the project from the left window, and click **Edit** at the bottom of the detail window. Edit the settings as necessary and click **Save**.

Tip To change the name of a project, highlight the project and select **Rename** from the Edit menu. To delete a project, highlight the project and select **Delete** from the Edit menu.

Step 13 Import the project in ICPAM and start the project to begin importing records.

See Importing, Starting, and Monitoring EDI Projects in ICPAM, page 14-37

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.

For example, select **Administrators**.

You can also select the profile name and click **Edit**.

c. In the *Edit - Profile* window, select the **Modules** tab (Figure 14-9).

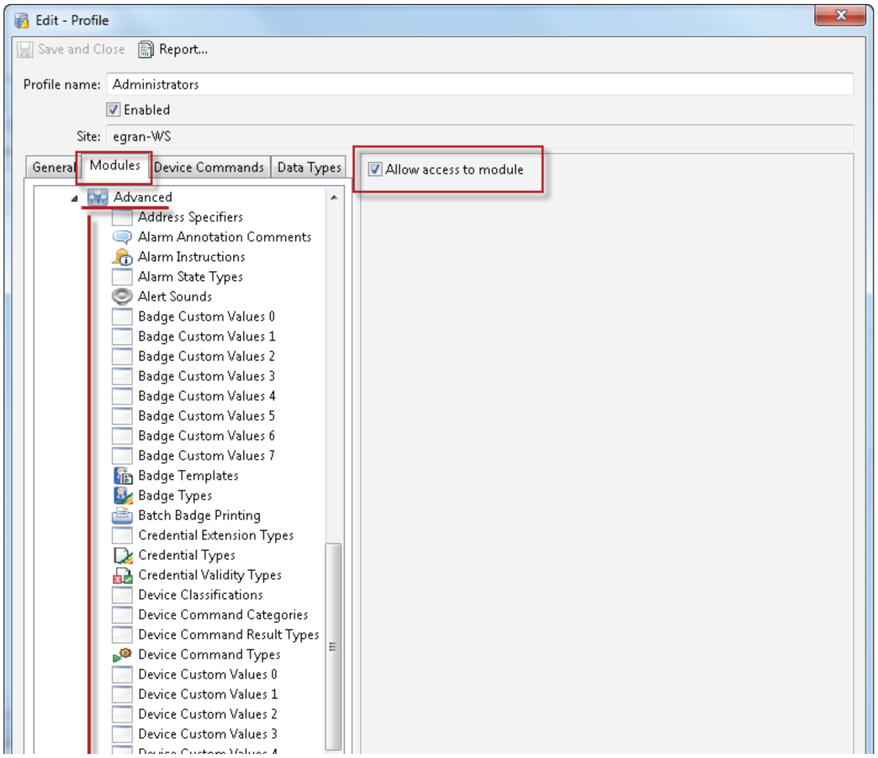
d. Expand the **Advanced** category.

e. Select **Employee Statuses** to highlight it.

f. Select the **Allow access to module** check box.

g. Click **Save and Close**.

Figure 14-9 Modules Available to a User Profile



Profile name: Administrators

☑ Enabled

Site: egran-WS

☑ Allow access to module

- Advanced
  - Address Specifiers
  - Alarm Annotation Comments
  - Alarm Instructions
  - Alarm State Types
  - Alert Sounds
  - Badge Custom Values 0
  - Badge Custom Values 1
  - Badge Custom Values 2
  - Badge Custom Values 3
  - Badge Custom Values 4
  - Badge Custom Values 5
  - Badge Custom Values 6
  - Badge Custom Values 7
  - Badge Templates
  - Badge Types
  - Batch Badge Printing
  - Credential Extension Types
  - Credential Types
  - Credential Validity Types
  - Device Classifications
  - Device Command Categories
  - Device Command Result Types
  - Device Command Types
  - Device Custom Values 0
  - Device Custom Values 1
  - Device Custom Values 2
  - Device Custom Values 3
  - Device Custom Values 4

Step 2 To display the new menu, logout of ICPAM and log back in.

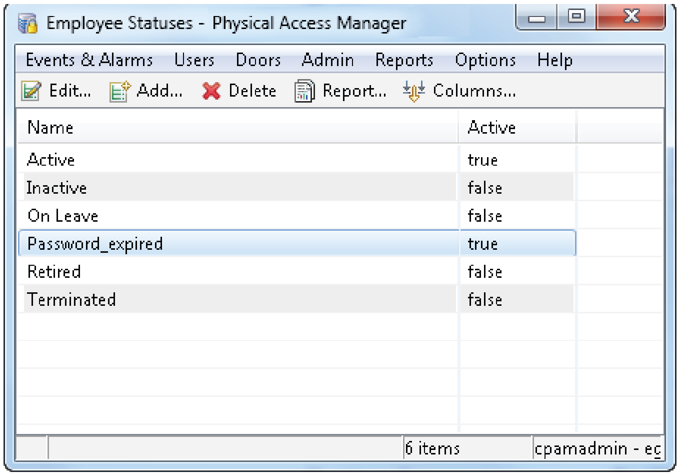
a. Choose **Logout** from the **Options** menu.

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).

Figure 14-10 Employee Statuses Window



Name	Active
Active	true
Inactive	false
On Leave	false
Password_expired	true
Retired	false
Terminated	false

6 items cpamadmin - ec

Step 4 Create a new employee status entry.

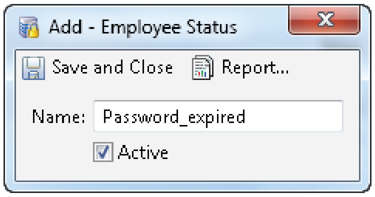
a. Click **Add**.

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



Name: Password_expired

☑ Active

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 ICPAM EDI module to begin data synchronization.

This section provides an example to import personnel records into ICPAM from one of the following databases:

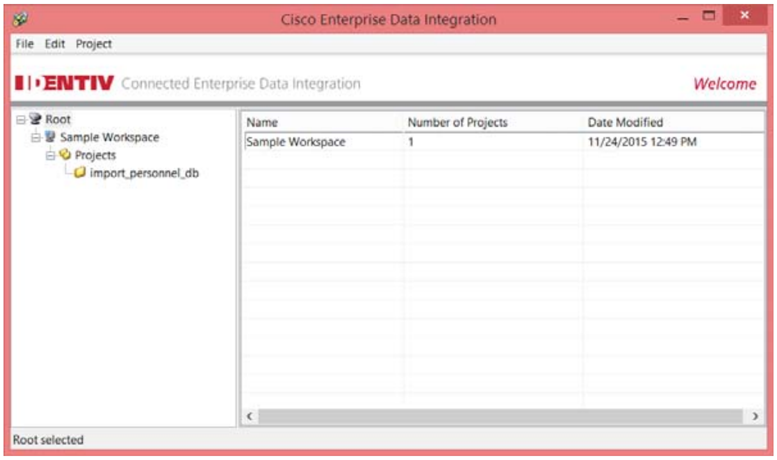
- MySQL version 5.0.4
- Oracle versions 10g and 11g
- SqlServer 2005 and SqlServer 2000

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 **EDI Studio** on your Windows PC. The ICPAM Enterprise Data Integration window opens, as shown in Figure 14-12.

Figure 14-12 EDI Studio: ICPAM Enterprise Data Integration Window



Name	Number of Projects	Date Modified
Sample Workspace	1	11/24/2015 12:49 PM

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).

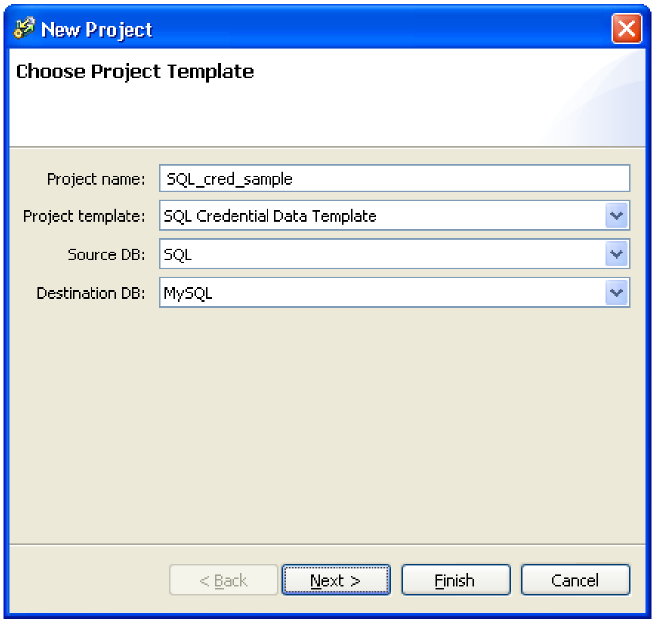
b. Enter the workspace name and click **OK**. The new workspace is created along with a Projects folder.

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 one of the available project templates, as shown in Figure 14-13.

Figure 14-13 EDI Studio: Choose Project Template


New Project

Choose Project Template

Project name: SQL_cred_sample

Project template: SQL Credential Data Template

Source DB: SQL

Destination DB: MySQL

a. **Project name**: enter a name for the project.

b. **Project template**: select a template that defines the data type (such as SQL credential data)

c. **Source DB**: select the database source (such as Oracle or MySQL).

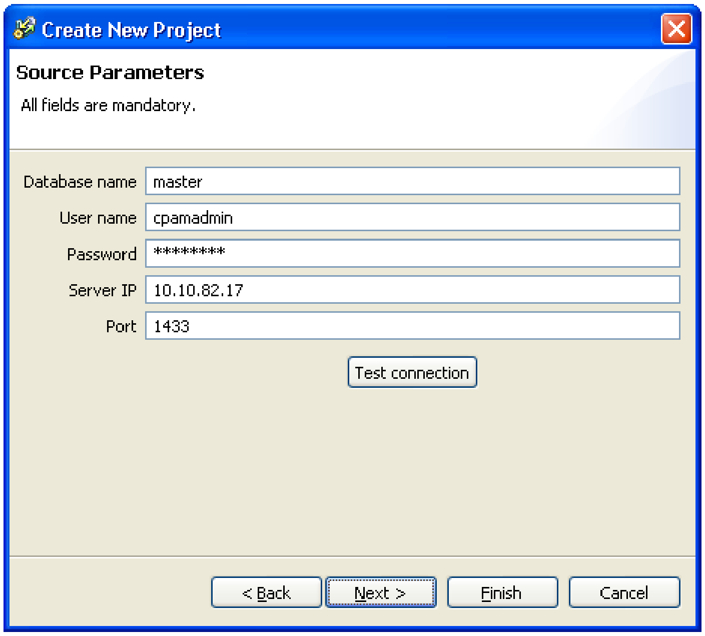
d. **Destination DB**: select the destination database (SQL or MySQL).

Note Oracle databases do not support boolean data types. You must define numeric data types and use them as boolean.

e. Click **Next**.

Step 5 Enter the source parameters, as shown in Figure 14-14.

Figure 14-14 EDI Studio: Enter Parameters for the Source Database



Create New Project

Source Parameters

All fields are mandatory.

Database name: master

User name: cpamadmin

Password: *********

Server IP: 10.10.82.17

Port: 1433

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 [ICPAM] 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 [ICPAM]** 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 14-1 Required Fields for Data Mapping

Data Type	Required Fields
Organization	**Organization Data** • **name**: (primary key) Name of the organization. **Department Data** • **name**: (primary key) Name of the department. • **orgName**: (primary key) Organization name
Personnel	• **site**: Site of the personnel record. • **firs_name**: User's first name. • **last_name**: User's last name • **govt_id**: (primary key) Government ID number. If the govt_id is a social security number, the length must be exactly nine digits. The valid values are: I, II, III, Jr., and Sr. • **govt_id_spec**: a unique id that can identify a personnel record. Valid values are SSN, FIN, and ID#. • **emp_status**: Employment status. The valid values are: active, inactive, on_leave, retired, and terminated. If your organization has additional employee status codes, such as *Active Password Expired*, you can manually add those codes to the bottom of the list: enter the ICPAM Value in the left column (it must be one of the 5 supported **emp_status** attributes, as shown), and then enter your organization's code in the right column. • The **emp_type** is not required, but has the following valid values: contractor, employee, employee_full_time, employee_part_time, intern, other, vendor, and visitor. **emp_type** is a type of employee. **Note** The Region and Nationality fields be values already defined in system.

Table 14-1 Required Fields for Data Mapping (continued)

Data Type	Required Fields
Credential (Badge Records)	**Note** The primary keys are **badgeId** and **facilityCode**. • **badgeId**: (primary key) The badge ID. • **badgetemplate**: Use this field to assign the parameters from a badge template in ICPAM to imported badges. This option is used when importing badges into ICPAM for the first time. For example, create or edit a badge template in ICPAM as described in Configuring Badge Templates, page 9-22. This template can contain settings for fields such as access policy, facility code, badge type, watch level, and effective date. Enter the name of the badge template in the Source Attribute Value column for **badgetemplate**. For example: KeyPad_BCD4, 26BitWiegandCT, 26BitWiegandKeyPadCT, etc. • **facilityCode**: (primary key) The facility code • **activationDate**: Activation date for the badge. • **expirationDate**: Date the badge expires. This date must be greater than the activation date. • **validity**: The valid values are: active, inactive, destroyed, lost, and stolen. • **role**: The user's role in the organization. The valid values are: employee, contractor, vendor, and temporary.

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.

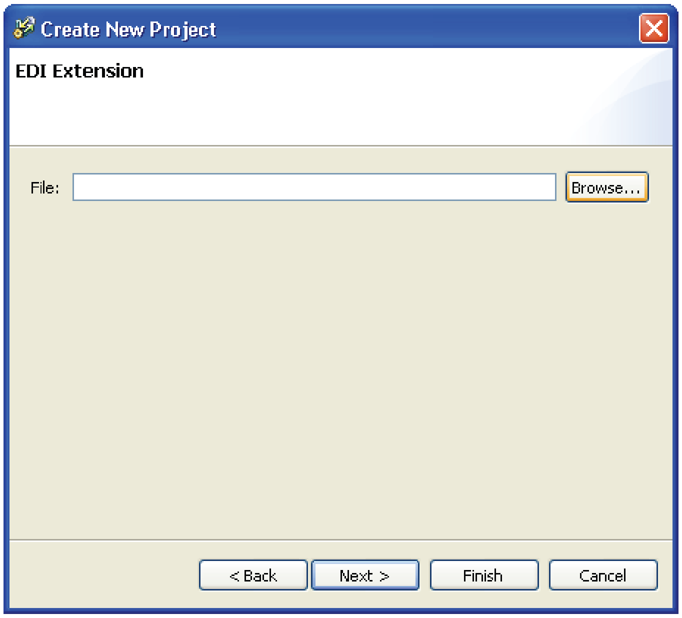
d. Click **Next.**

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 14-15).

Figure 14-15 EDI Studio: EDI Extension

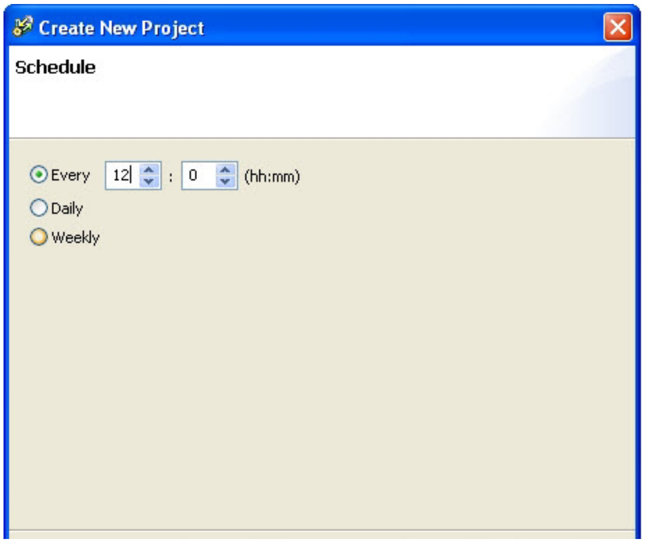


Step 9 Choose a schedule to specify how often data will be synchronized, as shown in Figure 14-16.

Note EDI actions are conducted according to the ICPAM 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.

Figure 14-16 EDI Studio: Choose Schedule


Create New Project

Schedule

● Every 12 : 0 (hh:mm)
○ Daily
○ Weekly

Note The minimum time frame to schedule a EDI job for synchronization is one hour.

Step 10 Click **Finish** to create the new database project and return to the ICPAM Data Enterprise application window (Figure 14-12 on page 14-26).

The project is shown in the main window and the project file is saved to the default EDI project directory on your PC:

```
C:\Program Files\ICPAM 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 ICPAM.

See Importing, Starting, and Monitoring EDI Projects in ICPAM, page 14-37.

EDI Project Data Field Mapping

This is the mapping information on equivalent fields between the destination ICPAM database and Source DB attributes.

Table 14-2 Personal Interface Data (Mandatory Fields)

Column Name	Type	Length	Mandatory/Comments
Updated TS	Datetime		Mandatory
Created TS	Datetime		Mandatory
first_name	String	255	Mandatory

Table 14-2 Personal Interface Data (Mandatory Fields)

Column Name	Type	Length	Mandatory/Comments
last_name	String	255	Mandatory
govt_id	String	255	Mandatory (employee ID)
govt_id_spec	String	255	Mandatory. Default mapping through GUI
emp_status	String	255	Mandatory. Transform values through GUI
Site	String	24	Default mapping through GUI
Photo	mediumblob (binary)		JPEG supported

Table 14-3 Personal Interface Table (Optional Fields)

Column Name	Type	Length	Optional/Comments
middle_name	String	255	Optional
Nickname	String	255	Optional
name_title	String	255	Optional
name_suffix	String	255	Optional
title_in_org	String	255	Optional
Org	String	255	Optional
Dept	String	255	Optional
user_id	String	255	Optional
emp_type	String	255	Optional
dob	Date		Optional
doh	Date		Optional
employee_number	String	255	Optional
comments	String	255	Optional
home_addr_line1	String	255	Optional
home_addr_line2	String	255	Optional
home_addr_city	String	255	Optional
home_addr_state_province	String	255	Optional
home_addr_country	String	255	Optional
work_addr_line1	String	255	Optional
work_addr_line2	String	255	Optional
work_addr_city	String	255	Optional
work_addr_state_province	String	255	Optional
work_addr_country	String	255	Optional
other_addr_line1	String	255	Optional
other_addr_line2	String	255	Optional
other_addr_city	String	255	Optional

Table 14-3 Personal Interface Table (Optional Fields) (continued)

Column Name	Type	Length	Optional/Comments
other_addr_state_province	String	255	Optional
other_addr_countr	String	255	Optional
home_phone	String	255	Optional
work_phone	String	255	Optional
mobile_phone	String	255	Optional
other_phone	String	255	Optional
Fax	String	255	Optional
primary_email	String	255	Optional
secondary_email	String	255	Optional
other_email	String	255	Optional
customAttr 0-19	String	255	Optional
customDateAttr 0-3	String	255	Optional

Table 14-4 Organization Interface Table

Column Name	Type	Length	Mandatory/Optional/Comments
Updated TS	Datetime		Mandatory
Created TS	Datetime		Mandatory
name	String	255	Mandatory
comments	String	255	Optional

Table 14-5 Department Interface Table

Column Name	Type	Length	Mandatory/Optional/Comments
Updated TS	Datetime		Mandatory
Created TS	Datetime		Mandatory
name	String	255	Mandatory
OrgName	String	255	Mandatory (organization and department has parent child relationship)
comments	String	255	Optional

Table 14-6 Badge Interface Table

Column Name	Type	Length	Mandatory/Comments
Updated TS	Datetime		Mandatory
Created TS	Datetime		Mandatory
badgeID	String	255	Mandatory
Validity String	255		Mandatory

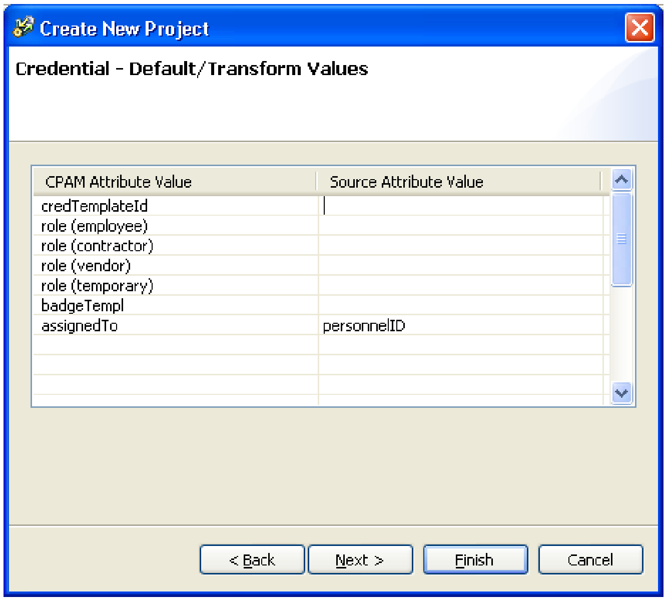
Table 14-6 Badge Interface Table

Column Name	Type	Length	Mandatory/Comments
role	String	255	Mandatory. Transform values through GUI
assignedTo	String	255	Optional. To get the badge import to associate to the appropriate users in the ICPAM automatically. Please refer the detailed process below.
credTemplateId	String	255	Mandatory
facilityCode	Int	11	Optional
pincode	String	255	Optional
isExemptOk	bit	1	Optional
useLimit	Int	11	Optional
activationDate	Date		Optional
expirationDate	Date		Optional
Comments	String	255	Optional
tempDeactivationDate	Date		Optional
tempDeactivationDays	Int	11	Optional
antiPassbackExempt	bit	1	Optional
useADADoorStrikeTime	bit	1	Optional
executiveCredential	bit	1	Optional
customAttr 0-7	String	255	Optional
customDateAttr 0-1	Date		Optional

Importing and Associating Badges to Corresponding Personnel Automatically

By default, the **assignedTo** field containing the default value as the personnel ID should appear in the EDI studio-mapping screen while creating a new project [SQL credential data template].

Figure 14-17 Creating a New Project



Create New Project

Credential - Default/Transform Values

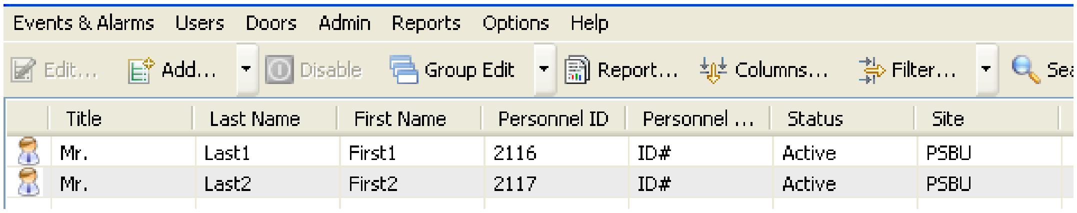
CPAM Attribute Value	Source Attribute Value
credTemplateId	
role (employee)	
role (contractor)	
role (vendor)	
role (temporary)	
badgeTempl	
assignedTo	personnelID

Note The personnel records in ICPAM should exist before importing the badge records.

Steps to Associate

Step 1 When the Personnel records are imported into ICPAM through EDI, the personnel module appears as below:

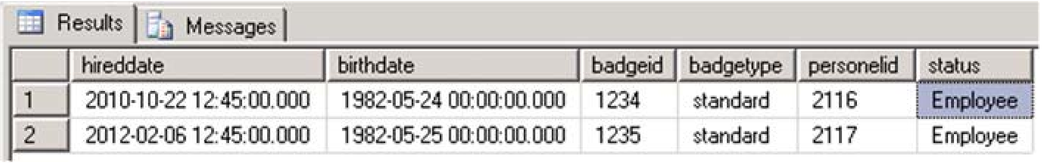
Figure 14-18 Personnel module



Title	Last Name	First Name	Personnel ID	Personnel ...	Status	Site
Mr.	Last1	First1	2116	ID#	Active	PSBU
Mr.	Last2	First2	2117	ID#	Active	PSBU

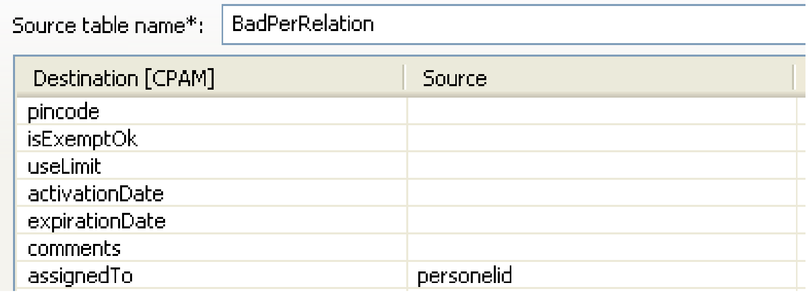
Step 2 While importing, it is necessary to associate the badges correctly to the personnel/users. To achieve that, the Personnel ID column in the Badge table can be correlated to the Personnel table via EDI. To accomplish this, the assignedTo column in the EDI attribute screen should be used.

Figure 14-19 Table mapping



	hireddate	birthdate	badgeid	badgetype	personelid	status
1	2010-10-22 12:45:00.000	1982-05-24 00:00:00.000	1234	standard	2116	Employee
2	2012-02-06 12:45:00.000	1982-05-25 00:00:00.000	1235	standard	2117	Employee

Figure 14-20 EDI Studio Attribute Screen



Source table name*: BadPerRelation

Destination [CPAM]	Source
pincode	
isExemptOk	
useLimit	
activationDate	
expirationDate	
comments	
assignedTo	personelid

Step 3 Launch ICPAM client. Upload the created project on EDI Admin module.

Step 4 Run the project. Check if the **assignedTo** field in the badges module is mapped to the required personnel.

Importing, Starting, and Monitoring EDI Projects in ICPAM

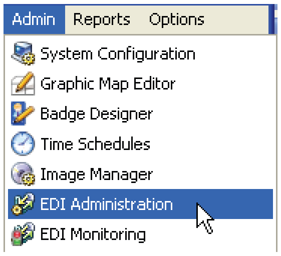
This section includes the following information:

- Importing and Starting EDI Projects, page 14-37
- Verifying EDI Projects (EDI Monitoring), page 14-39
- Modifying a Running EDI Project, page 14-42
- Restarting a Failed EDI Project, page 14-43
- Summary of EDI Administration Functions, page 14-44

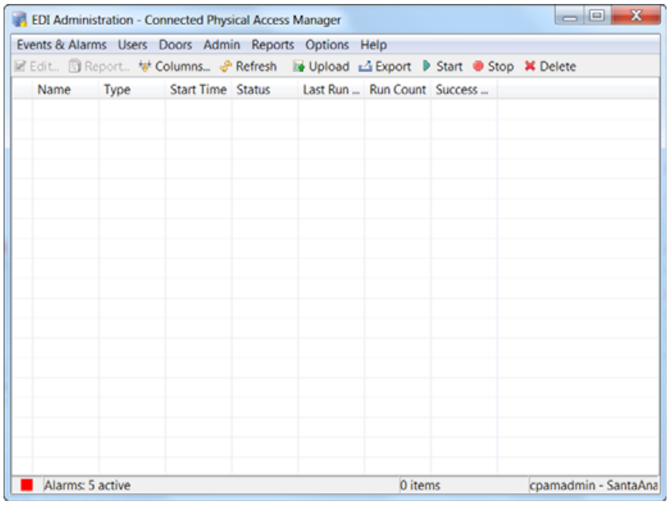
Importing and Starting EDI Projects

After the EDI projects are created, you must import the `.jar` project files into the ICPAM using the EDI Administration module.

Step 1 Select **EDI Administration** from the **Admin** menu.



The EDI administration screen appears like this example:



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:

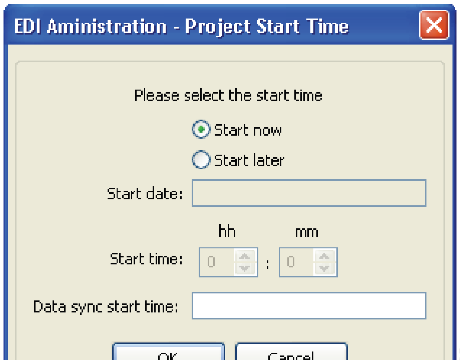
`C:\Program Files\ICPAM Systems\EDI Studio\workspaces\<`*`project_folder_name`*`>\projects\`

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.



EDI Aministration - Project Start Time

Please select the start time

● Start now

○ Start later

Start date:

Start time: hh 0 : mm 0

Data sync start time:

Note Active Directory EDI projects restart when the ICPAM 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.

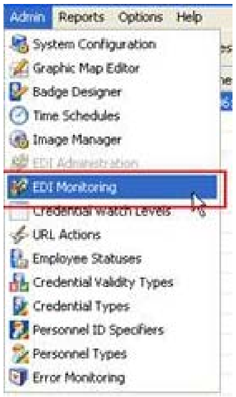
Step 5 Verify that the project is started.

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 14-21).

Figure 14-21 EDI Monitoring Menu



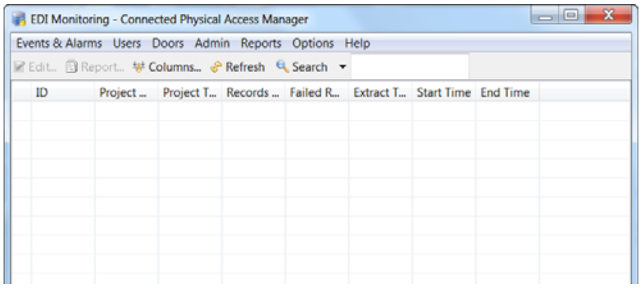
The following information is displayed for each record

Column	Description
ID	The EDI event ID number.
Project Name	The name of the EDI project that the event as defined in the EDI Desktop Studio.
Project Type	The type of data, such as personnel, badge, or organization records.
Records Succeeded	The number of records successfully updated during the integration event.
Failed Records	The number of records that were not updated by the integration event. Failed record details are stored in the log files.
Extract Type	The type of data extraction including interface or core (see the following step).
Start Time	The date and time when the data integration event began.
End Time	The date and time when the data integration event ended.

Step 2 Review the EDI projects on the EDI monitoring screen. There are two types of Extract Types (see Figure 14-22):

- **Interface**: this occurs when the ICPAM 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 ICPAM server validates the records retrieved by the interface process, and then edits the ICPAM personnel database to make the additions, deletions, or edits.

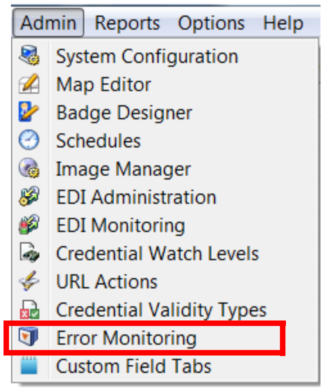
Figure 14-22 EDI Monitoring Window



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 ICPAM databases.

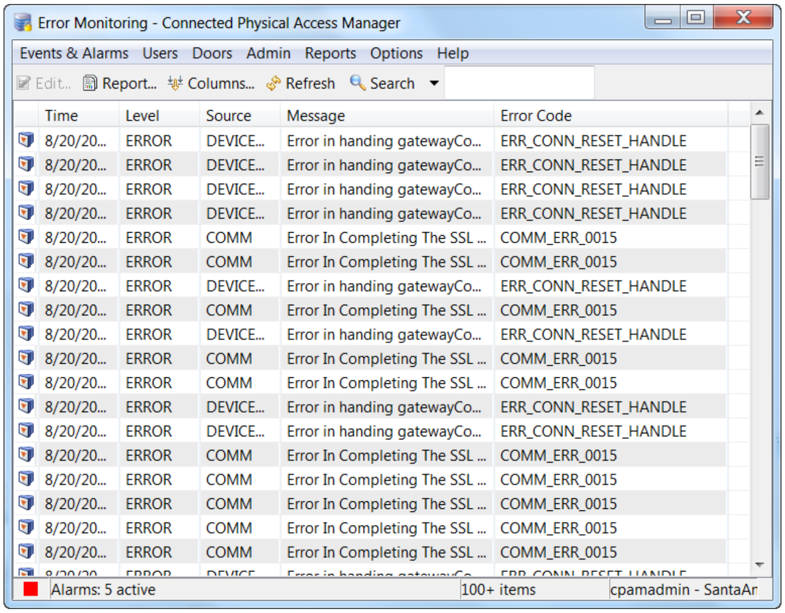
Step 3 To troubleshoot the errors and view additional error details, select **Error Monitoring** from the **Admin** menu (Figure 14-23).

Figure 14-23 EDI Error Monitoring Menu



Step 4 The Error Monitoring window displays entries for each failed record, as shown in Figure 14-24. 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 14-24 Error Monitoring



Time	Level	Source	Message	Error Code
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	COMM	Error In Completing The SSL ...	COMM_ERR_0015
8/20/20...	ERROR	DEVICE...	Error in handing gatewayCo...	ERR_CONN_RESET_HANDLE

🟥 Alarms: 5 active 100+ items cpamadmin - SantaAr

In addition, the following can occur:

Record updates in AD include a timestamp for the edit. When the ICPAM server connects, it compares the timestamp of the last edit in AD with what the last edit is that ICPAM knows about. If the AD timestamp is newer, the record is extracted.

Once the record is extracted from AD into ICPAM, the fields are checked for validity during the Core extract. For example if the AD last name (attribute `sn`) contains a number, ICPAM 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 14-42. If an EDI data integration project fails, identify and resolve the problem, and then complete the instructions in Restarting a Failed EDI Project, page 14-43.

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\ICPAM Systems\EDI Studio\workspaces\`*`Project_Folder`*`\`*`projects`*`\.`

Step 3 Edit the project in EDI Studio:

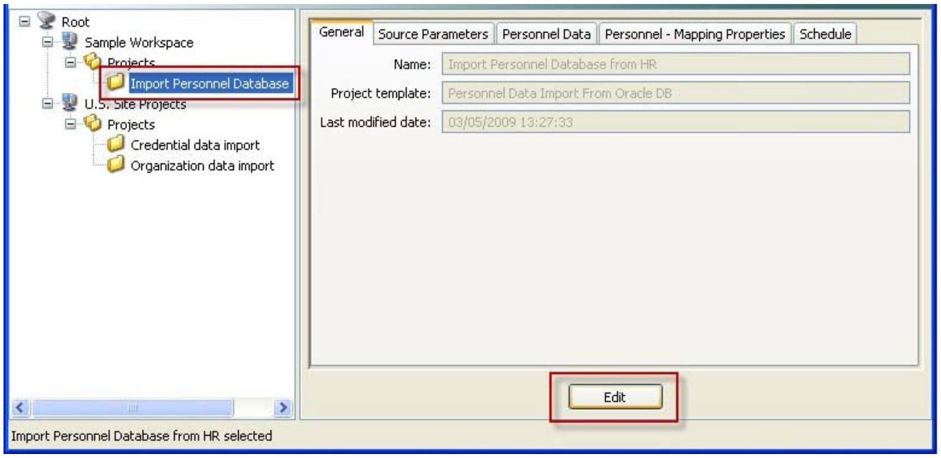
a. Open the EDI Studio application on your PC.

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 14-15.

Figure 14-25 Editing EDI Projects



Name: Import Personnel Database from HR

Project template: Personnel Data Import From Oracle DB

Last modified date: 03/05/2009 13:27:33

Import Personnel Database from HR selected

Step 4 Upload the modified project to ICPAM:

a. Select **EDI Administration** from the **Admin** menu.

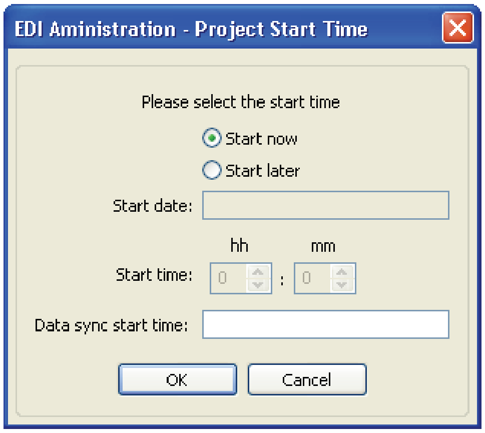
b. Click **Upload** and select the `.jar` file that was saved in the default EDI project directory on your PC:

`C:\Program Files\ICPAM 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 14-26):

Figure 14-26 EDI Project Start Time



EDI Aministration - Project Start Time

Please select the start time

● Start now

○ Start later

Start date:

Start time: hh 0 : mm 0

Data sync 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.

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 14-44.

Resolving ICPAM or EDI Studio Issues

If an error occurs in the ICPAM database, do the following.

Step 1 Correct the issue. For example:

- No organization values exist in the ICPAM records.
  When organization and department values are included in an imported personnel record, those values must already exist in the ICPAM 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 9-10 for more information.
- The project mapping is incorrect. See Modifying a Running EDI Project, page 14-42 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 14-37.

Summary of EDI Administration Functions

- Column Descriptions
- EDI Administration Functions, page 14-44

Column Descriptions

The EDI Administration window includes the following columns:

Column	Description
Name	The data integration project name, as defined in the EDI Desktop Studio.
Type	The type of data, such as personnel, badge, or organization records.
Recent Start Time	The most recent time that data integration began for the project.
Status	Specifies if the project is running, stopped, or scheduled.
Last Run Date	The date of project was last executed (successful and unsuccessful attempts).
Run Count	The number of times the project has been run (successful and unsuccessful attempts).
Success Run Count	The number of times the project has been successfully run.

EDI Administration Functions

The following functions are available from the menu at the top of the project list:

Function	Description
Refresh	Refresh the window to display current information.
Upload	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\ICPAM Systems\EDI Studio\workspaces\`*`Project_Folder`*`\projects\`
Export	Exports the project in the `.jar` file format.
Start	Runs a data integration project now, or at a specified time. **Tip** To create a recurring schedule for sxDI projects, use EDI studio. **Note** Active Directory EDI projects restart when the ICPAM 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.
Stop	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.
Delete	Removes the data integration project from ICPAM. The project remains in the EDI Desktop Studio.

Accessing the SQL Database

The ICPAM 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 ICPAM errors or system failures.

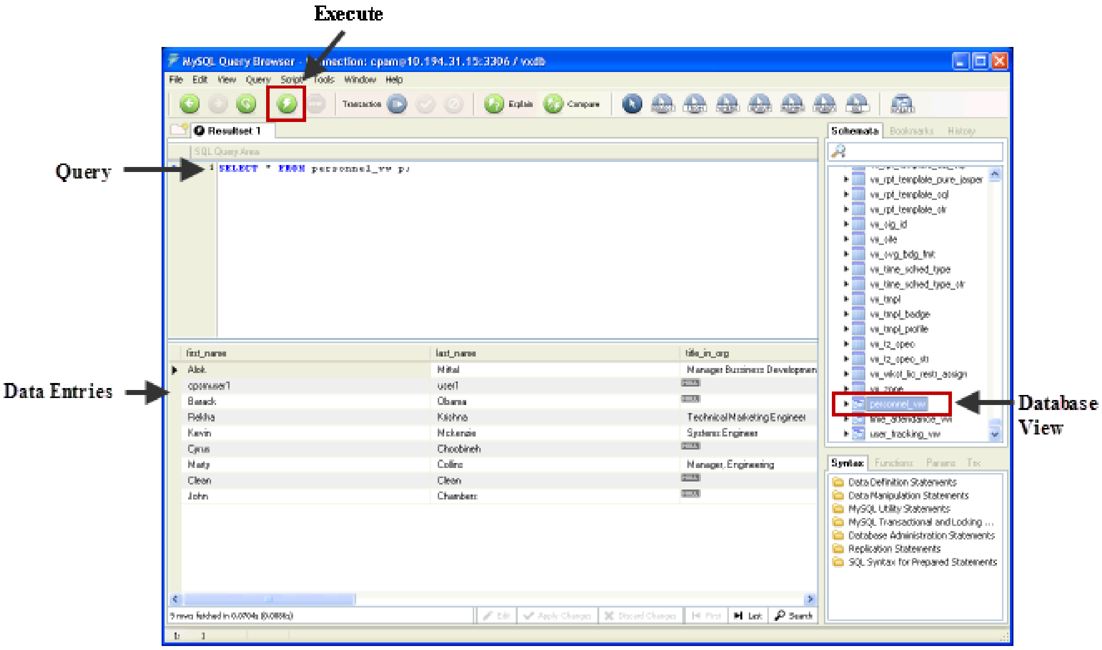
To view the ICPAM SQL database, complete the following procedure:

Step 1 Contact Identiv 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 Identiv 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 14-27).

Figure 14-27 MySQL Query Browser



```
1 SELECT * FROM personnel_vw p;
```

first_name	last_name	title_in_org
Alok	Mittal	Manager Business Developmen
cpamuser1	user1	NULL
Barack	Obama	NULL
Rekha	Krishna	Technical Marketing Engineer
Kevin	Mckenzie	Systems Engineer
Cyrus	Choobineh	NULL
Marty	Collins	Manager, Engineering
Clean	Clean	NULL
John	Chambers	NULL

9 rows fetched in 0.0704s (0.0858s)

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.

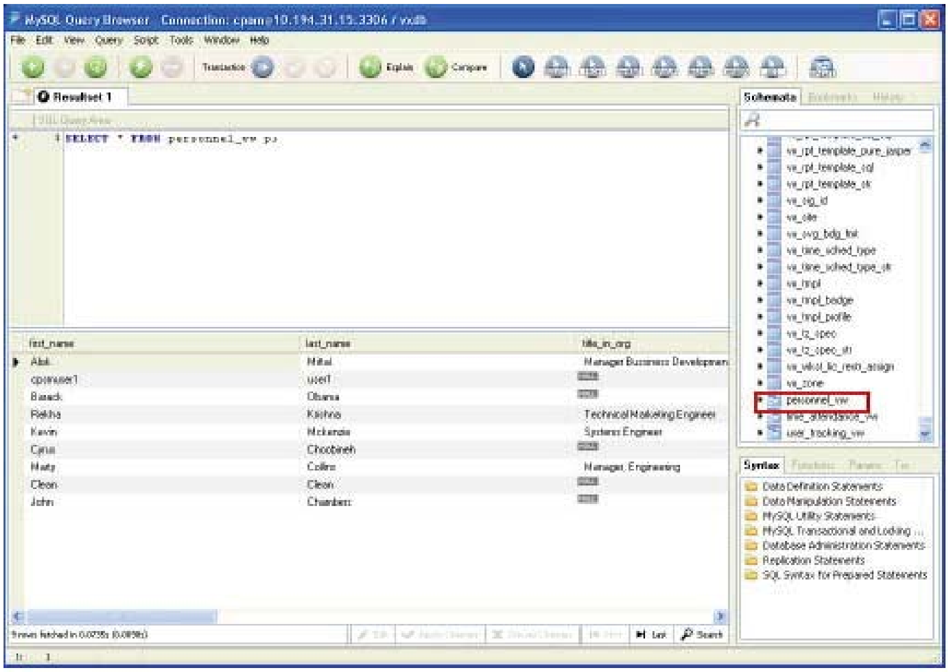
See the following for examples of the SQL data views:

- Personnel, page 14-46
- Time and Attendance, page 14-47
- User Tracking Data, page 14-48

Personnel

The Personnel view (Figure 14-28) provides personnel information such as first name, last name, user id, personnel id, photo image, and the image type.

Figure 14-28 Personnel



MySQL Query Browser - Connection: cpam@10.194.31.15:3306 / vxdb

```
SELECT * FROM personnel_vw p;
```

first_name	last_name	title_in_org
Alok	Mittal	Manager Business Developmen
cpamuser1	user1	NULL
Barack	Obama	NULL
Rekha	Krishna	Technical Marketing Engineer
Kevin	Mckenzie	Systems Engineer
Cyrus	Choobineh	NULL
Marty	Collins	Manager, Engineering
Cleon	Cleon	NULL
John	Chambers	NULL

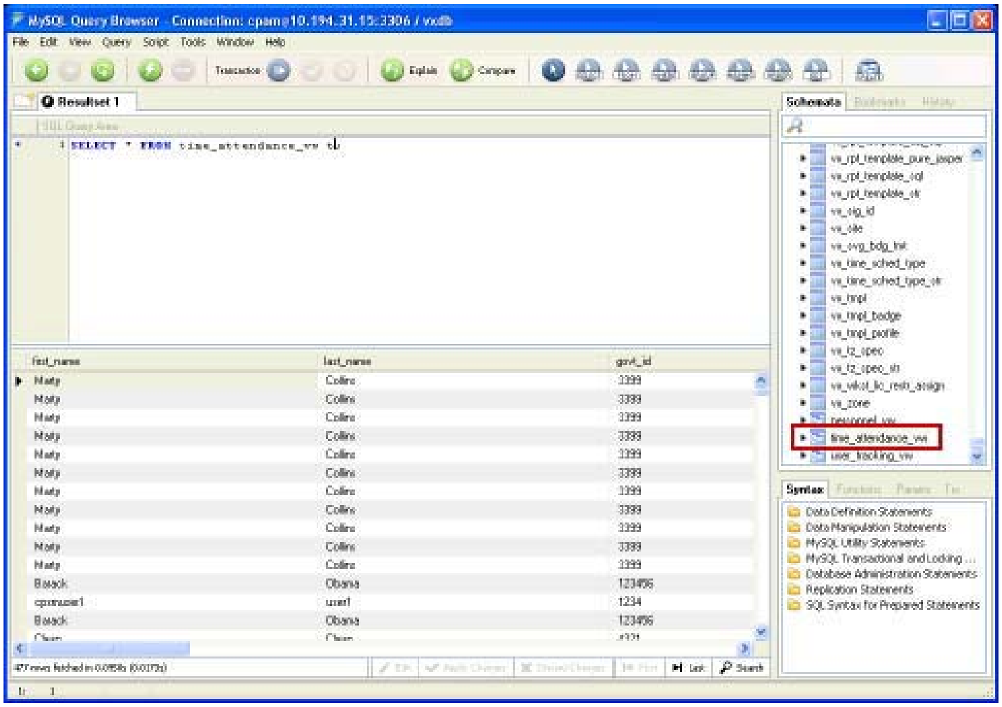
9 rows fetched in 0.0735s (0.0858s)

Time and Attendance

The Time and Attendance view (Figure 14-29) provides information on user entry and exit through the 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 14-29 Time and Attendance



MySQL Query Browser - Connection: cpam@10.194.31.15:3306 / vxdb

```
SELECT * FROM time_attendance_vw tb
```

first_name	last_name	govt_id
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Marty	Collins	3399
Barack	Obama	123456
cpamuser1	user1	1234
Barack	Obama	123456

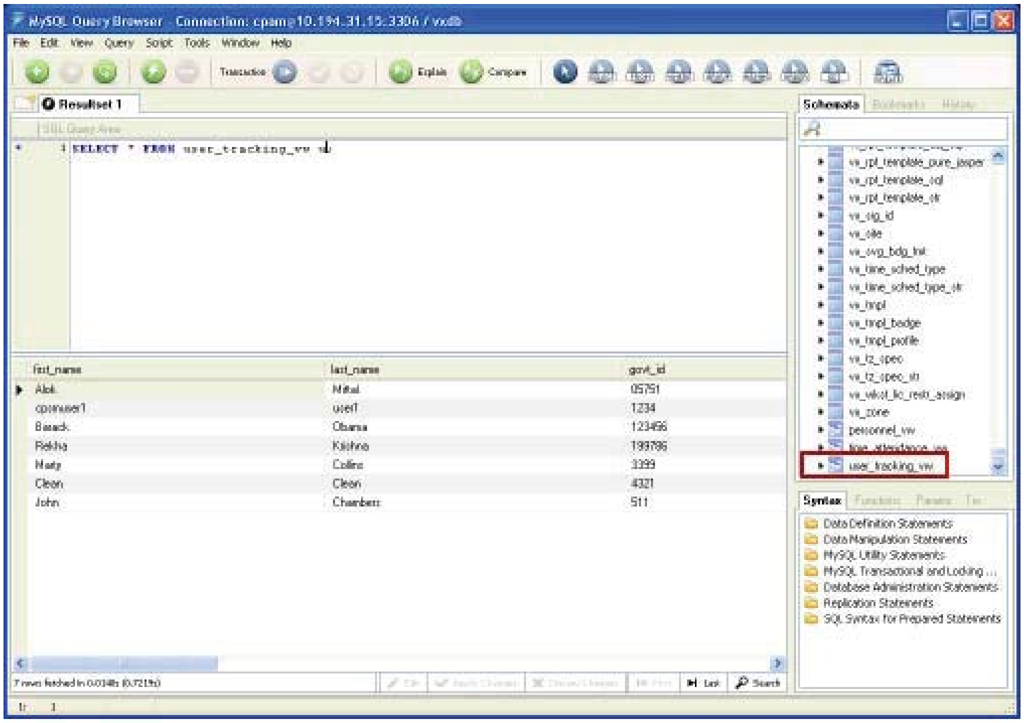
477 rows fetched in 0.0958s (0.0173s)

User Tracking Data

The User Tracking view (Figure 14-30) 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 14-30 User Tracking



MySQL Query Browser - Connection: cpam@10.194.31.15:3306 / vxdb

```
SELECT * FROM user_tracking_vw u
```

first_name	last_name	govt_id
Alok	Mittal	05751
cpamuser1	user1	1234
Barack	Obama	123456
Rekha	Krishna	199786
Marty	Collins	3399
Cleon	Cleon	4321
John	Chambers	511

7 rows fetched in 0.0348s (0.7219s)

CHAPTER 15

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 ICPAM, 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 ICPAM

If the profile enhancement feature is set in the system configuration settings (Logins Settings, page 17-10), 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 ICPAM 2.1. 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:

Changes	New Cisco VSM Camera Driver 7X	New Cisco VSM Camera Driver 7.5X
Configuration Changes	To Setup Cisco VSM the server name, username and password is given.	To Setup Cisco VSM the server name, username and password is not given
Architectural changes	Not Applicable	Not Applicable

Changes	New Cisco VSM Camera Driver 7X	New Cisco VSM Camera Driver 7.5X
Live video Layout	Only single and 4-way layout	Several layout views are available
Location specific video	The user can view videos only of locations and sub-locations that they are assigned.	The user can view videos only of locations and sub-locations that they are assigned.

- In 7X version, if a camera is removed from the VSM configuration then it is deleted completely from ICPAM provided the camera is not associated with any devices, CCTV camera arrangements, or 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 ICPAM, but not removed. We recommend that you do not manually remove or delete cameras from the ICPAM 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 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 ICPAM.

Note Problems may occur when viewing video from analog cameras that use Cisco Stream Manager IP Gateway Encoder CIVS-SGxx. Contact your Identiv support representative for details.

Contents

- Deleting Individual Cameras, page 15-34
- Recording Motion Events from Cisco VSM Cameras, page 15-35

Enabling Video Monitoring

To enable video viewing in ICPAM, 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.

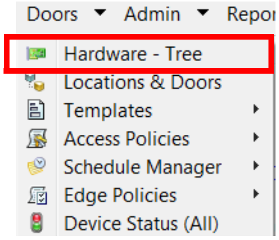
Complete the following instructions to enable video monitoring:

- Configuring the Camera Driver, page 15-4
- Associating Cameras with Doors and Devices, page 15-9
- 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

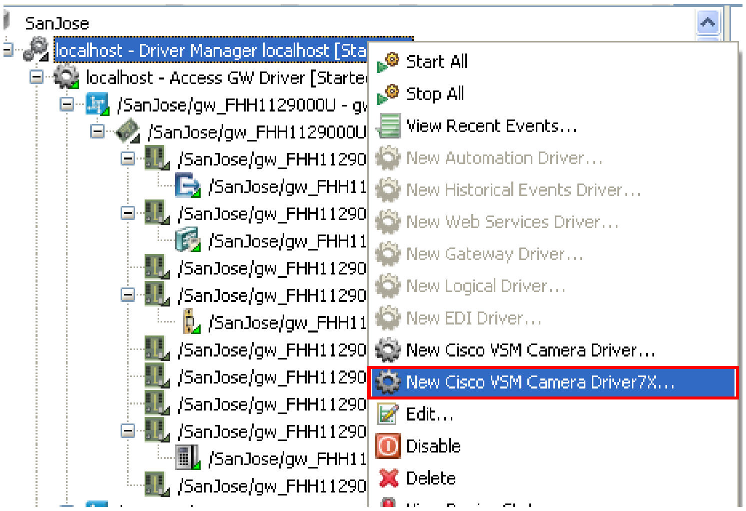
To add the VSM Camera Driver to enable video sharing and playback with the Cisco VSM system:

Step 1 Select **Hardware - Tree** from the **Doors** menu.

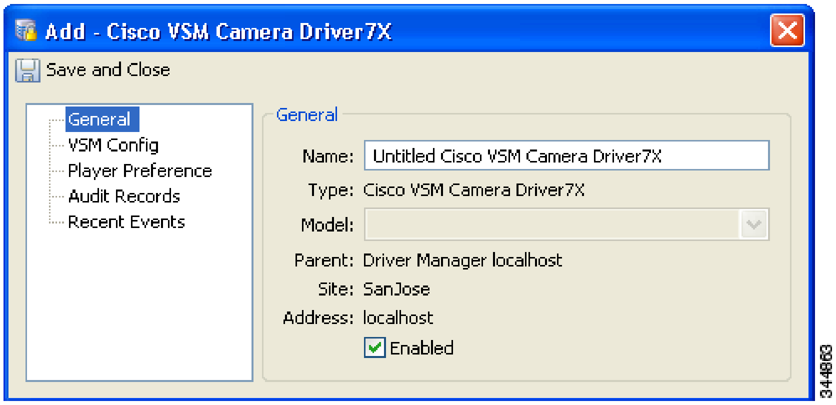


Step 2 Right-click the **Driver Manager** and select the appropriate camera driver version:

- New Cisco VSM Camera Driver
- New Cisco VSM Camera Driver 7X



Step 3 Enter the driver name in the properties window. For example: `Cisco VSM Camera Driver7x`.



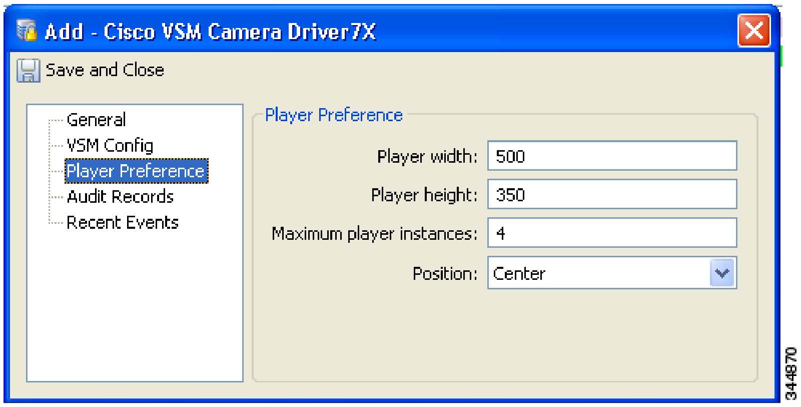
General

Name: Untitled Cisco VSM Camera Driver7X
Type: Cisco VSM Camera Driver7X
Model:
Parent: Driver Manager localhost
Site: SanJose
Address: localhost
☑ Enabled

Note Verify that the **Enabled** check box 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.



Player Preference

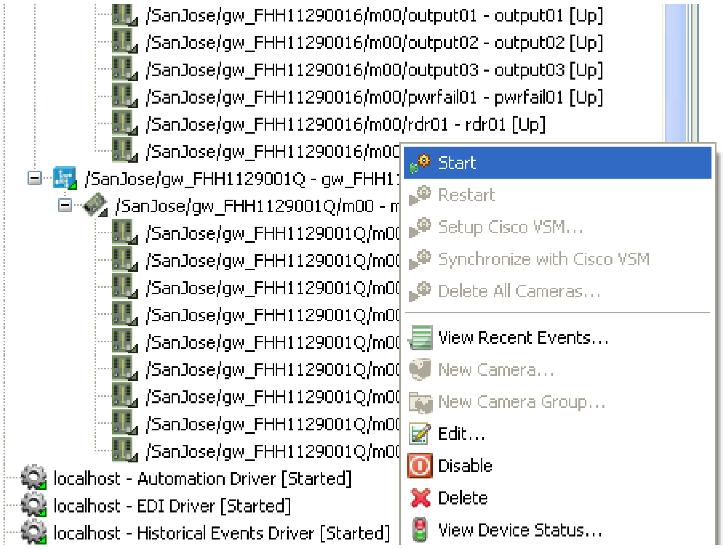
Player width: 500
Player height: 350
Maximum player instances: 4
Position: Center

Tip The VSM Config tab displays VSM server settings. See Note 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.

Step 6 Right-click the **VSM Camera Driver** and select **Start** to enable the ICPAM video features.

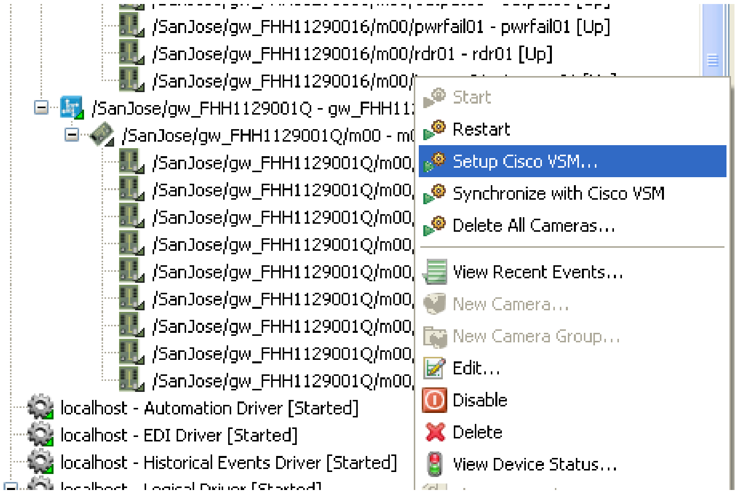


/SanJose/gw_FHH11290016/m00/output01 - output01 [Up]
/SanJose/gw_FHH11290016/m00/output02 - output02 [Up]
/SanJose/gw_FHH11290016/m00/output03 - output03 [Up]
/SanJose/gw_FHH11290016/m00/pwrfail01 - pwrfail01 [Up]
/SanJose/gw_FHH11290016/m00/rdr01 - rdr01 [Up]
/SanJose/gw_FHH11290016/m00
/SanJose/gw_FHH1129001Q - gw_FHH11
/SanJose/gw_FHH1129001Q/m00 - m
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
/SanJose/gw_FHH1129001Q/m00
localhost - Automation Driver [Started]
localhost - EDI Driver [Started]
localhost - Historical Events Driver [Started]

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 VSM**.

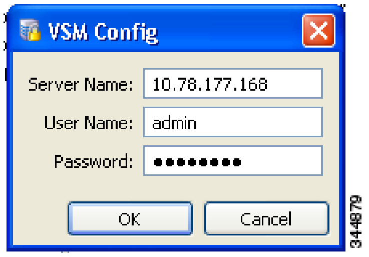


/SanJose/gw_FHH11290016/m00/pwrfail01 - pwrfail01 [Up]
/SanJose/gw_FHH11290016/m00/rdr01 - rdr01 [Up]
/SanJose/gw_FHH11290016/m00/
/SanJose/gw_FHH1129001Q - gw_FHH11
/SanJose/gw_FHH1129001Q/m00 - m0
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
/SanJose/gw_FHH1129001Q/m00,
localhost - Automation Driver [Started]
localhost - EDI Driver [Started]
localhost - Historical Events Driver [Started]
localhost - Logical Driver [Started]

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.



VSM Config

Server Name: 10.78.177.168
User Name: admin
Password: ●●●●●●●●●

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**.

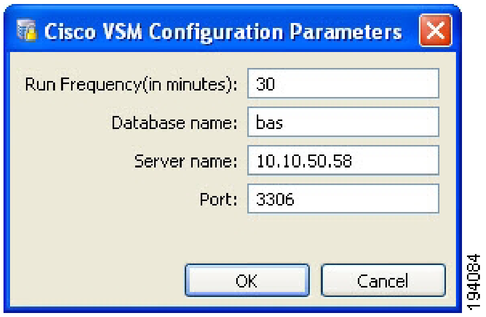
Note Do not change the database name or port number once they are configured.

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`.

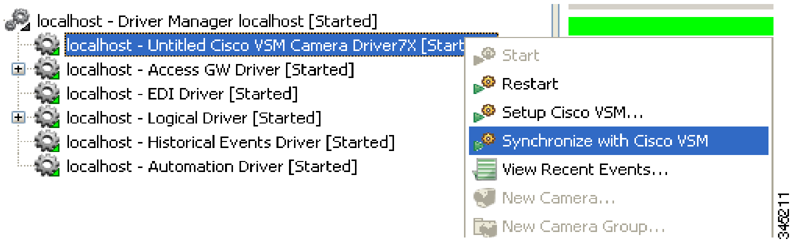
e. Click **OK** to save the changes and close the window.



Cisco VSM Configuration Parameters

Run Frequency(in minutes): 30
Database name: bas
Server name: 10.10.50.58
Port: 3306

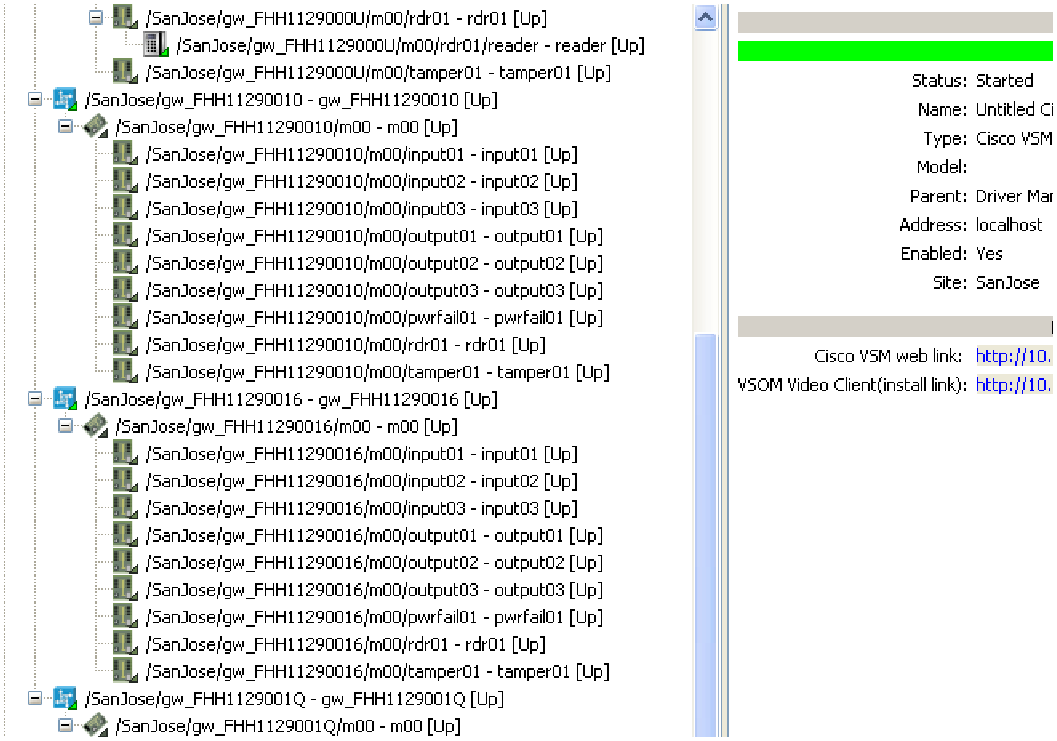
Step 9 Right-click the **VSM Camera Driver** and select **Synchronize with Cisco VSM** to populate ICPAM with the Cisco VSM cameras.



localhost - Driver Manager localhost [Started]
localhost - Untitled Cisco VSM Camera Driver7X [Start
localhost - Access GW Driver [Started]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - Historical Events Driver [Started]
localhost - Automation Driver [Started]
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
View Recent Events...
New Camera...
New Camera Group...
346211

Note For 7x version follow the same step to populate the ICPAM with the Cisco VSM cameras.

Step 10 Verify that the Cisco VSM cameras appear as children of the Camera Driver.



```
/SanJose/gw_FHH1129000U/m00/rdr01 - rdr01 [Up]
    /SanJose/gw_FHH1129000U/m00/rdr01/reader - reader [Up]
/SanJose/gw_FHH1129000U/m00/tamper01 - tamper01 [Up]
/SanJose/gw_FHH11290010 - gw_FHH11290010 [Up]
  /SanJose/gw_FHH11290010/m00 - m00 [Up]
    /SanJose/gw_FHH11290010/m00/input01 - input01 [Up]
    /SanJose/gw_FHH11290010/m00/input02 - input02 [Up]
    /SanJose/gw_FHH11290010/m00/input03 - input03 [Up]
    /SanJose/gw_FHH11290010/m00/output01 - output01 [Up]
    /SanJose/gw_FHH11290010/m00/output02 - output02 [Up]
    /SanJose/gw_FHH11290010/m00/output03 - output03 [Up]
    /SanJose/gw_FHH11290010/m00/pwrfail01 - pwrfail01 [Up]
    /SanJose/gw_FHH11290010/m00/rdr01 - rdr01 [Up]
    /SanJose/gw_FHH11290010/m00/tamper01 - tamper01 [Up]
/SanJose/gw_FHH11290016 - gw_FHH11290016 [Up]
  /SanJose/gw_FHH11290016/m00 - m00 [Up]
    /SanJose/gw_FHH11290016/m00/input01 - input01 [Up]
    /SanJose/gw_FHH11290016/m00/input02 - input02 [Up]
    /SanJose/gw_FHH11290016/m00/input03 - input03 [Up]
    /SanJose/gw_FHH11290016/m00/output01 - output01 [Up]
    /SanJose/gw_FHH11290016/m00/output02 - output02 [Up]
    /SanJose/gw_FHH11290016/m00/output03 - output03 [Up]
    /SanJose/gw_FHH11290016/m00/pwrfail01 - pwrfail01 [Up]
    /SanJose/gw_FHH11290016/m00/rdr01 - rdr01 [Up]
    /SanJose/gw_FHH11290016/m00/tamper01 - tamper01 [Up]
/SanJose/gw_FHH1129001Q - gw_FHH1129001Q [Up]
  /SanJose/gw_FHH1129001Q/m00 - m00 [Up]
```

Status: Started
Name: Untitled Ci
Type: Cisco VSM
Model:
Parent: Driver Mar
Address: localhost
Enabled: Yes
Site: SanJose

Cisco VSM web link: http://10.
VSOM Video Client(install link): http://10.

If the cameras do not appear, see Updating the Camera Inventory, page 15-28.

Note Cameras in ICPAM are organized in the same camera groups as Cisco VSM. In ICPAM, each camera can only appear in one group. In Cisco VSM, cameras can appear in multiple groups.

Note If a camera is deleted from the Cisco VSM configuration, it is disabled in ICPAM, but not removed. We recommend that you do not manually remove or delete cameras from the ICPAM configuration. Use the synchronize command to update the camera inventory.

Note In 7X version, if a camera is removed from the VSM configuration then it is deleted completely from ICPAM provided the camera is not associated with any devices/map/CCTV Camera Arrangements/uncleared Alarms.

Note The ICPAM client must run on Windows 7 platform to view video from the cameras under the 7X driver.

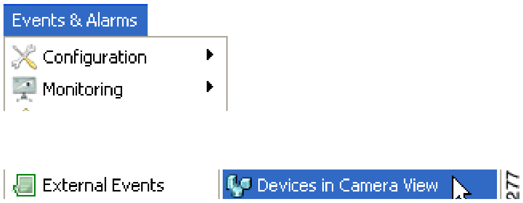
Associating Cameras with Doors and Devices

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.

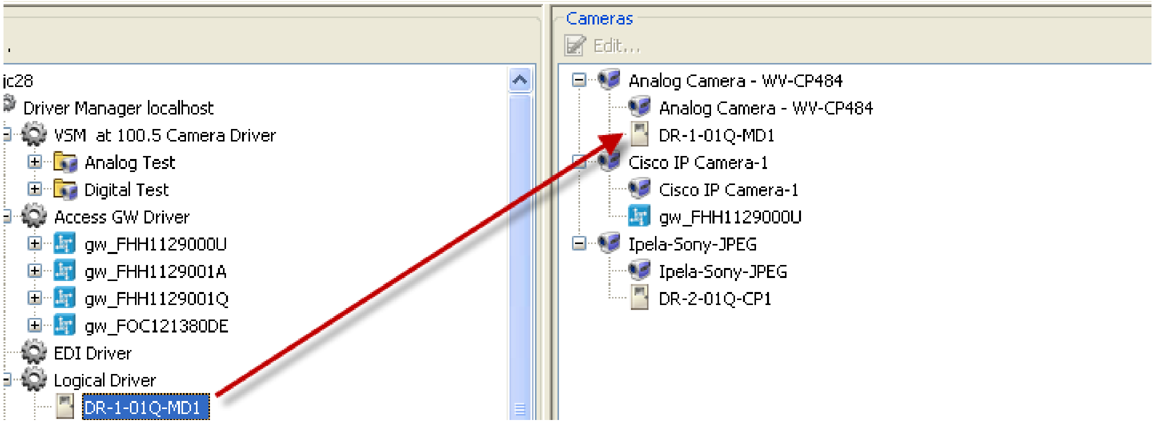
To associate a camera with a door or device, do the following:

Step 1 Select **Devices in Camera View** from the **Events & Alarms** menu, in the **Video** submenu.



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.

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 - Tree windows.

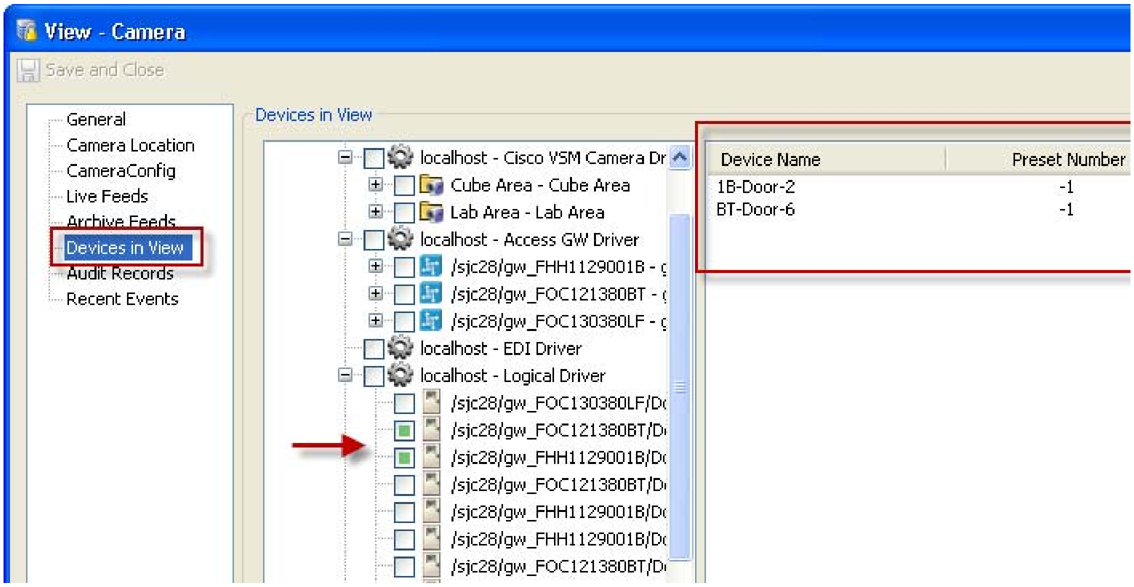
The **Edit - Camera** window opens.

b. Select the **Devices in View** tab.

c. Check the devices to be associated with the camera.

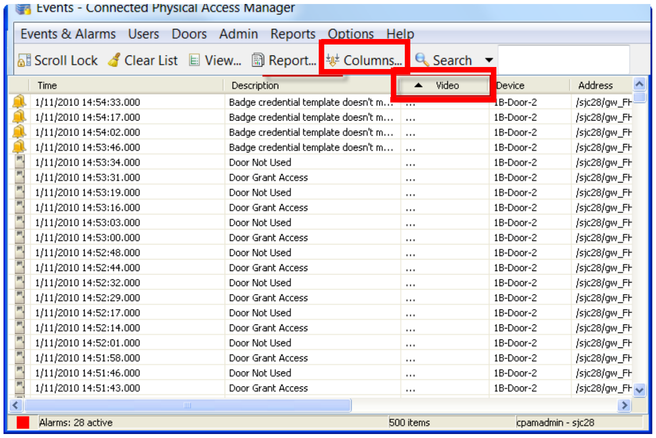
Associated cameras are listed in the far-right table.

d. Click **Save and Close**.



Device Name	Preset Number
1B-Door-2	-1
BT-Door-6	-1

Step 4 (Optional) Exit and relaunch the ICPAM client to ensure the camera associations appear correctly in the Events window.



Time	Description	Video	Device	Address
1/11/2010 14:54:33.000	Badge credential template doesn't m...	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:54:17.000	Badge credential template doesn't m...	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:54:02.000	Badge credential template doesn't m...	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:46.000	Badge credential template doesn't m...	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:34.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:31.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:19.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:16.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:03.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:53:00.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:48.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:44.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:32.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:29.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:17.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:14.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:52:01.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:51:58.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:51:46.000	Door Not Used	...	1B-Door-2	/sjc28/gw_FH
1/11/2010 14:51:43.000	Door Grant Access	...	1B-Door-2	/sjc28/gw_FH

Alarms: 28 active 500 items cpamadmin - sjc28

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.

Tip 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 15-1 Video Surveillance Monitoring Workstation Recommended Baseline Specification

Workstation Attribute	Baseline Specification
OS	Windows 7 64-bit, SP3
CPU	Intel 950 i7 Core - 3.07 GHz
Memory	6 GB DDR3
Graphics	NVIDIA GeForce GTX260 896MB PCIe
Cisco VSOM configuration	VMR mode enabled
Browser	Microsoft Internet Explorer 7
Network connection	Gigabit Ethernet (GigE) network connection required
Display configuration	Single monitor

For related information, see *Video Surveillance Monitoring Workstation Recommended Baseline Specification*, which is available here:

http://www.cisco.com/c/en/us/support/physical-security/video-surveillance-manager/products-technical-reference-list.html

Installing the Cisco VSOM Video Client Desktop Application

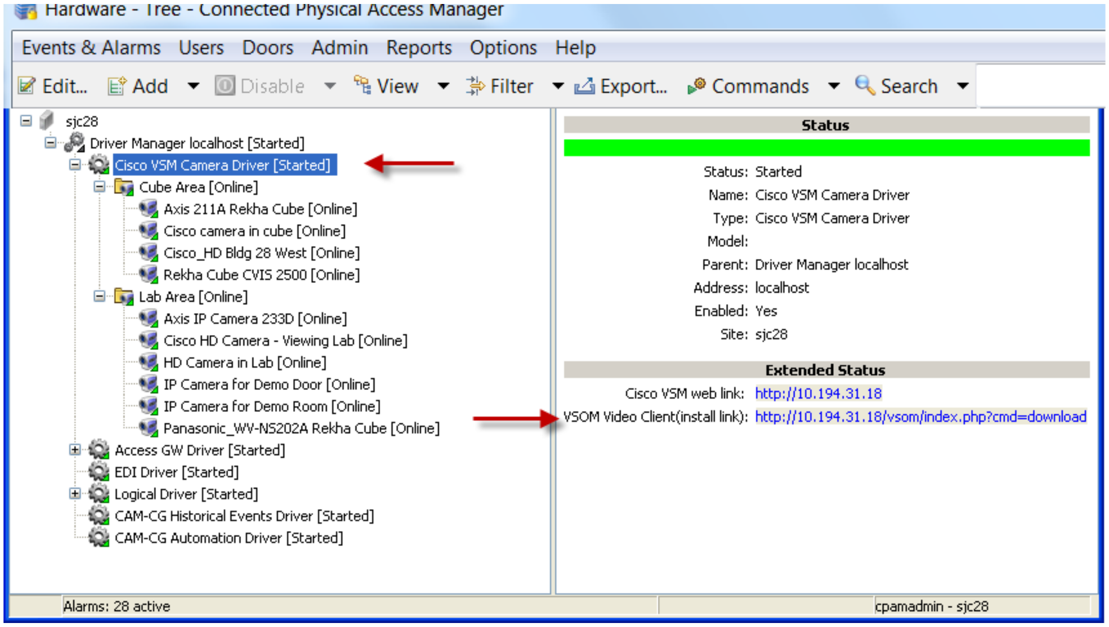
The Cisco VSOM Video Client includes the ActiveX controls required for event video viewing. Install the player to enable the video features, or anytime the Cisco VSM server is upgraded. When the player is installed, any existing version is automatically deinstalled.

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**.

Figure 15-1 Hardware Tree ICPAM



```
sjc28
  Driver Manager localhost [Started]
    Cisco VSM Camera Driver [Started]
      Cube Area [Online]
        Axis 211A Rekha Cube [Online]
        Cisco camera in cube [Online]
        Cisco_HD Bldg 28 West [Online]
        Rekha Cube CVIS 2500 [Online]
      Lab Area [Online]
        Axis IP Camera 233D [Online]
        Cisco HD Camera - Viewing Lab [Online]
        HD Camera in Lab [Online]
        IP Camera for Demo Door [Online]
        IP Camera for Demo Room [Online]
        Panasonic_WV-NS202A Rekha Cube [Online]
    Access GW Driver [Started]
    EDI Driver [Started]
    Logical Driver [Started]
    CAM-CG Historical Events Driver [Started]
    CAM-CG Automation Driver [Started]
```

Status

Status: Started
Name: Cisco VSM Camera Driver
Type: Cisco VSM Camera Driver
Model:
Parent: Driver Manager localhost
Address: localhost
Enabled: Yes
Site: sjc28

Extended Status

Cisco VSM web link: http://10.194.31.18
VSOM Video Client(install link): http://10.194.31.18/vsom/index.php?cmd=download

Alarms: 28 active
cpamadmin - sjc28

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 - Tree module) and select **View Live Video**.

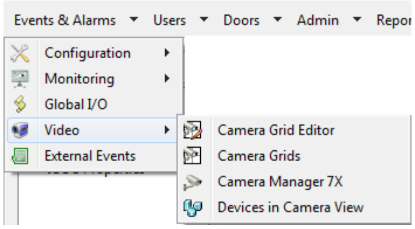
This section includes the following instructions:

- Viewing Live Video in a Grid Arrangement -VSM 6X, page 15-13
- Viewing Video for an Event, page 15-20

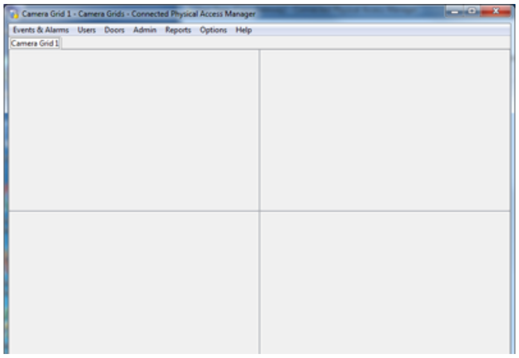
Viewing Live Video in a Grid Arrangement -VSM 6X

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.

Step 1 Select **Camera Grids** from the **Events & Alarms** menu, in the **Video** submenu.



The Camera Grid window appears.


Camera Grid 1 - Camera Grids - Connected Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Camera Grid 1

Only those grids that have been previously created using the Camera Grid Editor appear in this window. For more on the Camera Grid Editor, refer to Camera Grid Editor, page 15-15.

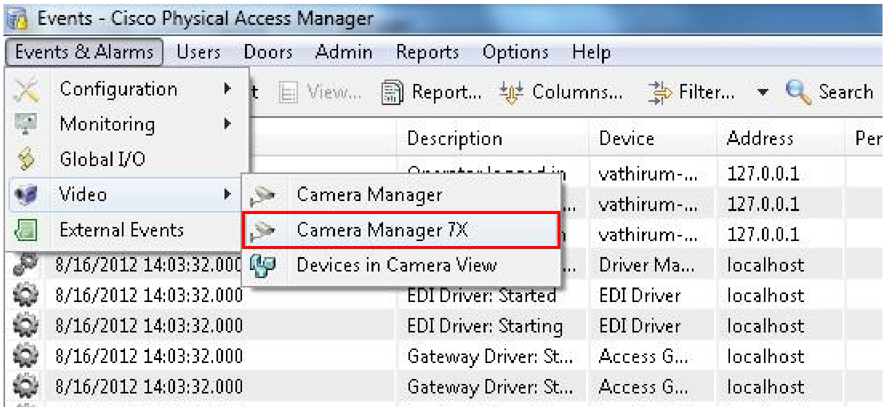
Step 2 From the available grid tabs, select the tab containing the video feeds you need to view.

Viewing Live Video in a Grid Arrangement -VSM 7X

This video view is not supported unless the necessary VSM 7X drivers are installed.

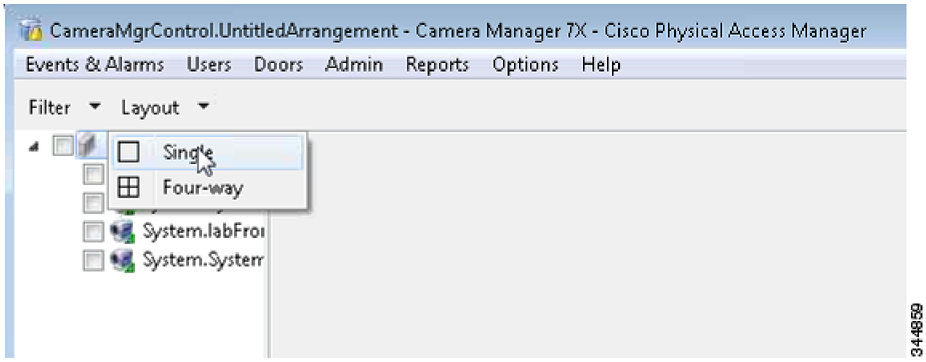
To view live video in a grid arrangement while using **VSM Camera Driver 7X**, do the following:

Step 1 Select **Camera Manager 7X** from the **Events & Alarms** menu, in the **Video** submenu.

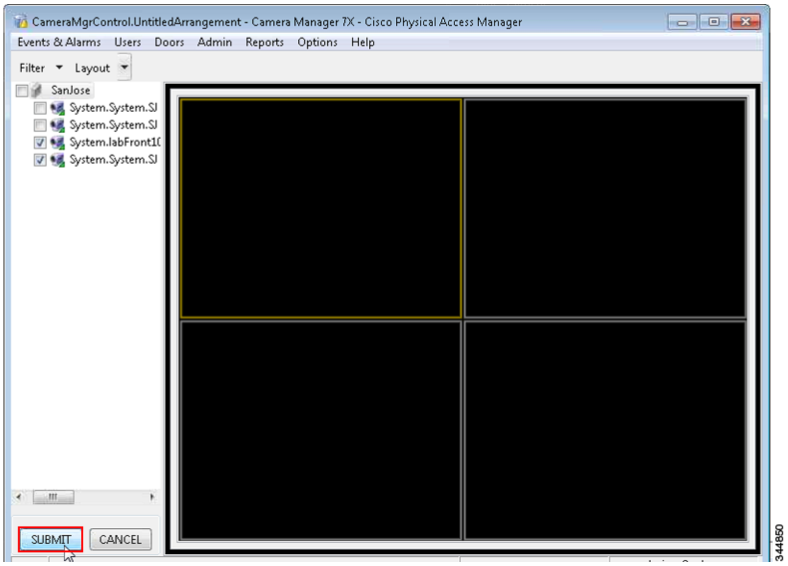


	Description	Device	Address	Per
	Operator logged in	vathirum-...	127.0.0.1	
	...	vathirum-...	127.0.0.1	
		vathirum-...	127.0.0.1	
8/16/2012 14:03:32.000	...	Driver Ma...	localhost	
8/16/2012 14:03:32.000	EDI Driver: Started	EDI Driver	localhost	
8/16/2012 14:03:32.000	EDI Driver: Starting	EDI Driver	localhost	
8/16/2012 14:03:32.000	Gateway Driver: St...	Access G...	localhost	
8/16/2012 14:03:32.000	Gateway Driver: St...	Access G...	localhost	

Step 2 Click the **Layouts** menu and select a layout that includes the number of cameras you want to view.



Step 3 Select the cameras and click **SUBMIT** to view the videos of the selected cameras.


CameraMgrControl.UntitledArrangement - Camera Manager 7X - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Filter
Layout
SanJose
System.System.SJ
System.System.SJ
System.labFront1(
System.System.SJ
SUBMIT
CANCEL
344850

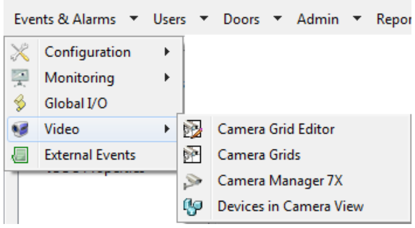
Note Based on the system configuration settings (see Logins Settings, page 17-10), only cameras that are assigned to your user profile, location, and sub location will be listed for selection.

Camera Grid Editor

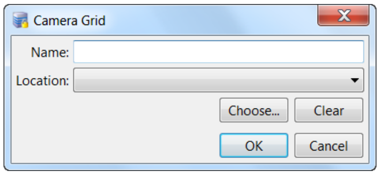
Use the camera grid editor to create multi-frame screens from which to monitor live video. Later, you can recall the created grids to using the camera grid feature as detailed in Viewing Live Video in a Grid Arrangement -VSM 6X, page 15-13 and Viewing Live Video in a Grid Arrangement -VSM 7X, page 15-14.

To use the Camera Grid Editor:

Step 1 Select **Camera Grid Editor** from the **Events & Alarms** menu, in the **Video** submenu.



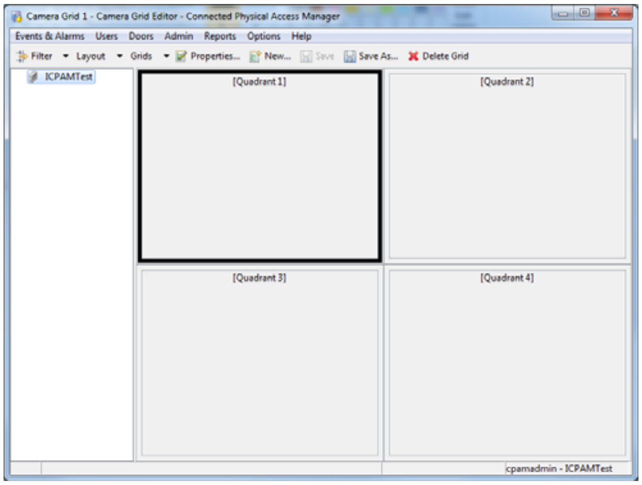
The Camera Grid window appears.



Step 2 Enter a name for this new grid, then in the 'Location' pull-down field, select a location where the video for this grid originates, and click **OK**.

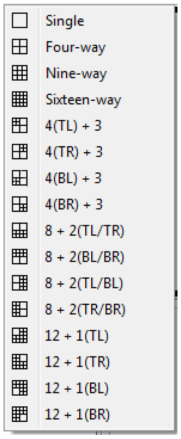
If required, click **Choose...** to browse for the required location.

The Camera Grid Editor for the new grid appears.



By default, the grid contains four frames.

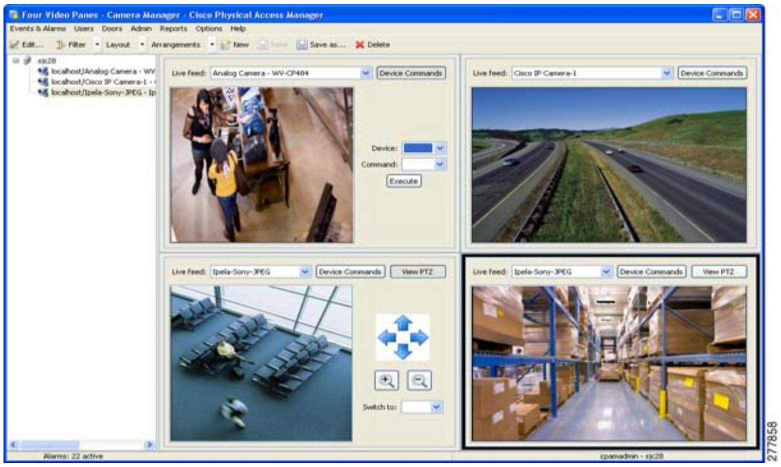
Step 3 To change the number of frames in this grid, click the **Layouts** menu and select a layout that includes the number of cameras you want to view.



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.



Live feed: Analog Camera - WV-CP484

Live feed: Cisco IP Camera-1

Live feed: Ipela-Sony-JPEG

Live feed: Ipela-Sony-JPEG

Tip To remove the camera, click and drag the title bar of the camera screen off the grid.

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.

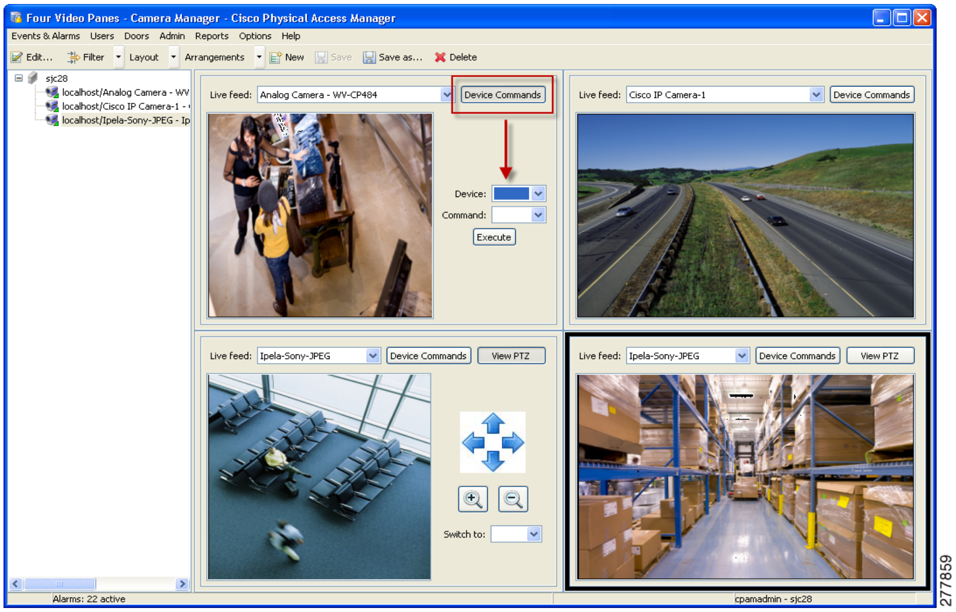
b. Select a **Device**.

c. Select a **Command**.

Tip The commands are also available by right-clicking the camera name in the Hardware - Tree module.

d. Click **Execute**.

e. If additional options are available, select an option from the pop-up window and click **OK**.



sjc28
localhost/Analog Camera - WV
localhost/Cisco IP Camera-1 -
localhost/Ipela-Sony-JPEG - Ip

Live feed: Analog Camera - WV-CP484
Device:
Command:

Live feed: Cisco IP Camera-1

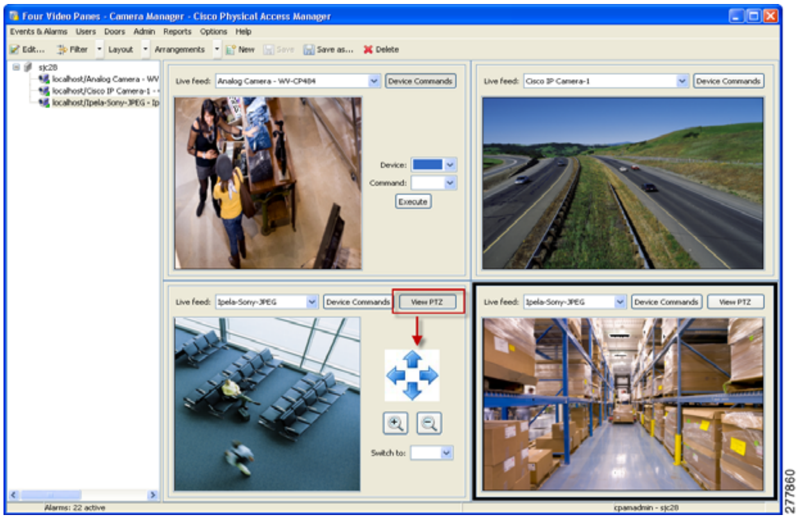
Live feed: Ipela-Sony-JPEG
Switch to:

Live feed: Ipela-Sony-JPEG

Alarms: 22 active
cpamadmin - sjc28

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.



sjc28
localhost/Analog Camera - WV
localhost/Cisco IP Camera-1 -
localhost/Ipela-Sony-JPEG - Ip

Live feed: Analog Camera - WV-CP484
Device:
Command:

Live feed: Cisco IP Camera-1

Live feed: Ipela-Sony-JPEG
Switch to:

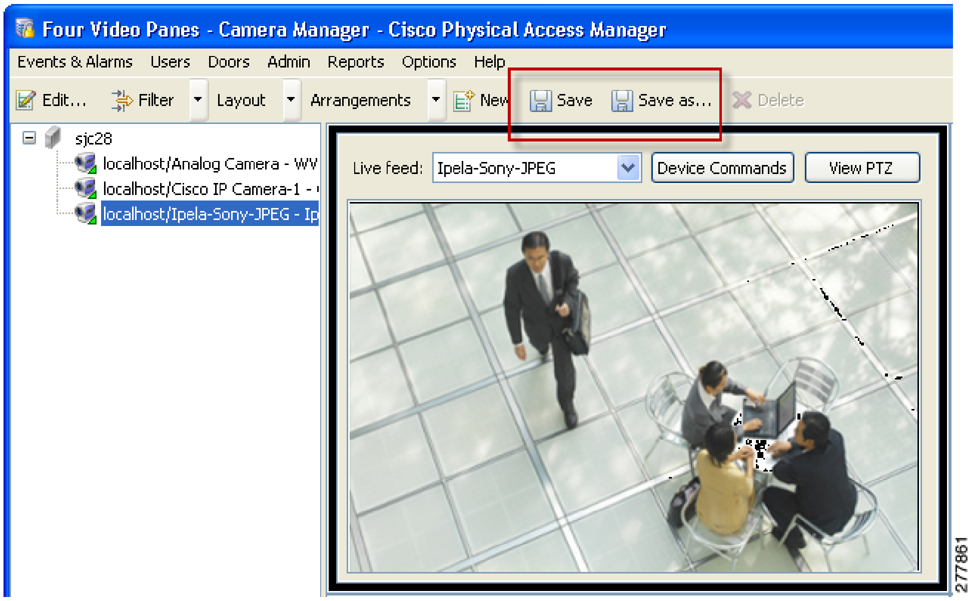
Live feed: Ipela-Sony-JPEG

Alarms: 22 active
cpamadmin - sjc28

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**.

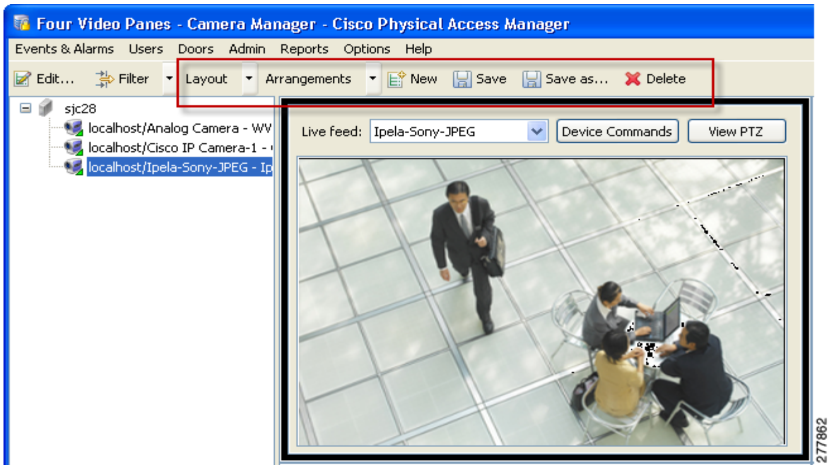
b. Enter the arrangement name and click **OK**. The layout name appears in the window title bar.


Four Video Panes - Camera Manager - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Filter Layout Arrangements New Save Save as... Delete
sjc28
localhost/Analog Camera - WV
localhost/Cisco IP Camera-1 -
localhost/Ipela-Sony-JPEG - Ip
Device Commands
View PTZ
277861

Live feed: Ipela-Sony-JPEG

Step 8 (Optional) Create or modify additional arrangements using the menu bar controls:

- **Layout**: selects a blank layout to display video from one or more cameras.
- **Grids**: selects one of the existing grids.
- **Properties**: change the definition of the currently selected grid.
- **New**: creates a new screen of views and cameras.
- **Save**: saves the current view as an Arrangement.
- **Save As**: saves the Arrangement under a different name.
- **Delete**: deletes the current layout.


Four Video Panes - Camera Manager - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Filter Layout Arrangements New Save Save as... Delete
sjc28
localhost/Analog Camera - WV
localhost/Cisco IP Camera-1 -
localhost/Ipela-Sony-JPEG - Ip
Device Commands
View PTZ
277862

Live feed: Ipela-Sony-JPEG

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

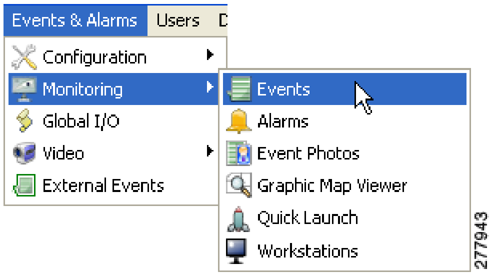
- In the main Events window, you can display a Video column to signify if a camera is associated with a door or device. Click **Columns** in the menu bar, select **Video**, and click **OK**. The Video column displays three dots if a camera is associated with the door or device. To ensure the stars appear correctly, you must exit and relaunch the ICPAM 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** submenu.
  - 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 - Tree 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 procedure.

Step 1 Select **Events** from the **Events & Alarms** > **Monitoring** 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.

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:

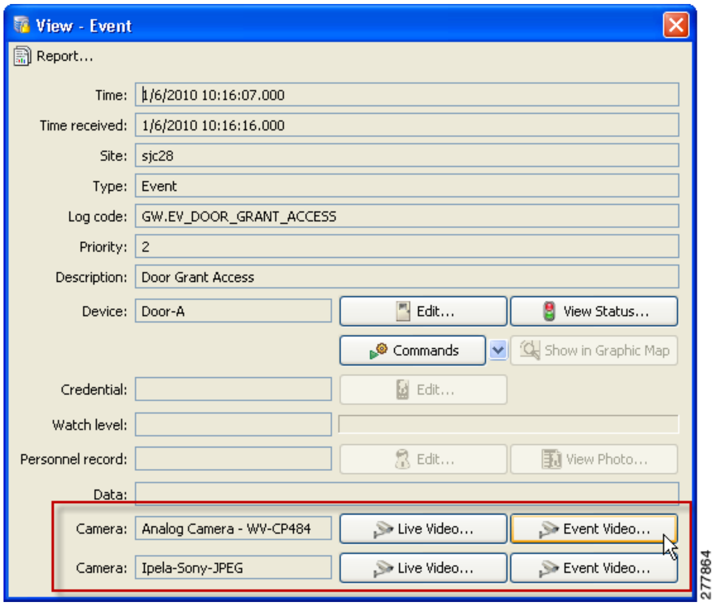
- **View Live Video**—view live video from the camera associated with the event.
- **View Event Video**—view the video archive for the event.
- **View Live and Event Video**—open both live and archive video windows.
- **Show Camera Arrangement**—displays all camera arrangements that include the camera 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.

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**.



View - Event

Time: 1/6/2010 10:16:07.000

Time received: 1/6/2010 10:16:16.000

Site: sjc28

Type: Event

Log code: GW.EV_DOOR_GRANT_ACCESS

Priority: 2

Description: Door Grant Access

Device: Door-A

Credential:

Watch level:

Personnel record:

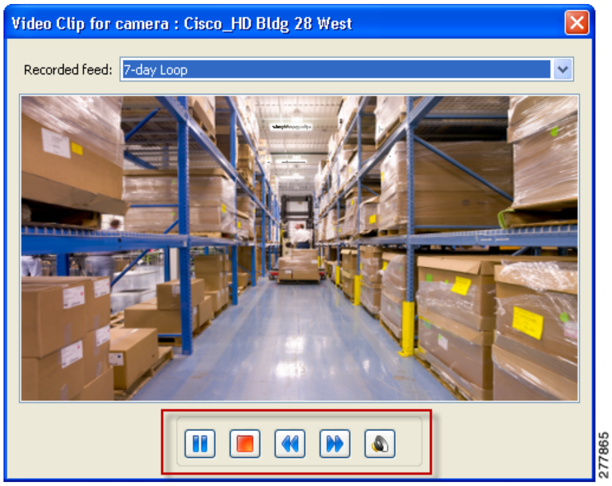
Data:

Camera: Analog Camera - WV-CP484

Camera: Ipela-Sony-JPEG

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.



Video Clip for camera : Cisco_HD Bldg 28 West

Recorded feed: 7-day Loop

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.

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

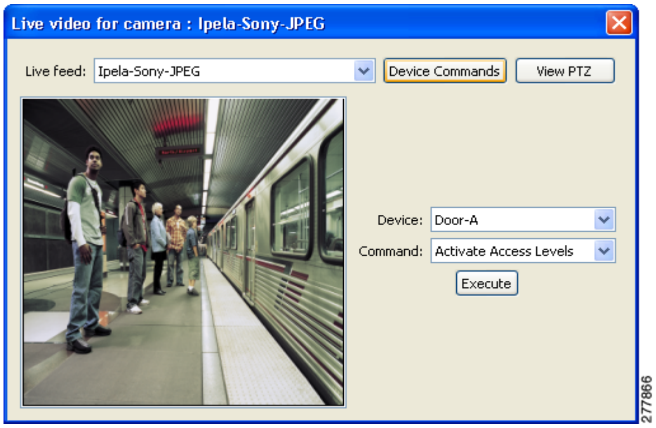
a. Click **Device Commands** to show (or hide) the controls.

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**.


Live video for camera : Ipela-Sony-JPEG
Live feed: Ipela-Sony-JPEG
Device Commands
View PTZ
Device: Door-A
Command: Activate Access Levels
Execute
277866

Tip The commands are the same commands available by right-clicking the device in the Hardware - Tree 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.

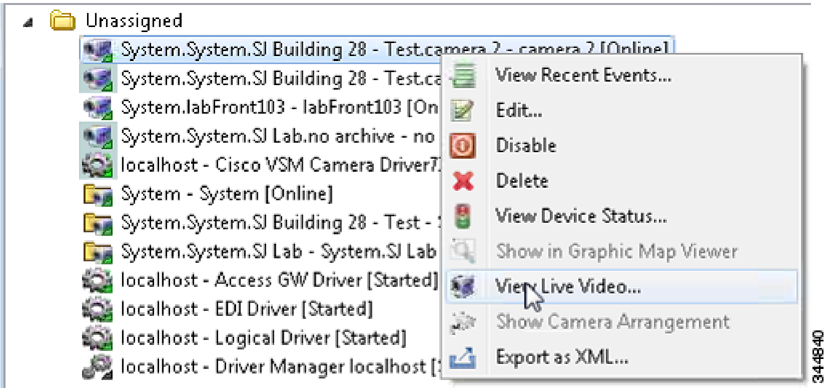
  or

- Select a PTZ preset from the **Switch to** drop-down menu.

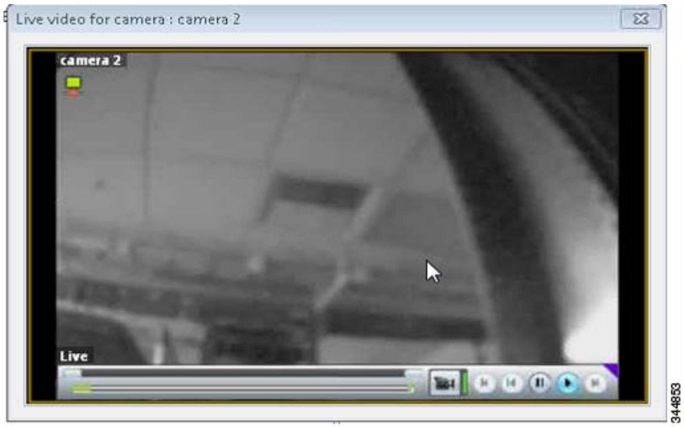
Viewing Event on a VSM Camera Driver 7X

To view events on a VSM Camera Driver 7X, do the following procedure.

Step 1 From the hardware tree view, right-click the VSM camera and select **View Live Video.**


Unassigned
System.System.SJ Building 28 - Test.camera 2 - camera 2 [Online]
System.System.SJ Building 28 - Test.ca
System.labFront103 - labFront103 [On
System.System.SJ Lab.no archive - no
localhost - Cisco VSM Camera Driver7
System - System [Online]
System.System.SJ Building 28 - Test -
System.System.SJ Lab - System.SJ Lab
localhost - Access GW Driver [Started]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - Driver Manager localhost [
View Recent Events...
Edit...
Disable
Delete
View Device Status...
Show in Graphic Map Viewer
View Live Video...
Show Camera Arrangement
Export as XML...
344840

The live video window opens.



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:

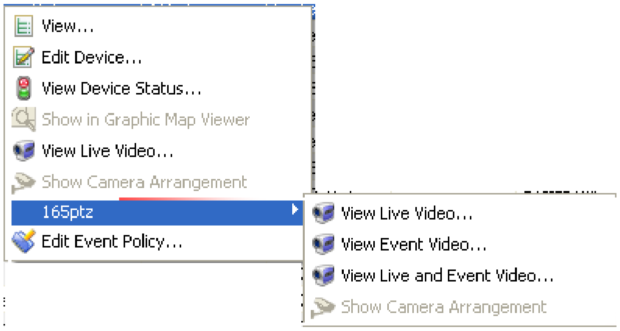
a. Right-click an event or alarm entry.

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).

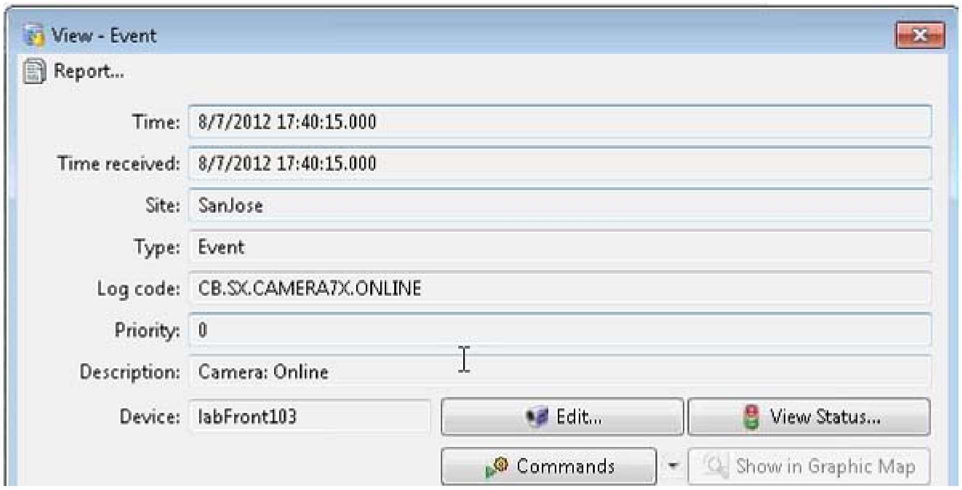


Tip The video and camera options appear only if video is available for that event.

Step 2 (Optional) You can also select the video options from the event detail window.

a. Double-click an event or alarm entry.

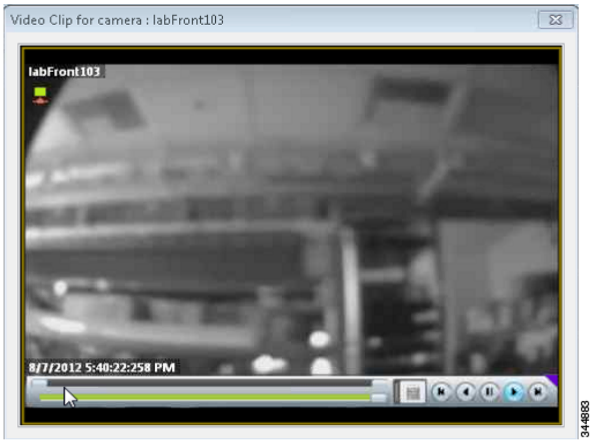
b. In the detail window, click a viewing option: **Live Video**, **Event Video**, **Live and Event Video**, or **Arrangement**.



Time: 8/7/2012 17:40:15.000
Time received: 8/7/2012 17:40:15.000
Site: SanJose
Type: Event
Log code: CB.SX.CAMERA7X.ONLINE
Priority: 0
Description: Camera: Online
Device: labFront103

Tip The video and camera options appear only if video is available for that event.

Step 3 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.

If this is an event video, a time bar is displayed.

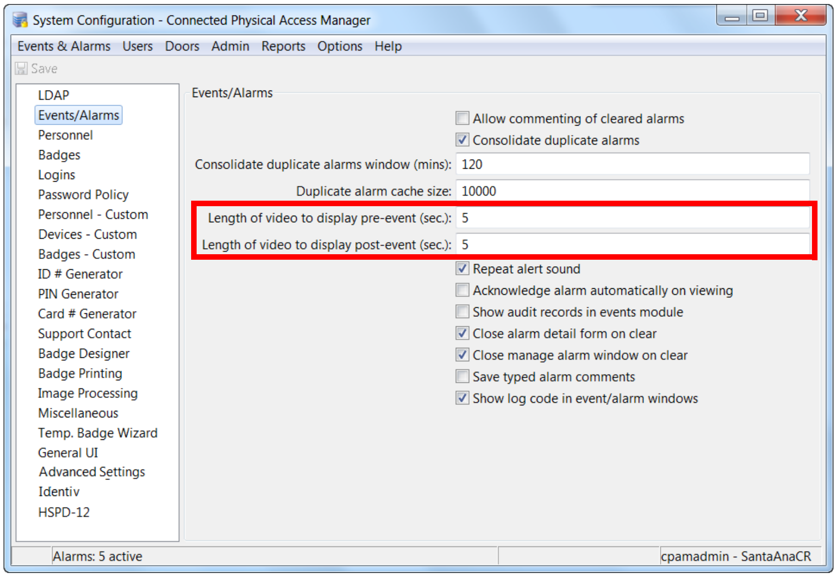
Defining the Duration of Event Video Recording

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** submenu.

Figure 15-2 System Configuration Events/Alarm Window



Events/Alarms

□ Allow commenting of cleared alarms
☑ Consolidate duplicate alarms

Consolidate duplicate alarms window (mins): 120
Duplicate alarm cache size: 10000
Length of video to display pre-event (sec.): 5
Length of video to display post-event (sec.): 5

☑ Repeat alert sound
□ Acknowledge alarm automatically on viewing
□ Show audit records in events module
☑ Close alarm detail form on clear
☑ Close manage alarm window on clear
□ Save typed alarm comments
☑ Show log code in event/alarm windows

Step 2 Enter the following:

Length of video to display pre-event	The number of seconds of video that are included before the event occurred.
Length of video to display post-event	The number of seconds of video that are included after an event occurs.

Step 3 Click **Save**.

Step 4 Log out and log back in to the ICPAM 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 15-34

Updating the Camera Inventory

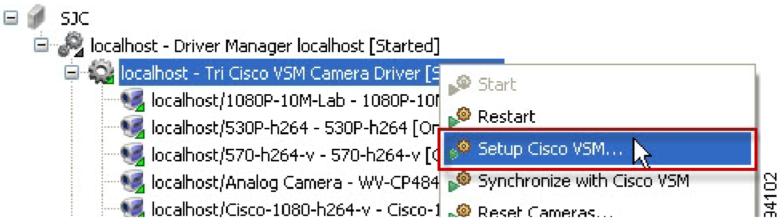
The list of available Cisco VSM cameras is automatically updated as cameras are added or removed from the Cisco VSM system. In most situations, users do not need to update or manage the camera inventory. However, if the camera list is not accurate, do one of the following, in the order shown:

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 ICPAM, but not removed. We recommend that you do not manually remove or delete cameras from the ICPAM configuration. Use the **Synchronize with Cisco VSM** command to update the camera inventory.

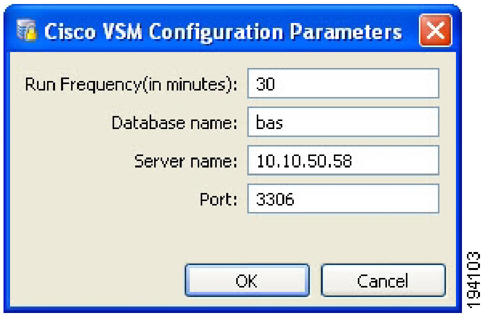
Step 1 Revise the time span between automatic synchronization:

a. Right-click the **Cisco VSM Camera Driver** and select **Setup Cisco VSM**.


SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [S
localhost/1080P-10M-Lab - 1080P-10
localhost/530P-h264 - 530P-h264 [Or
localhost/570-h264-v - 570-h264-v [
localhost/Analog Camera - WV-CP484
localhost/Cisco-1080-h264-v - Cisco-1
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
Reset Cameras...
194102

b. Enter the **Run Frequency (in minutes)**: this defines the time between synchronization. Cameras added or removed from Cisco VSM are updated in ICPAM. 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.

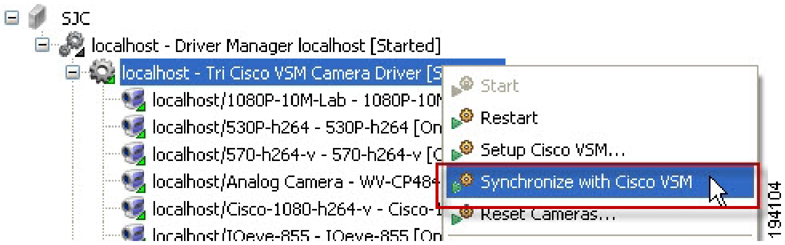

Cisco VSM Configuration Parameters

Run Frequency(in minutes): 30
Database name: bas
Server name: 10.10.50.58
Port: 3306

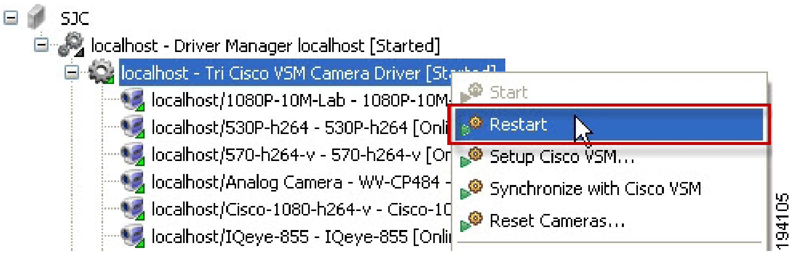
Tip These fields are disabled if the camera driver was previously set up and includes cameras.

Step 2 Right-click the **Cisco VSM Camera Driver** and select **Synchronize with Cisco VSM**.

This command manually synchronizes ICPAM with the Cisco VSM inventory.


SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [S
localhost/1080P-10M-Lab - 1080P-10M
localhost/530P-h264 - 530P-h264 [On
localhost/570-h264-v - 570-h264-v [O
localhost/Analog Camera - WV-CP48
localhost/Cisco-1080-h264-v - Cisco-1
localhost/IQeye-855 - IQeye-855 [On
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
Reset Cameras...
194104

Step 3 If the camera inventory is still not correct, restart the camera driver: right-click the **Cisco VSM Camera Driver** and select **Restart**.

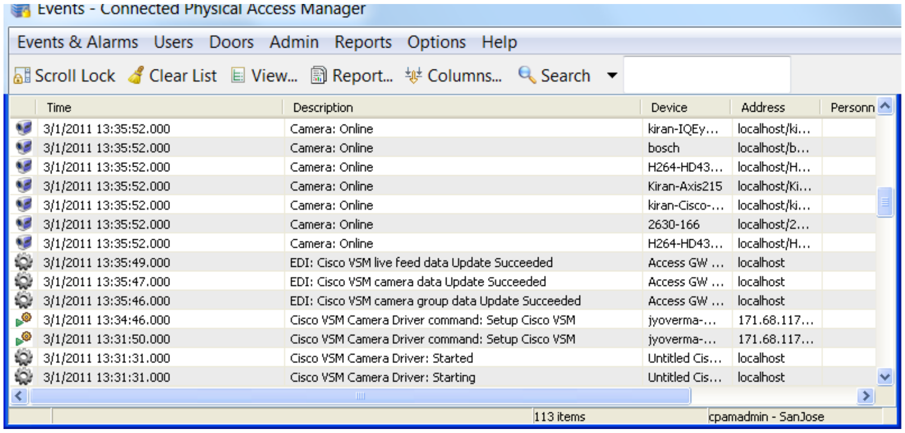

SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [Started]
localhost/1080P-10M-Lab - 1080P-10M
localhost/530P-h264 - 530P-h264 [Onli
localhost/570-h264-v - 570-h264-v [On
localhost/Analog Camera - WV-CP484
localhost/Cisco-1080-h264-v - Cisco-10
localhost/IQeye-855 - IQeye-855 [Onli
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
Reset Cameras...
194105

Step 4 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 successful:

- *archive data feed*
- *live data feed*
- *camera data feed*



Time	Description	Device	Address	Personn
3/1/2011 13:35:52.000	Camera: Online	kiran-IQEy...	localhost/ki...	
3/1/2011 13:35:52.000	Camera: Online	bosch	localhost/b...	
3/1/2011 13:35:52.000	Camera: Online	H264-HD43...	localhost/H...	
3/1/2011 13:35:52.000	Camera: Online	Kiran-Axis215	localhost/Ki...	
3/1/2011 13:35:52.000	Camera: Online	kiran-Cisco-...	localhost/ki...	
3/1/2011 13:35:52.000	Camera: Online	2630-166	localhost/2...	
3/1/2011 13:35:52.000	Camera: Online	H264-HD43...	localhost/H...	
3/1/2011 13:35:49.000	EDI: Cisco VSM live feed data Update Succeeded	Access GW ...	localhost	
3/1/2011 13:35:47.000	EDI: Cisco VSM camera data Update Succeeded	Access GW ...	localhost	
3/1/2011 13:35:46.000	EDI: Cisco VSM camera group data Update Succeeded	Access GW ...	localhost	
3/1/2011 13:34:46.000	Cisco VSM Camera Driver command: Setup Cisco VSM	jyoverma-...	171.68.117...	
3/1/2011 13:31:50.000	Cisco VSM Camera Driver command: Setup Cisco VSM	jyoverma-...	171.68.117...	
3/1/2011 13:31:31.000	Cisco VSM Camera Driver: Started	Untitled Cis...	localhost	
3/1/2011 13:31:31.000	Cisco VSM Camera Driver: Starting	Untitled Cis...	localhost	

113 items cpamadmin - SanJose

Step 5 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 ICPAM cameras and downloads a new, updated list from the Cisco VSM server.

Deleting the cameras does the following in ICPAM.

- Removes the Cisco VSM server configuration.
- Removes the history of all cameras from the ICPAM database.
- Deletes all events and audit records for the cameras.
- Deletes the entire camera inventory.

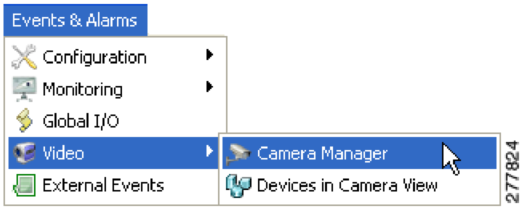
Note To successfully reset the camera database, you must remove all camera associating in the Camera Manager and Graphic Maps, as described in the following instructions.

To delete all cameras from ICPAM and reload the camera inventory from the Cisco VSM server, do the following:

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** submenu.

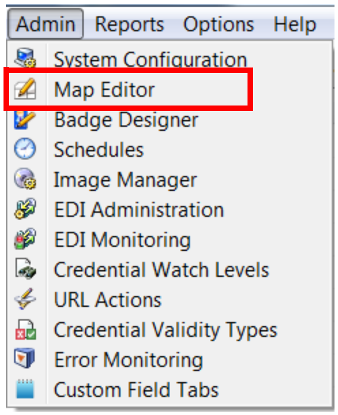
b. Select each arrangement, and click and drag the title bar of each camera off the grid.



Tip You can also delete the arrangement to remove the camera references.

c. Click **Save**.

d. Select **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:

- Viewing Live Video in a Grid Arrangement -VSM 6X, page 15-13.
- Map Editor, page 12-50.

Step 2 Do the following:

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 **ICPAM Settings** submenu.

f. Select the check-box for **Display Delete All Cameras command on the camera driver**.

g. Select the **Miscellaneous** submenu.

h. Select the check-box for **Allow deletion of devices with events**. This allows cameras with associated events to be deleted from ICPAM.

i. Click **Save**.

j. To activate the change, stop and then restart the ICPAM server. See Using the Web Admin Menus, Commands and Options, page 2-18 for instructions.

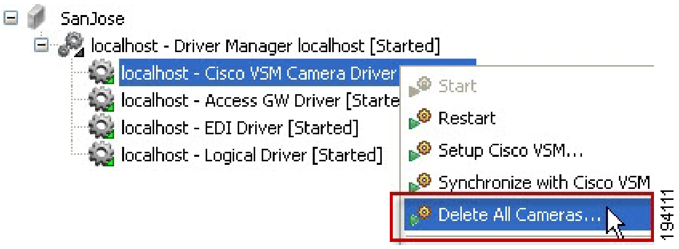
Step 3 Delete the cameras from ICPAM:

a. Open the Hardware - Tree module.

b. Right-click the Cisco VSM camera driver.

c. Select the **Delete All Cameras** command.

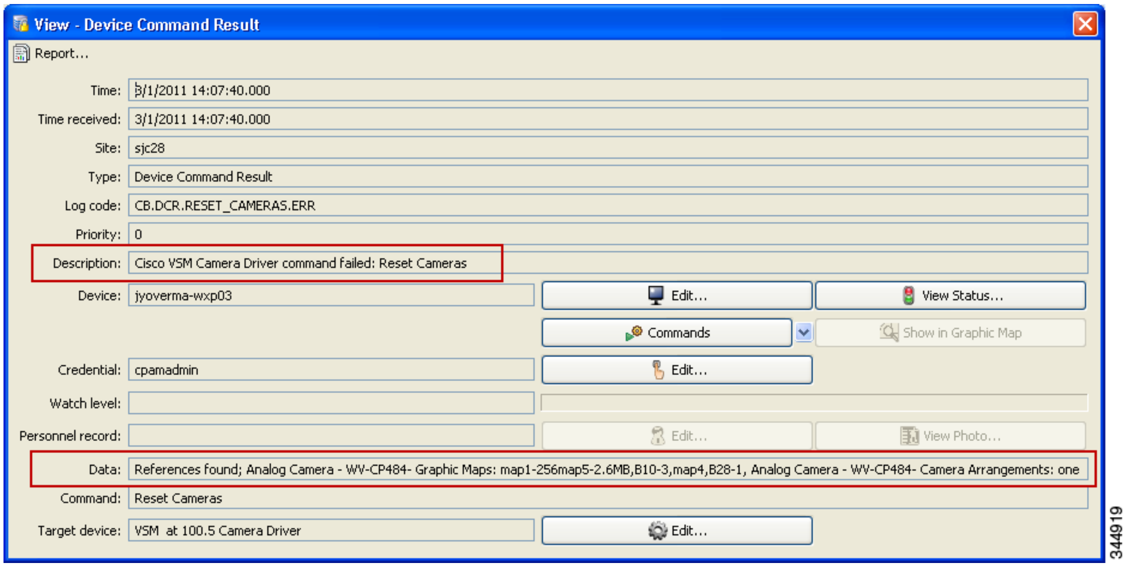
d. Click **OK** when the warning message appears. All events, alarms and audit messages for the cameras will be deleted.


SanJose
localhost - Driver Manager localhost [Started]
localhost - Cisco VSM Camera Driver
localhost - Access GW Driver [Starte
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
Delete All Cameras...
194111

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 substep d.
- 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- s: Graphic Maps: map1-256map5-2.6MB,B10-3, map4,B28-1, Analog Camera - WV-CP484- Camera Arrangements: one."


View - Device Command Result

Report...

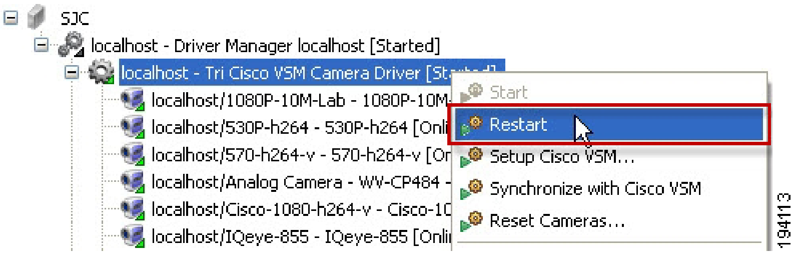
Time: 3/1/2011 14:07:40.000
Time received: 3/1/2011 14:07:40.000
Site: sjc28
Type: Device Command Result
Log code: CB.DCR.RESET_CAMERAS.ERR
Priority: 0
Description: Cisco VSM Camera Driver command failed: Reset Cameras
Device: jyoverma-wxp03
Credential: cpamadmin
Watch level:
Personnel record:
Data: References found; Analog Camera - WV-CP484- Graphic Maps: map1-256map5-2.6MB,B10-3,map4,B28-1, Analog Camera - WV-CP484- Camera Arrangements: one
Command: Reset Cameras
Target device: VSM at 100.5 Camera Driver

  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 substep j..

Step 5 After the **Delete Cameras** command is successful, restart the camera driver: right-click the **Cisco VSM Camera Driver** and select **Restart**.


SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [Started]
localhost/1080P-10M-Lab - 1080P-10M
localhost/530P-h264 - 530P-h264 [Onli
localhost/570-h264-v - 570-h264-v [Or
localhost/Analog Camera - WV-CP484
localhost/Cisco-1080-h264-v - Cisco-10
localhost/IQeye-855 - IQeye-855 [Onli
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
Reset Cameras...
194113

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*

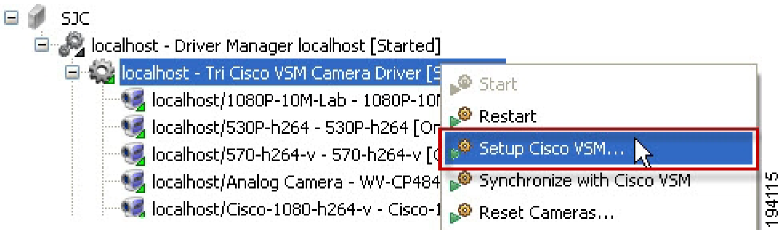
– *live data feed*

– *camera data feed*

Step 7 Re-enter the Cisco VSM server settings:

Note Do not change the database name or port number once they are configured.

a. Right-click the **Cisco VSM Camera Driver** and select **Setup Cisco VSM**.


SJC
localhost - Driver Manager localhost [Started]
localhost - Tri Cisco VSM Camera Driver [S
localhost/1080P-10M-Lab - 1080P-10M
localhost/530P-h264 - 530P-h264 [Or
localhost/570-h264-v - 570-h264-v [
localhost/Analog Camera - WV-CP484
localhost/Cisco-1080-h264-v - Cisco-1
Start
Restart
Setup Cisco VSM...
Synchronize with Cisco VSM
Reset Cameras...
194115

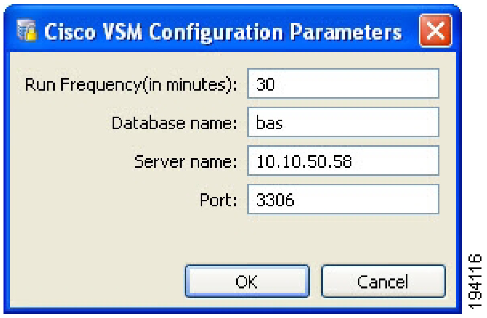
b. Enter the **Run Frequency (in minutes)**: the time between ICPAM / VSM synchronization. Cameras added or removed from Cisco VSM are updated in ICPAM. If the camera inventory changes often, enter a low number. If the inventory changes rarely, enter a high number. The default is 30 minutes.

c. Enter the **Database name**: the name of the Cisco VSM database. The default is `bas`.

d. Enter the **Server name**: the name or IP Address of the Cisco VSM database server.

e. Enter the **Port number**: the port number for the Cisco VSM database server.

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


Cisco VSM Configuration Parameters

Run Frequency(in minutes): 30
Database name: bas
Server name: 10.10.50.58
Port: 3306

Tip Entering the **Restart**, **Setup VSOM**, or **Synchronize with Cisco VSM** commands will retrieve the camera inventory immediately, regardless of the configured run frequency. After the initial synchronization, the inventory is updated based on the scheduled run frequency.

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.

a. Select the **Miscellaneous** submenu.

a. Select the check-box for **Allow deletion of devices with events**. This allows cameras with associated events to be deleted from ICPAM.

b. Log out and log back in to the ICPAM 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 Door, page 7-15 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 ICPAM. 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 Verify that ICPAM Web Services are enabled:

Note Skip to Step 3 if ICPAM Web Services are already enabled.

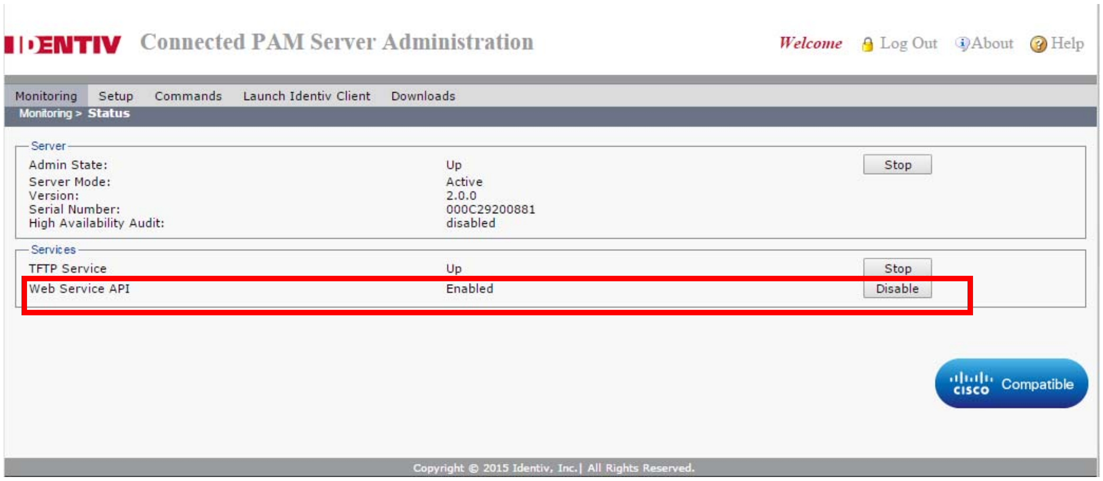
a. Log on to the ICPAM Server Administration utility, as described in the "Logging on to the ICPAM Server Administration Utility" section on page 2-2.

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 15-3).

Figure 15-3 Web Services API Status



Server

Admin State: Up
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

Services

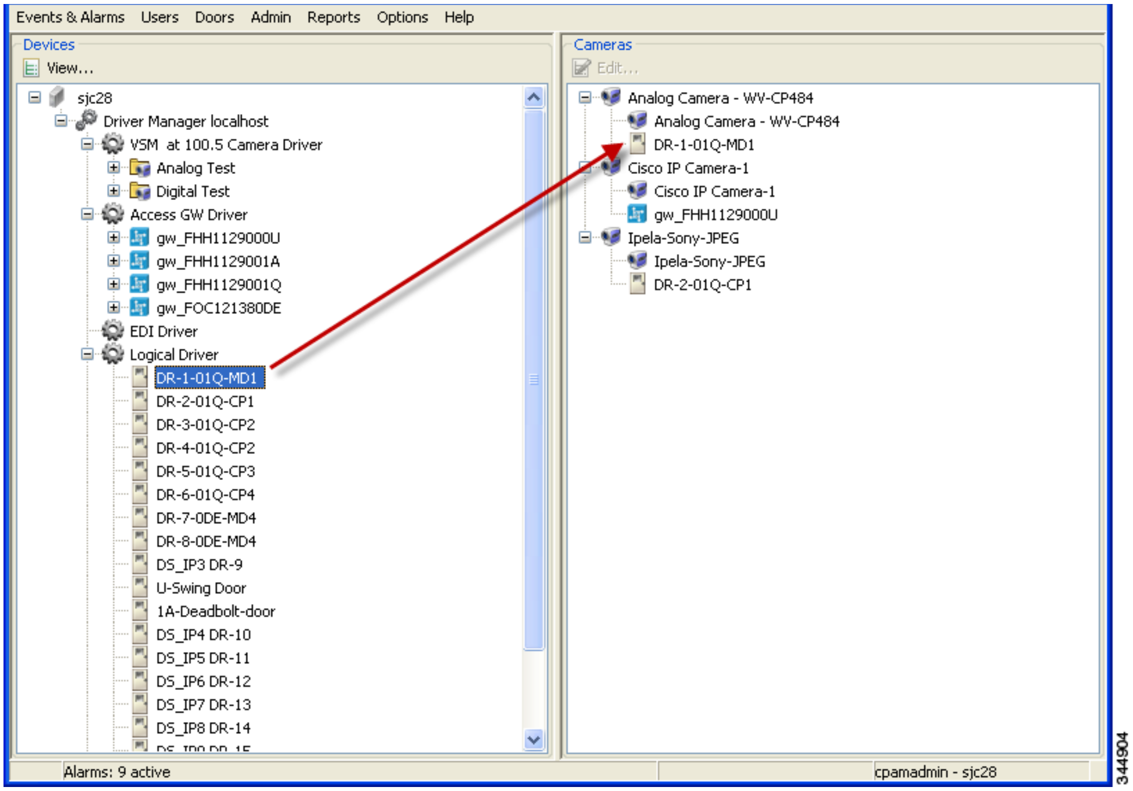
TFTP Service Up
Web Service API Enabled

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Step 3 (Optional) To open a video pop-up window for door events, associate a door with the camera:

a. Expand the **Physical Driver** to display the configured doors, as shown in Figure 15-4.

Figure 15-4 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 4 Identify and record the Camera ID, as shown in Figure 15-5.

The Camera ID is used in the URL used to call the event, as described in Step 5.

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

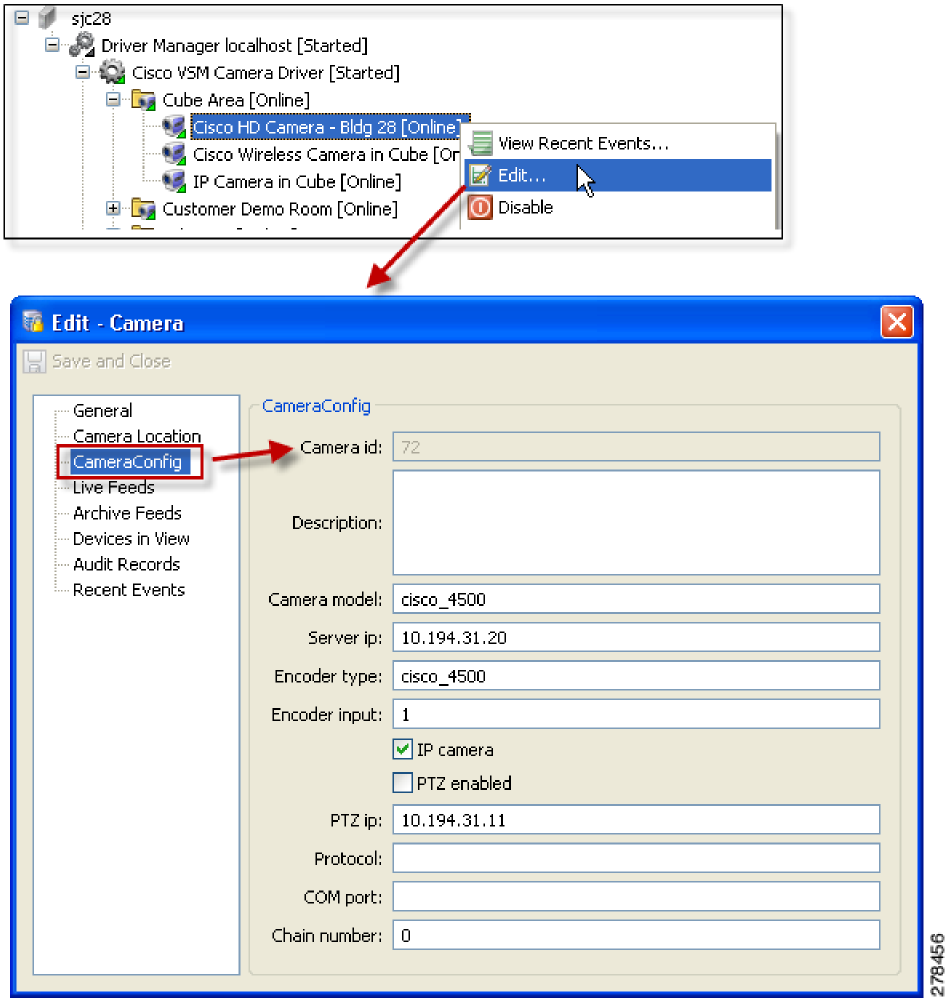
b. Expand the **Camera Driver** to display the available cameras.

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.

Figure 15-5 Locating the Camera ID



Camera id: 72

Description:

Camera model: cisco_4500

Server ip: 10.194.31.20

Encoder type: cisco_4500

Encoder input: 1

☑ IP camera

□ PTZ enabled

PTZ ip: 10.194.31.11

Protocol:

COM port:

Chain number: 0

Step 5 Add a URL Notification to the motion event using the Cisco VSOM web-based software.

Note Only Cisco VSM events configured with URL notifications are sent to ICPAM.

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 15-6).

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 ICPAM URL for the motion event in the following format:

http://*icpam-ip-addr***/***acws/services/acvsm/recordCameraEvent?cameraId=number&eventType=type&eventTime=time_value*

The URL includes the following parameters:

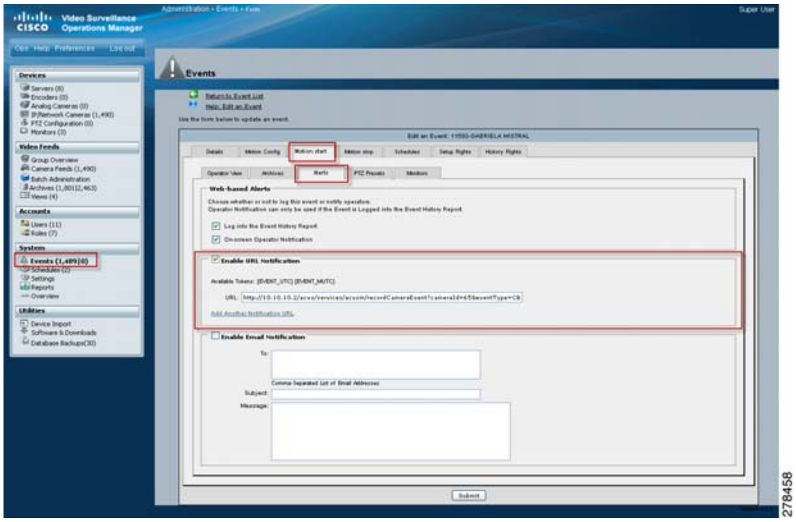
- *icpam-ip-addr*: the IP address of the ICPAM server.
- *number*: the **cameraId** number recorded in Step 4. For example: `65`.
- *type*: the **eventType**. For example:`CB.MOTION_START` or `CB_MOTION_STOP`
- *time_value*: the **eventTime**. Enter a timestamp or 0 for the current time.

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.

```
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 15-6 Enable URL Notification in the Cisco VSOM Events Configuration Page



Choose whether or not to log this event or notify operators.
Operator Notification can only be used if the Event is Logged into the Event History Report.

☑ Log into the Event History Report

☑ On-screen Operator Notification

☑ Enable URL Notification

Available Tokens: {EVENT_UTC} {EVENT_MUTC}

URL: http://10.10.10.2/acws/services/acvsm/recordCameraEvent?cameraId=65&eventType=CB

□ Enable Email Notification

To:

Comma Separated List of Email Addresses

Subject:

Message:

Step 6 View the motion events in ICPAM Events:

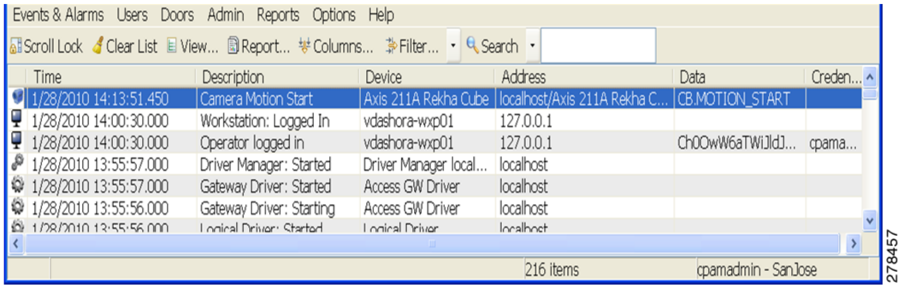
a. Launch the ICPAM software and log in, if necessary.

b. Select **Events** from the **Events & Alarms** menu, under the **Monitoring** submenu.

c. Sort or search for the event, as described in the “Viewing Events” section on page 12-4.

Figure 15-7 shows an example of a **Camera Motion Start** event. Double-click the event entry for additional details.

Figure 15-7 Camera Events in ICPAM



Time	Description	Device	Address	Data	Creden...
1/28/2010 14:13:51.450	Camera Motion Start	Axis 211A Rekha Cube	localhost/Axis 211A Rekha C...	CB.MOTION_START	
1/28/2010 14:00:30.000	Workstation: Logged In	vdashora-wxp01	127.0.0.1		
1/28/2010 14:00:30.000	Operator logged in	vdashora-wxp01	127.0.0.1	Ch0OwW6aTWiJldJ...	cpama...
1/28/2010 13:55:57.000	Driver Manager: Started	Driver Manager local...	localhost		
1/28/2010 13:55:57.000	Gateway Driver: Started	Access GW Driver	localhost		
1/28/2010 13:55:56.000	Gateway Driver: Starting	Access GW Driver	localhost		
1/28/2010 13:55:56.000	Logical Driver: Started	Logical Driver	localhost		

216 items cpamadmin - SanJose

Triggering Camera Actions and Video Recording in Cisco VSM

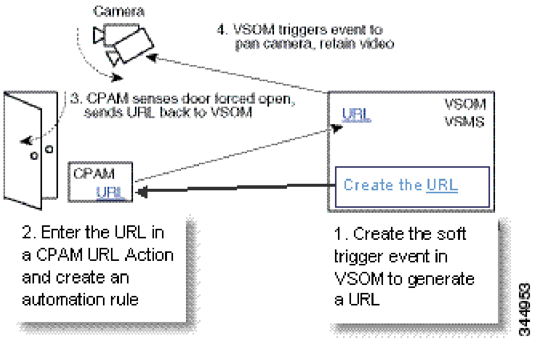
Events in Cisco VSM can use a *soft trigger* to perform an action (such as adjusting a camera PTZ setting). The soft trigger is activated when Cisco VSM receives a URL from an external system, such as ICPAM.

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 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 ICPAM, create a URL action using the Cisco VSM URL that was automatically generated when you created the VSM soft trigger.
3. In ICPAM, create an automation rule (global I/O rule) that triggers the URL action when a *door forced open* event occurs.
4. ICPAM sends the URL to Cisco VSM.
5. When Cisco VSM receives the URL, the camera pans and a video archive is created.

Figure 15-8 illustrates this example.

Figure 15-8 Soft Trigger Event in Cisco VSM


Camera
4. VSOM triggers event to pan camera, retain video
3. CPAM senses door forced open, sends URL back to VSOM
URL
VSOM
VSMS
CPAM
URL
Create the URL
2. Enter the URL in a CPAM URL Action and create an automation rule
1. Create the soft trigger event in VSOM to generate a URL
344953

Tip See the Cisco Video Surveillance Manager User Guide for instructions to create Cisco VSM soft triggers.

CHAPTER 16

VoIP Integration

The integration of VoIP phone to ICPAM enables users to grant access to doors through the VoIP phone. This new feature of ICPAM allows the entry of personnel without badges. The VoIP integration does not require any configuration on the ICPAM. The ICPAM user receives the access request from the personnel/employees, enquires the credentials and grants them access through the VoIP phone.

VoIP phone integration to ICPAM is achieved by the following processes:

- Creating a phone service in **Unified Call Manager (UCM)** and
- Subscribing a service to a VoIP phone.

Contents

Creating a Phone Service in UCM

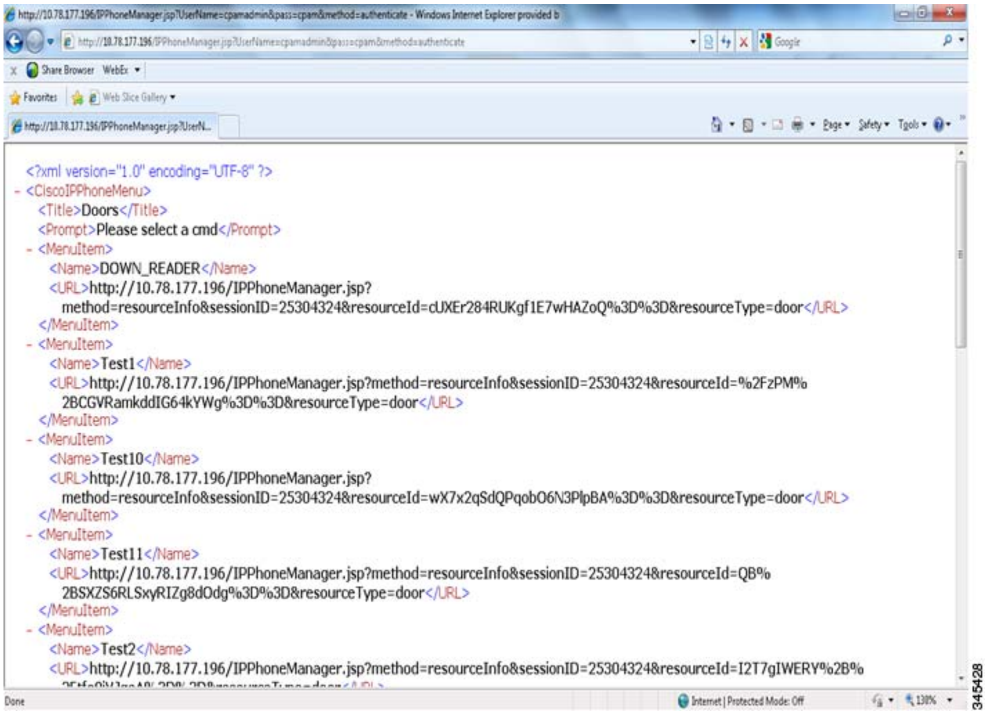
By creating a service in UCM, you establish a link between the ICPAM and UCM. The ICPAM IP is given while creating the service. The services can be created for single door or multiple doors in ICPAM. You need to ensure that the URL is validated before creating a service.

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.

Figure 16-1 Validating the URL



http://10.78.177.196/IPPhoneManager.jsp?UserName=cpamadmin&pass=cpam&method=authenticate - Windows Internet Explorer provided b
http://10.78.177.196/IPPhoneManager.jsp?UserName=cpamadmin&pass=cpam&method=authenticate
Google
Share Browser
WebEx
Favorites
Web Slice Gallery
http://10.78.177.196/IPPhoneManager.jsp?UserN...
Page
Safety
Tools
Done
Internet | Protected Mode: Off
130%
345428

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <CiscoIPPhoneMenu>
    <Title>Doors</Title>
    <Prompt>Please select a cmd</Prompt>
  - <MenuItem>
      <Name>DOWN_READER</Name>
      <URL>http://10.78.177.196/IPPhoneManager.jsp?
        method=resourceInfo&sessionID=25304324&resourceId=cUXEr284RUKgf1E7wHAZoQ%3D%3D&resourceType=door</URL>
    </MenuItem>
  - <MenuItem>
      <Name>Test1</Name>
      <URL>http://10.78.177.196/IPPhoneManager.jsp?method=resourceInfo&sessionID=25304324&resourceId=%2FzPM%
        2BCGVRamkddIG64kYWg%3D%3D&resourceType=door</URL>
    </MenuItem>
  - <MenuItem>
      <Name>Test10</Name>
      <URL>http://10.78.177.196/IPPhoneManager.jsp?
        method=resourceInfo&sessionID=25304324&resourceId=wX7x2qSdQPqobO6N3PlpBA%3D%3D&resourceType=door</URL>
    </MenuItem>
  - <MenuItem>
      <Name>Test11</Name>
      <URL>http://10.78.177.196/IPPhoneManager.jsp?method=resourceInfo&sessionID=25304324&resourceId=QB%
        2BSXZS6RLSxyRIZg8dOdg%3D%3D&resourceType=door</URL>
    </MenuItem>
  - <MenuItem>
      <Name>Test2</Name>
      <URL>http://10.78.177.196/IPPhoneManager.jsp?method=resourceInfo&sessionID=25304324&resourceId=I2T7gIWERY%2B%
```

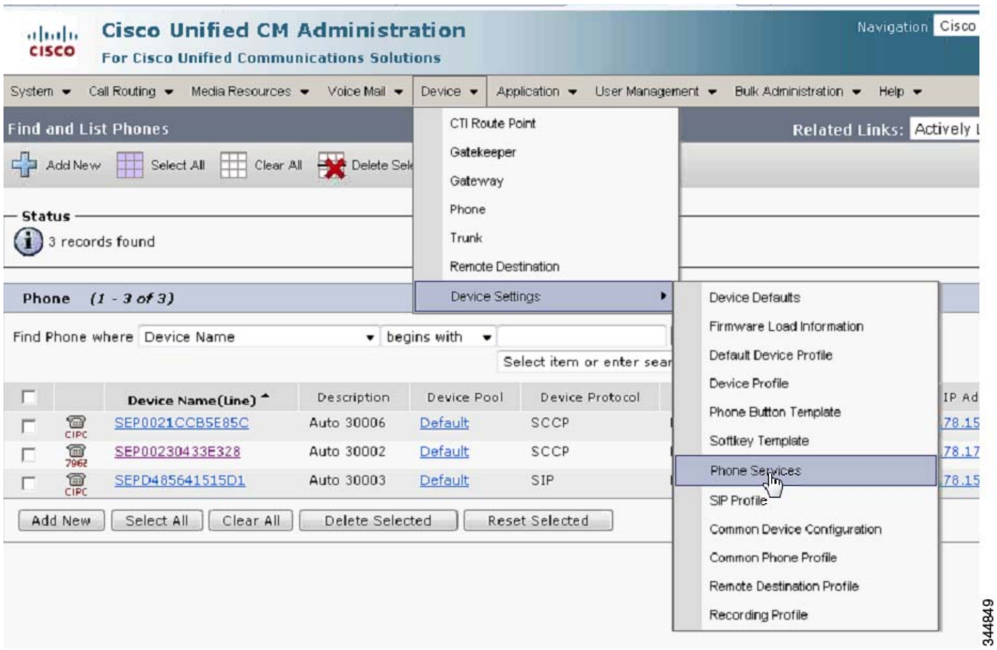
Procedure

To create a phone service, do the following:

Step 1 Go to the UCM administration page.

Step 2 Choose **Device** -> **Device Settings** -> **Phone services**.

Figure 16-2 UCM Phone Services



□		Device Name(Line)	Description	Device Pool	Device Protocol	IP Ad
□	CIPC	SEP0021CCB5E85C	Auto 30006	Default	SCCP	78.15
□	7962	SEP00230433E328	Auto 30002	Default	SCCP	78.17
□	CIPC	SEPD485641515D1	Auto 30003	Default	SIP	78.15

Step 3 Click **Add New** to create a new service.

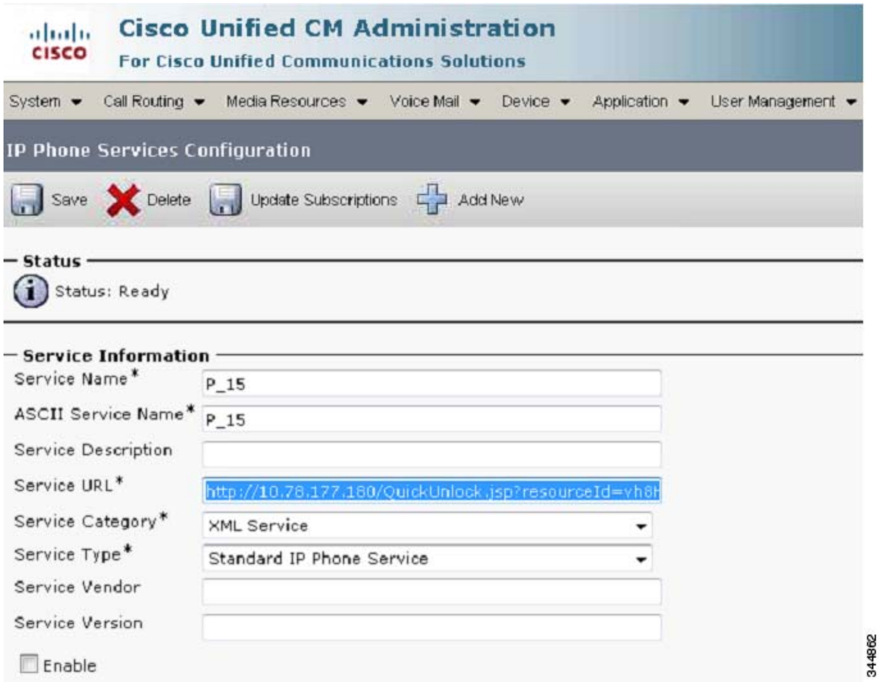
- You can also modify existing services.

Step 4 Enter the details in the **IP Phone Services Configuration** window.

Note Enter the ICPAM 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

Figure 16-3 Service URL



IP Phone Services Configuration

Status

Status: Ready

Service Information

Service Name*	P_15
ASCII Service Name*	P_15
Service Description	
Service URL*	http://10.78.177.180/QuickUnlock.jsp?resourceId=vh8I
Service Category*	XML Service
Service Type*	Standard IP Phone Service
Service Vendor	
Service Version	

□ Enable

Step 5 Click **Save**. The service is created.

Additional Information

ICPAM 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_icpam>/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_icpam>/IPPhoneManager.jsp?method=authenticate&UserName=<cpamadmin>& pass=<password_for_icpamadmin>

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.

Usecase 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_icpam>/QuickUnlock.jsp?method=authenticate&UserName=<cpamadmin>&pass=<password_for_icpamadmin>&resourceId=<Door_Unique_ID>&resourceType=door

More Information on the URLs

For quick unlock of a door:

http://<ip_address_of_icpam>/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_icpam>/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_icpam>/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

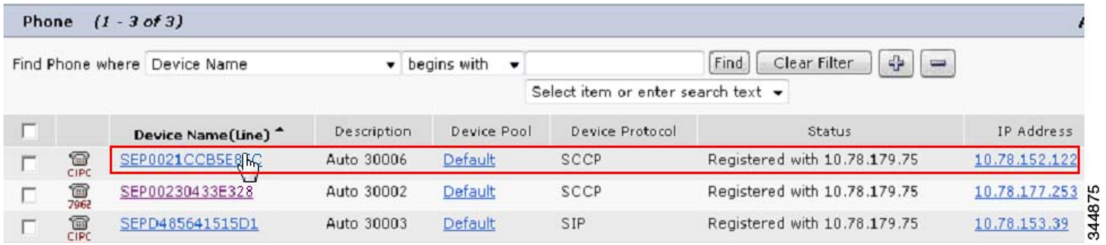
Note To Configure VoIP phone to UCM contact the UCM Admin.

Procedure

Step 1 Go to **Device->Phone** in the UCM 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



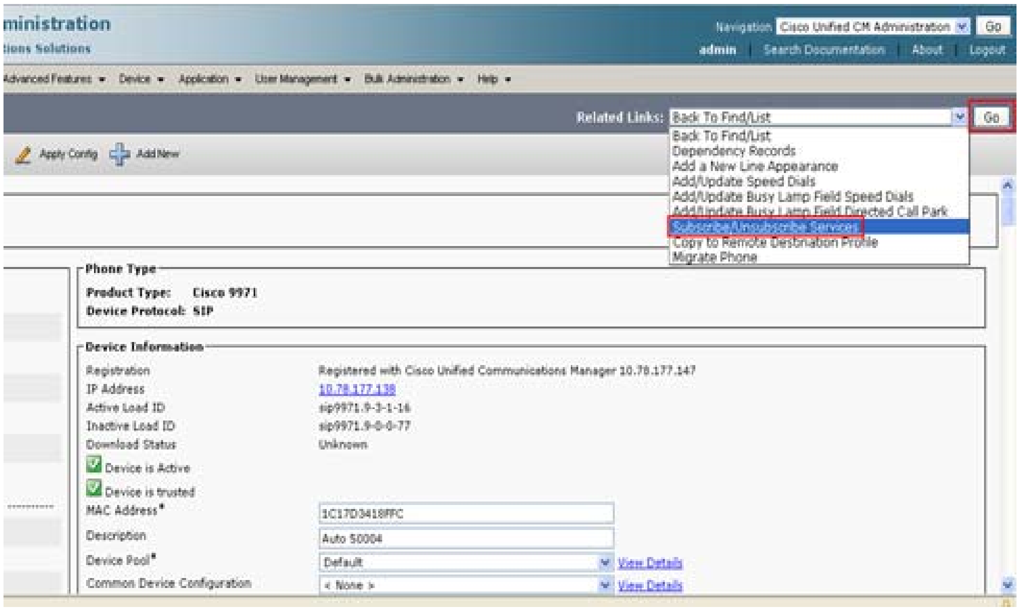
Phone (1 - 3 of 3)

Find Phone where Device Name begins with Select item or enter search text

□		Device Name(Line)	Description	Device Pool	Device Protocol	Status	IP Address
□	☎ CIPC	SEP0021CCB5E8[illegible]C	Auto 30006	Default	SCCP	Registered with 10.78.179.75	10.78.152.122
□	☎ 7962	SEP00230433E328	Auto 30002	Default	SCCP	Registered with 10.78.179.75	10.78.177.253
□	☎ CIPC	SEPD485641515D1	Auto 30003	Default	SIP	Registered with 10.78.179.75	10.78.153.39

Step 3 Choose **Subscribe/Unsubscribe Services** from Related Links and click **GO**.

Figure 16-5 Subscribed/Unsubscribed Services


ministration
tions Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Related Links: Back To Find/List Go
Back To Find/List
Dependency Records
Add a New Line Appearance
Add/Update Speed Dials
Add/Update Busy Lamp Field Speed Dials
Add/Update Busy Lamp Field Directed Call Park
Subscribe/Unsubscribe Services
Copy to Remote Destination Profile
Migrate Phone
Apply Config
Add New
View Details
View Details

Phone Type

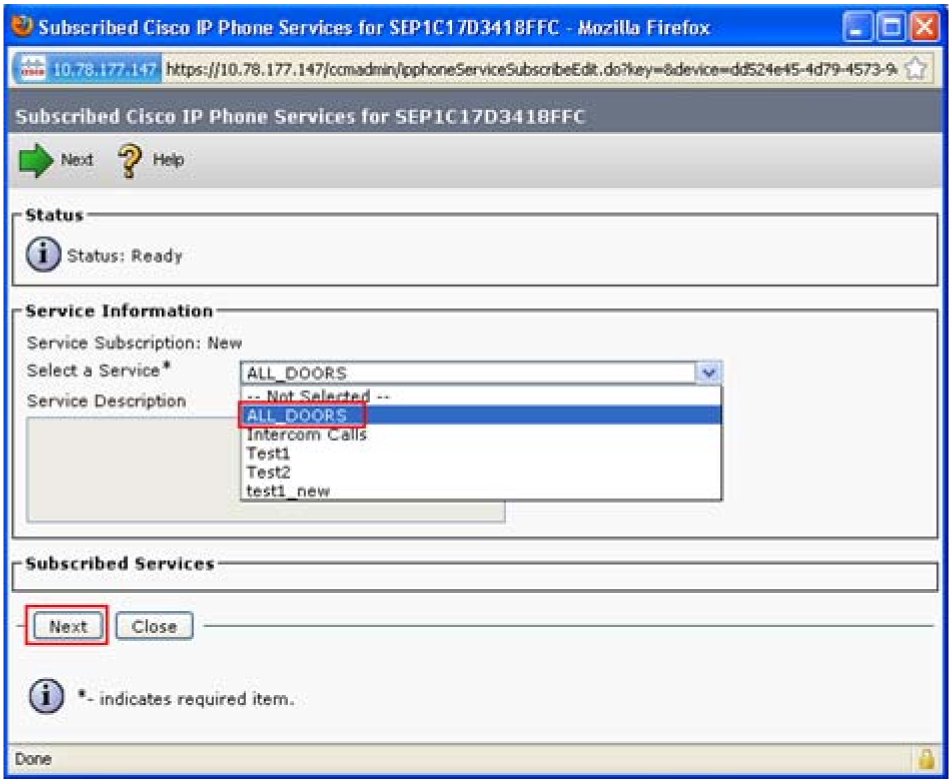
Product Type: Cisco 9971
Device Protocol: SIP

Device Information

Registration	Registered with Cisco Unified Communications Manager 10.78.177.147
IP Address	10.78.177.138
Active Load ID	sip9971.9-3-1-16
Inactive Load ID	sip9971.9-0-0-77
Download Status	Unknown
☑ Device is Active	
☑ Device is trusted	
MAC Address*	1C17D3418FFC
Description	Auto 50004
Device Pool*	Default
Common Device Configuration	< None >

Step 4 Select a Service from the drop down list. Click **Next**.

Figure 16-6 Select a service



https://10.78.177.147/ccmadmin/ipphoneServiceSubscribeEdit.do?key=&device=dd524e45-4d79-4573-9

Subscribed Cisco IP Phone Services for SEP1C17D3418FFC

Status

Status: Ready

Service Information

Service Subscription: New

Select a Service* ALL_DOORS

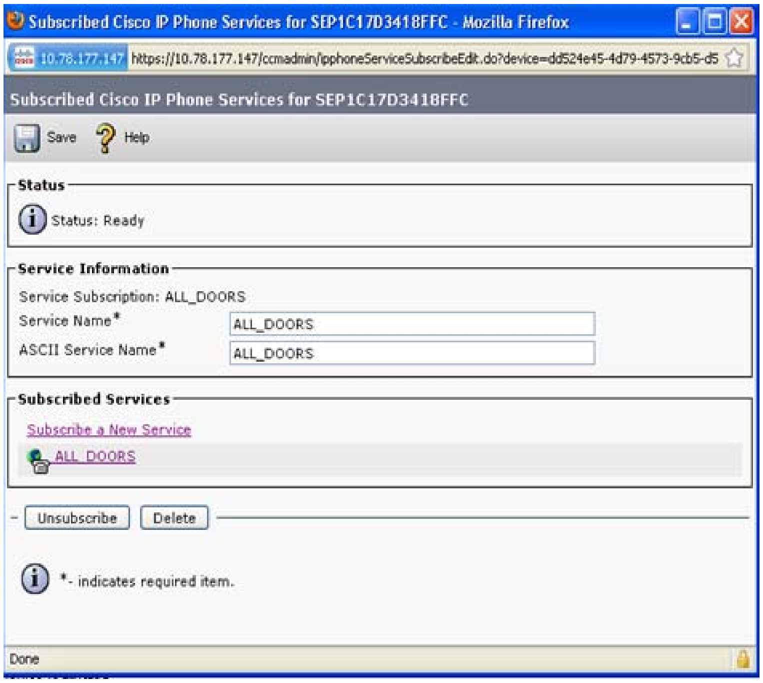
Service Description

Subscribed Services

*- indicates required item.

Step 5 Click **Subscribe**.The service is now subscribed to the phone and is listed under Subscribed Services.

Figure 16-7 Service Subscribed



Subscribed Cisco IP Phone Services for SEP1C17D3418FFC - Mozilla Firefox

10.78.177.147 https://10.78.177.147/ccmadmin/ipphoneServiceSubscribeEdit.do?device=dd524e45-4d79-4573-9cb5-d5

Subscribed Cisco IP Phone Services for SEP1C17D3418FFC

Status

Status: Ready

Service Information

Service Subscription: ALL_DOORS

Service Name* ALL_DOORS

ASCII Service Name* ALL_DOORS

Subscribed Services

Subscribe a New Service

ALL_DOORS

*- indicates required item.

Done

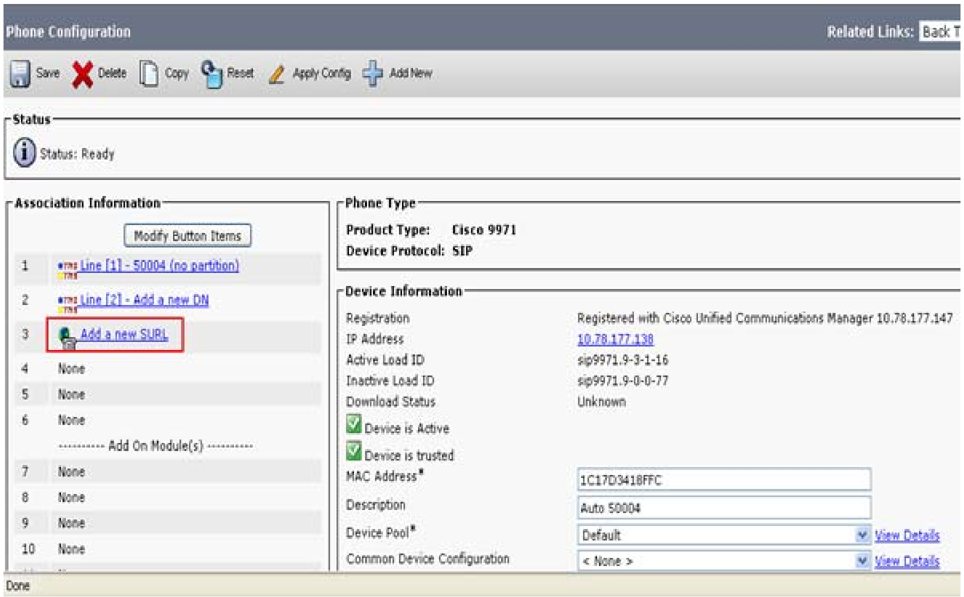
Note To subscribe for more services, Click **Subscribe a New Service** link in the subscribed services.

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



Phone Configuration Related Links: Back T

Status

Status: Ready

Association Information

1 Line [1] - 50004 (no partition)

2 Line [2] - Add a new DN

3 Add a new SURL

4 None

5 None

6 None

---------- Add On Module(s) ----------

7 None

8 None

9 None

10 None

Phone Type

Product Type: Cisco 9971

Device Protocol: SIP

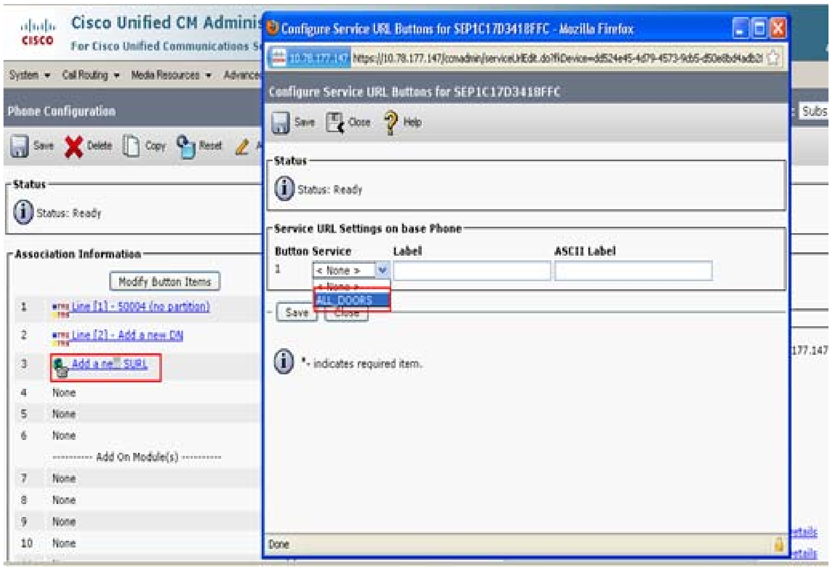
Device Information

Registration	Registered with Cisco Unified Communications Manager 10.78.177.147
IP Address	10.78.177.138
Active Load ID	sip9971.9-3-1-16
Inactive Load ID	sip9971.9-0-0-77
Download Status	Unknown
☑ Device is Active	
☑ Device is trusted	
MAC Address*	1C17D3418FFC
Description	Auto 50004
Device Pool*	Default View Details
Common Device Configuration	< None > View Details

Done

Step 8 Select the service to configure the service URL button.

Figure 16-9 Configure Service URL button



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Phone Configuration

Status

Status: Ready

Association Information

1 Line [1] - 50004 (no partition)
2 Line [2] - Add a new DN
3 Add a new SURL
4 None
5 None
6 None
---------- Add On Module(s) ----------
7 None
8 None
9 None
10 None

Configure Service URL Buttons for SEP1C17D3418FFC - Mozilla Firefox

https://10.78.177.147/ccmadmin/serviceUrlEdit.do?fkDevice=dd524e45-4d79-4573-9cb5-d50e8bd4adb2

Configure Service URL Buttons for SEP1C17D3418FFC

Status

Status: Ready

Service URL Settings on base Phone

Button	Service	Label	ASCII Label
1	< None > < None > ALL_DOORS		

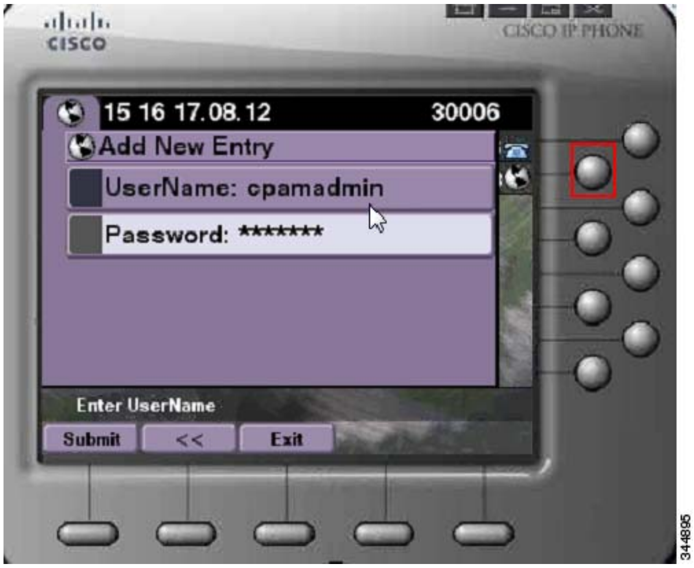
*- indicates required item.

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



15 16 17.08.12 30006

Add New Entry

UserName: cpamadmin

Password: *******

Enter UserName

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: ICPAM 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.

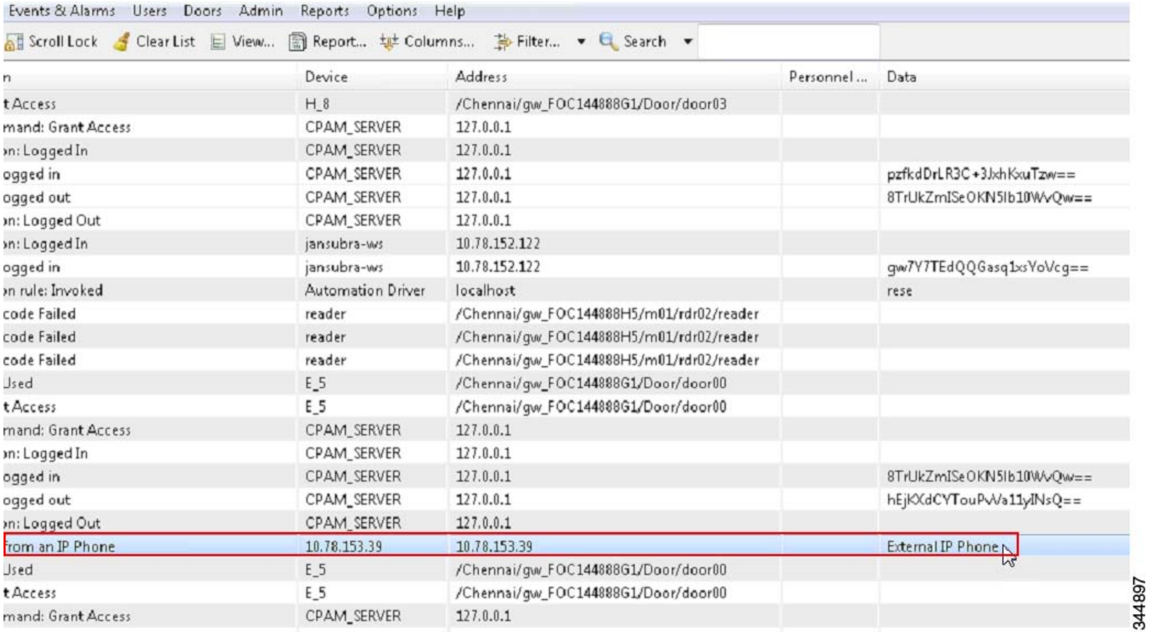
- Authentication failed.

Note

- If you have configured a list of doors to a service, the 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 ICPAM under **Events and Alarms->Monitoring->Events**.

Figure 16-11 Events



n	Device	Address	Personnel ...	Data
t Access	H_8	/Chennai/gw_FOC144888G1/Door/door03		
mand: Grant Access	CPAM_SERVER	127.0.0.1		
n: Logged In	CPAM_SERVER	127.0.0.1		
ogged in	CPAM_SERVER	127.0.0.1		pzfkdDrLR3C+3JxhKxuTzw==
ogged out	CPAM_SERVER	127.0.0.1		8TrUkZmISeOKN5Ib10WvQw==
n: Logged Out	CPAM_SERVER	127.0.0.1		
n: Logged In	jansubra-ws	10.78.152.122		
ogged in	jansubra-ws	10.78.152.122		gw7Y7TEdQQGasq1xsYoVcg==
n rule: Invoked	Automation Driver	localhost		rese
code Failed	reader	/Chennai/gw_FOC144888H5/m01/rdr02/reader		
code Failed	reader	/Chennai/gw_FOC144888H5/m01/rdr02/reader		
code Failed	reader	/Chennai/gw_FOC144888H5/m01/rdr02/reader		
Jsed	E_5	/Chennai/gw_FOC144888G1/Door/door00		
t Access	E_5	/Chennai/gw_FOC144888G1/Door/door00		
mand: Grant Access	CPAM_SERVER	127.0.0.1		
n: Logged In	CPAM_SERVER	127.0.0.1		
ogged in	CPAM_SERVER	127.0.0.1		8TrUkZmISeOKN5Ib10WvQw==
ogged out	CPAM_SERVER	127.0.0.1		hEjKXdCYTouPvVa11yINsQ==
n: Logged Out	CPAM_SERVER	127.0.0.1		
from an IP Phone	10.78.153.39	10.78.153.39		External IP Phone
Jsed	E_5	/Chennai/gw_FOC144888G1/Door/door00		
t Access	E_5	/Chennai/gw_FOC144888G1/Door/door00		
mand: Grant Access	CPAM_SERVER	127.0.0.1		

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.

CHAPTER 17

System Configuration Settings

This chapter describes the system-wide site settings available in the System Configuration module. The System Configuration module includes additional settings through which an user profile can be associated to a location hierarchy. This feature allow the users to control or execute actions on locations and sub locations mapped to their user profile. See Logins Settings, page 17-10

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 ICPAM application to activate the changes (select Logout from the Options menu).

Note Changes to system configuration settings do not take effect until you stop and start the ICPAM application. For some settings in the ICPAM Settings window, you must restart the ICPAM appliance. See the "Advanced Settings" section on page 17-29 for more information.

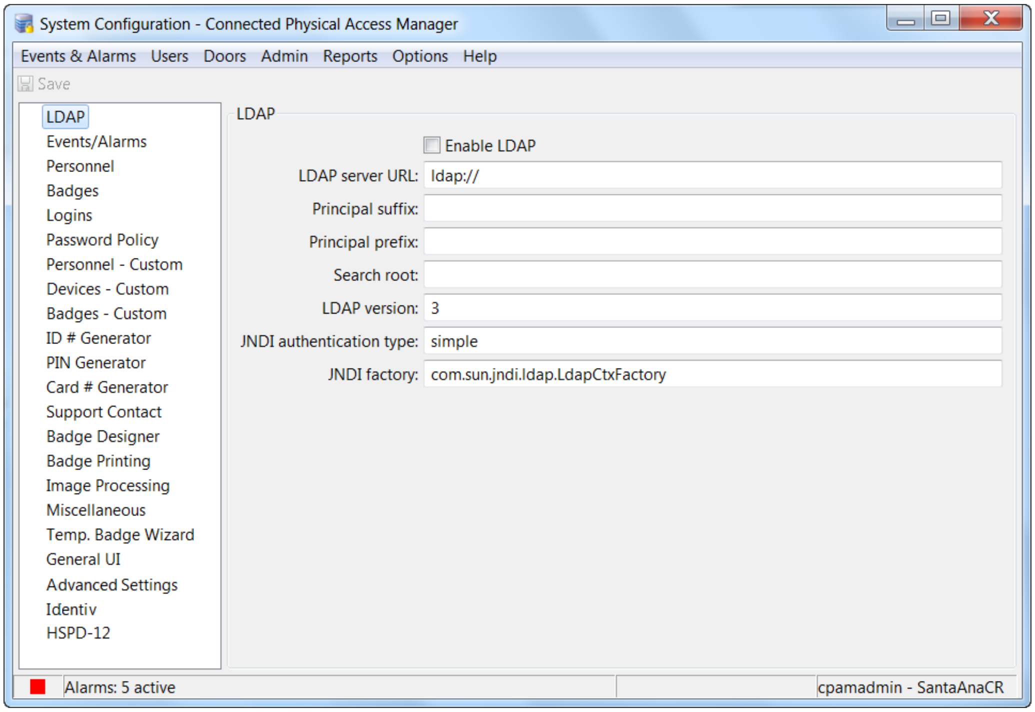
Contents

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.

Tip For more information, see Configuring LDAP User Authentication, page 4-12.

Figure 17-1 LDAP Settings



LDAP

□ Enable LDAP

LDAP server URL: ldap://

Principal suffix:

Principal prefix:

Search root:

LDAP version: 3

JNDI authentication type: simple

JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

Alarms: 5 active

cpamadmin - SantaAnaCR

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 17-1 System Configuration LDAP Settings

Field	Description
Enable LDAP	Click the check box to enable or disable LDAP support.
LDAP server URL	URL of LDAP server, must begin with `ldap://` Example: `ldap://192.168.1.1`

Table 17-1 System Configuration LDAP Settings (continued)

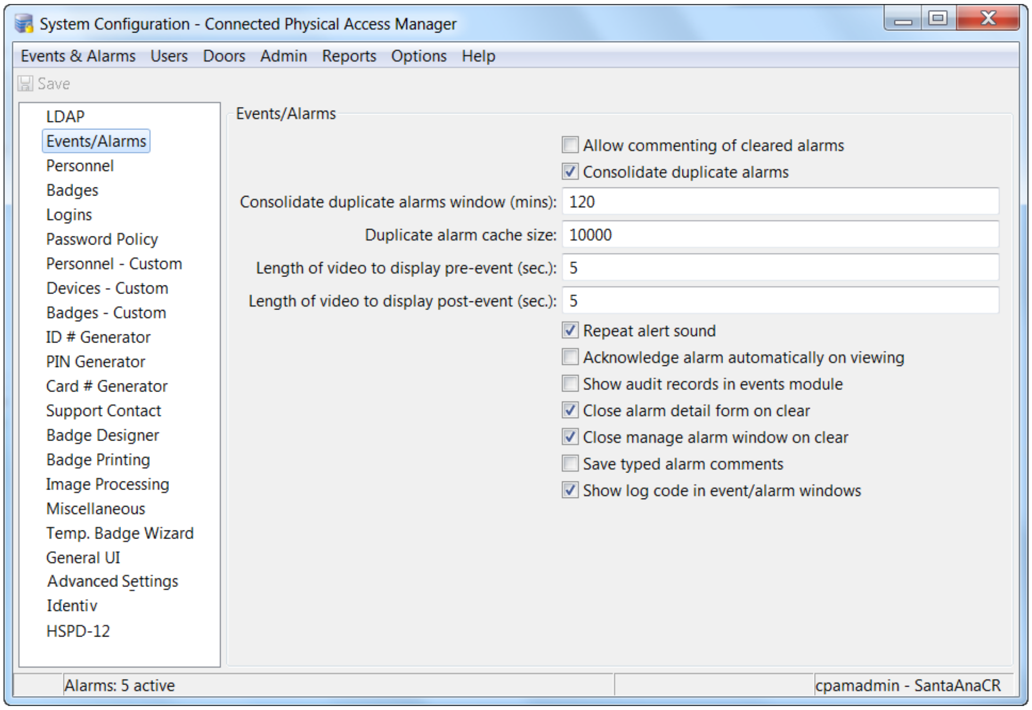
Field	Description
Principle suffix	Appended to the username for authentication. See above.
Principle prefix	Prepended to the username for authentication. See above.
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: `cn=Users,dc=my-domain,dc=com`. • 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.`
LDAP version	Advanced setting that generally should be left unchanged.
JNDI authentication type	Advanced setting that generally should be left unchanged as `simple`.
JNDI factory	Advanced setting that generally should be left unchanged as `com.sun.jndi.ldap.LdapCtxFactory`

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the **Options** menu).

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



□ Allow commenting of cleared alarms
☑ Consolidate duplicate alarms
Consolidate duplicate alarms window (mins): 120
Duplicate alarm cache size: 10000
Length of video to display pre-event (sec.): 5
Length of video to display post-event (sec.): 5
☑ Repeat alert sound
□ Acknowledge alarm automatically on viewing
□ Show audit records in events module
☑ Close alarm detail form on clear
☑ Close manage alarm window on clear
□ Save typed alarm comments
☑ Show log code in event/alarm windows

Table 17-2 describes the Event and Alarms settings.

Table 17-2 System Configuration Alarm Fields

Field	Description
Allow commenting of cleared alarms	Allow operators to comment on alarms that have already been cleared.
Consolidate duplicate alarms window (mins)	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.
Consolidate duplicate alarms	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.
Duplicate alarm cache size	The size of the cache for duplicate alarms.

Table 17-2 System Configuration Alarm Fields (continued)

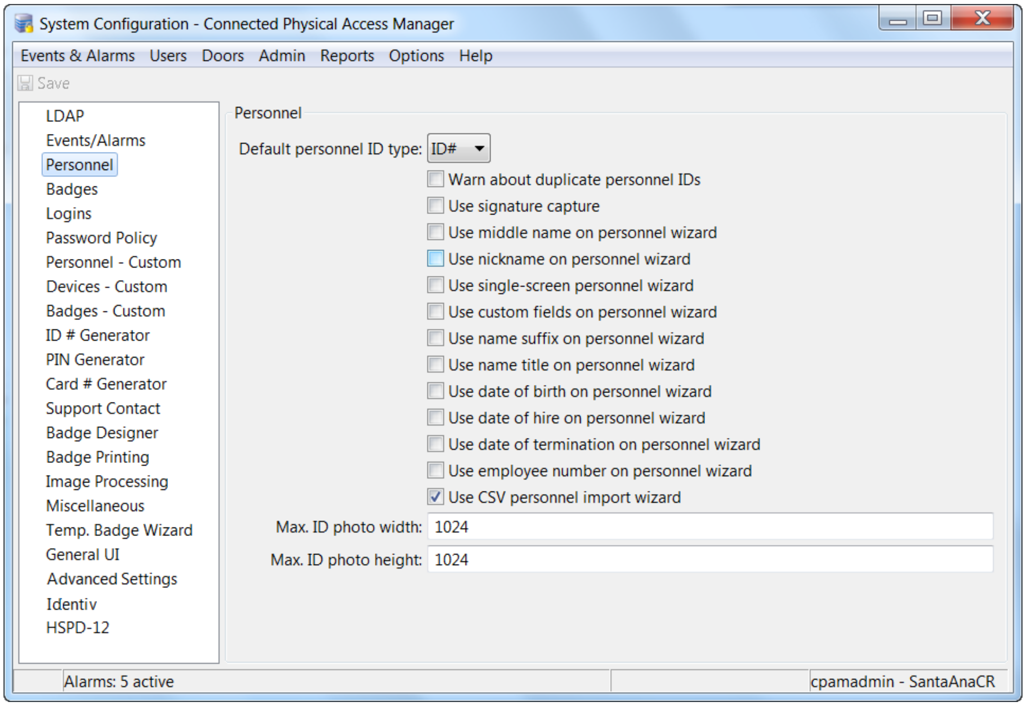
Field	Description
Length of video to display pre-event	The number of seconds of video that are included before the event occurred.
Length of video to display post-event	The number of seconds of video that are included after an event occurs.
Repeat alert sounds	Defines if alarms sounds are played only once, or repeated.
Show audit records in events	Lists the audit records of events.

Note Changes to system configuration settings do not take effect until the ICPAM desktop application is restarted (exit and re-launch the application).

Personnel Settings

Use the Personnel tab (Figure 17-3) to display the settings for personnel-related features in ICPAM.

Figure 17-3 Personnel Settings



Personnel

Default personnel ID type: ID#

- □ Warn about duplicate personnel IDs
- □ Use signature capture
- □ Use middle name on personnel wizard
- □ Use nickname on personnel wizard
- □ Use single-screen personnel wizard
- □ Use custom fields on personnel wizard
- □ Use name suffix on personnel wizard
- □ Use name title on personnel wizard
- □ Use date of birth on personnel wizard
- □ Use date of hire on personnel wizard
- □ Use date of termination on personnel wizard
- □ Use employee number on personnel wizard
- ☑ Use CSV personnel import wizard

Max. ID photo width: 1024

Max. ID photo height: 1024

Table 17-3 details the Personnel settings.

Table 17-3 Personnel Settings

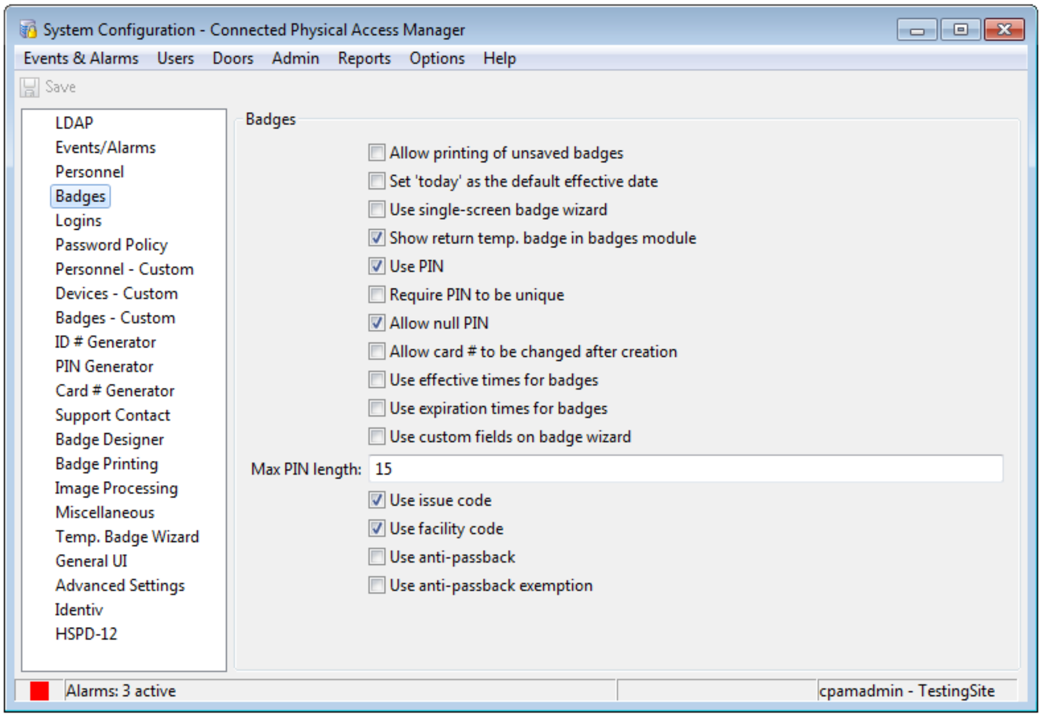
Field	Description
Default personnel ID specifier	The type of personnel ID specifier the field will default to. The various ID specifiers will be available in the drop-down.
Warn about duplicate personnel IDs	Warn if personnel are added with duplicate personnel IDs.
Use signature capture	Enable the ability 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 9-55.
Use single-screen personnel wizard	Enables a single-screen personnel wizard used for personnel data entry. All personnel information is available on one screen.
Use custom fields on personnel wizard	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.
Use name suffix on personnel wizard	Choose a value from the drop-down menu (such as I, II, III, Jr., and Sr.) or enter the text manually to add suffix at the end the person's name.
Use name title on personnel wizard	Choose a value from the drop-down menu (such as Dr., Mr., or Ms.) or enter the text manually to add a person's formal title.
Use date of birth on personnel wizard	The person's date of birth.
Use date of hire on personnel wizard	The date the employee was hired.
Use date of termination on personnel wizard	The date the employee was terminated.
Use employee number on personnel wizard	The employee number, if applicable. Generally, but not required to be, unique.
Use CSV personnel import wizard	Enables the CSV import wizard in the personnel module. The CSV import wizard allows operators to add personnel to ICPAM using a CSV file. See Importing Personnel Records Using a Comma Separated Value (CSV) File, page 9-12.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Badges Settings

Use the **Badges** tab (Figure 17-4) to display the settings for badge-related features in ICPAM.

Figure 17-4 Badges Settings



Badges

☐ Allow printing of unsaved badges
☐ Set 'today' as the default effective date
☐ Use single-screen badge wizard
☑ Show return temp. badge in badges module
☑ Use PIN
☐ Require PIN to be unique
☑ Allow null PIN
☐ Allow card # to be changed after creation
☐ Use effective times for badges
☐ Use expiration times for badges
☐ Use custom fields on badge wizard

Max PIN length: 15

☑ Use issue code
☑ Use facility code
☐ Use anti-passback
☐ Use anti-passback exemption

🟥 Alarms: 3 active | cpamadmin - TestingSite

Table 17-4 describes the Badges settings.

Table 17-4 Badges Settings

Field	Description
Allow printing of unsaved badges	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.
Set 'today' as the default effective date	Uses the current date as a new badge effective date.
Use single-screen badge wizard	Enables a single-screen badge wizard for data entry. Most badge properties are on one screen.
Show return temporary badge in badge module	Displays return badge field in the badge module window if the field is checked.
Use PIN	A PIN associated with the badge. Depending on the configuration of an access point, the pin is entered into the keypad on the access point's reader.
Require PIN to be unique	Requires cardholder PINs to be unique. Useful in systems that use PIN-only access-control.

Table 17-4 Badges Settings (continued)

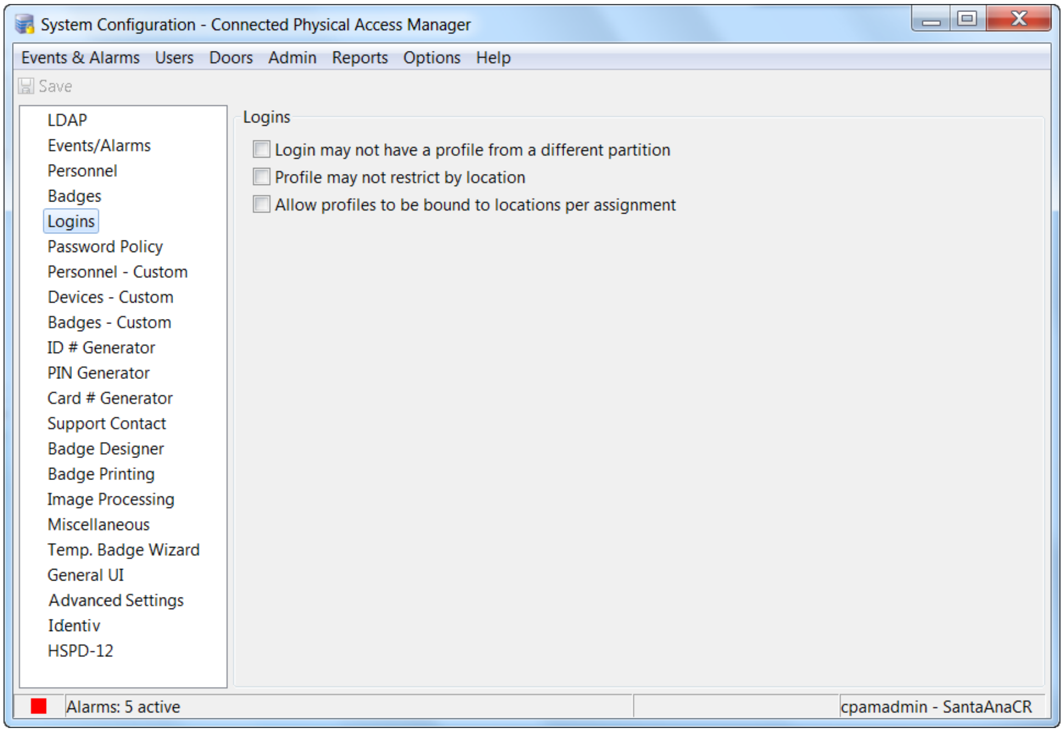
Field	Description
Allow null PIN	Allows badges to have null PINs. Useful in systems that do not use PIN for access-control.
Allow card # to be changed after creation	Also known as a badge. A type of credential encoded with a card number, generally on a magnetic stripe or a proximity card, and used to enter access points.
Require numeric hot stamp	Requires hot stamp field to be numeric.
Disallow leading zeros in hot stamp	Prohibits users from adding hot stamps with leading zeros.
Use effective times for badges	Select this check box to enable the effective time constraint for badges, in addition to effective date, which is always enabled.
Use expiration times for badges	Select this check box to enable the expiration time constraint for badges, in addition to effective date, which is always enabled.
Use custom fields on badge wizard	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.
Max PIN Length	The maximum number of characters in a PIN.
Use issue code	Displays the issue code field in the single screen badge wizard if the field is checked.
Use facility code	A segment of bits encoded on a card that represents a number for a facility. Often all cards issued for a single facility have the same facility code.
Use anti-passback	Enables the badge holder to be anti-passback exempt during the next reader use. After enabling this option "Grant one free APB button" is displayed in the badges.
Use anti-passback exemption	Enables the badge to be exempt from anti-passback enforcement if the access point is configured for anti-passback. After enabling this option "exempt from anti-passback" is displayed in the badges.

Note Changes to system configuration settings do not take effect until the ICPAM desktop application is restarted (exit and re-launch the application).

Logins Settings

The profile enhancement feature is set in this page. This configuration setting (Figure 17-5) facilitates the administrator to link a user profile to hierarchial location.

Figure 17-5 Logins Settings



□ Login may not have a profile from a different partition
□ Profile may not restrict by location
□ Allow profiles to be bound to locations per assignment

Alarms: 5 active
cpamadmin - SantaAnaCR

Table 17-5 describes the Logins Settings

Table 17-5 Logins Settings

Field	Description
Login may not have a profile from a different partition	Not supported in this version
Profile may not restrict by hierarchial location	select this check box if you do not want user profiles to be restricted by hierarchial locations
Allow profile to be bound to hierarchial locations per assignment	select this check box if you want user profiles to be restricted by hierarchial locations

On setting these changes, 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 a user can be associated to several profiles and the one with higher privileges is applied to the login user.

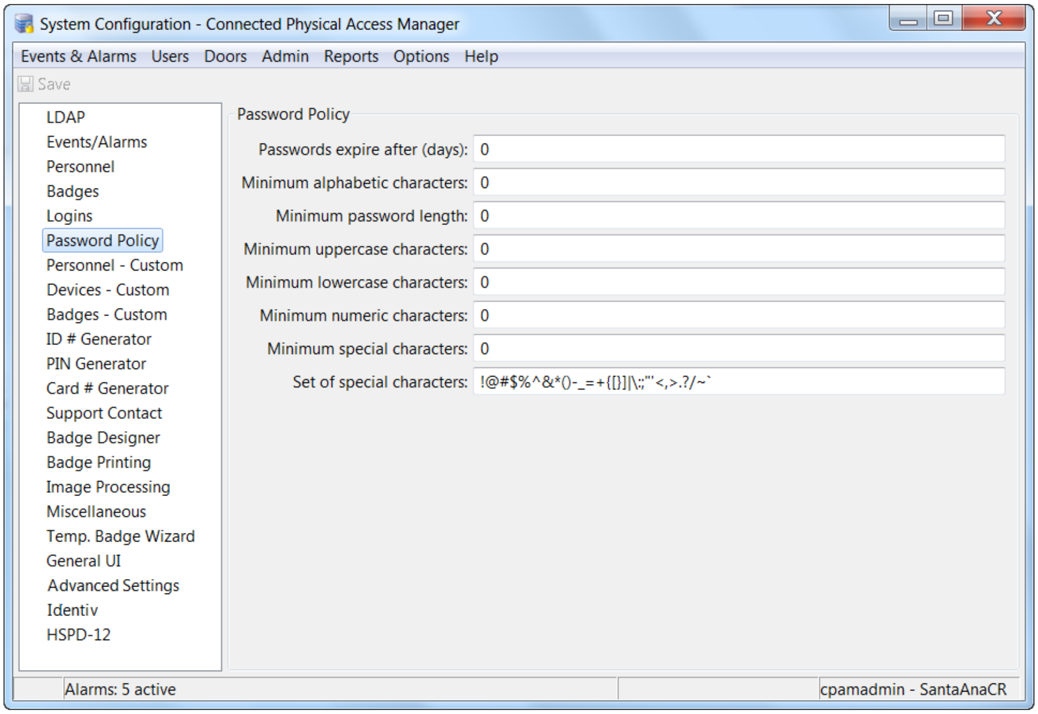
Tip You must select both profile may not restrict by hierarchial location and allow profile to be bound to hierarchial locations per assignment to associate profiles to hierarchial location.

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



Password Policy

Passwords expire after (days): 0
Minimum alphabetic characters: 0
Minimum password length: 0
Minimum uppercase characters: 0
Minimum lowercase characters: 0
Minimum numeric characters: 0
Minimum special characters: 0
Set of special characters: !@#$%^&*()-_=+{[}]|\:;"'<,>.?/~`

Table 17-6 describes the Password Policy settings.

Table 17-6 System Configuration Password Policy Fields

Field	Description
Passwords expire after (days)	Passwords expire after this many days.
Minimum alphabetic characters	Minimum number of a to z characters or A to Z characters in the password.
Minimum password length	Minimum number of characters in the password.
Minimum uppercase characters	Minimum number of uppercase password characters.
Minimum lowercase characters	Minimum number of lowercase password characters.
Minimum numeric characters	Minimum number of numeric password characters.

Table 17-6 System Configuration Password Policy Fields (continued)

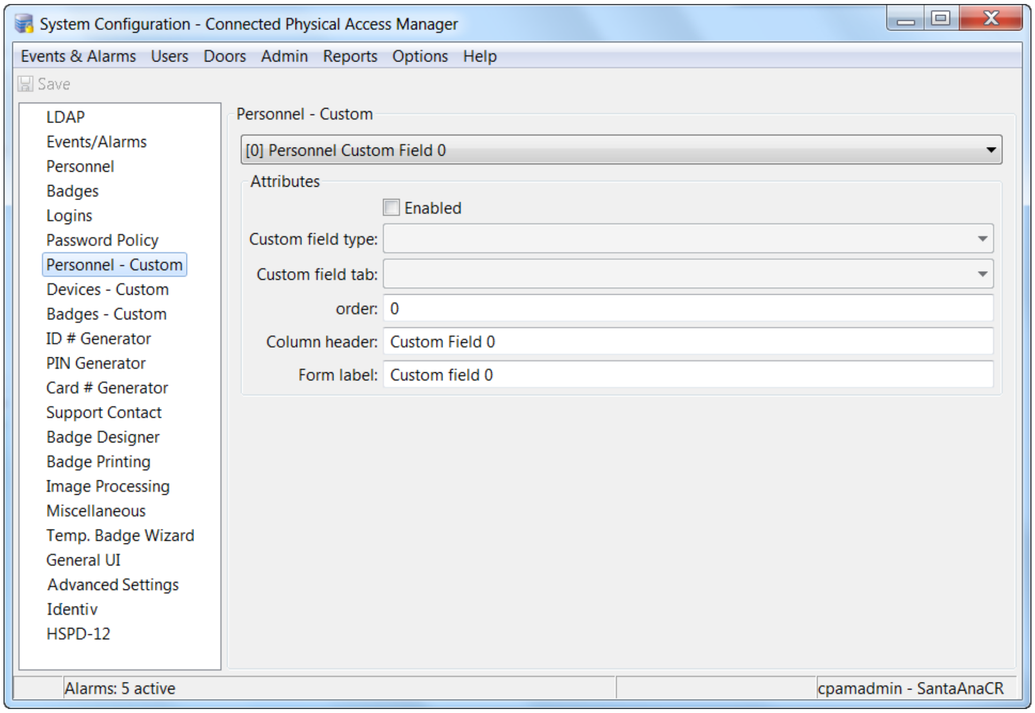
Field	Description
Minimum special characters	Minimum number of special characters in the set specified below.
Set of "special" characters	Which characters qualify as special characters for the above.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Personnel Custom Settings

The Custom Personnel fields define the custom fields available in the personnel detail window.

Figure 17-7 Personnel - Custom Fields



System Configuration - Connected Physical Access Manager

Personnel - Custom

[0] Personnel Custom Field 0

Attributes

□ Enabled

Custom field type:

Custom field tab:

order: 0

Column header: Custom Field 0

Form label: Custom field 0

Alarms: 5 active

cpamadmin - SantaAnaCR

Table 17-7 describes the Custom Personnel Fields settings.

Table 17-7 Personnel - Custom Fields

Field	Description
Custom Personnel Field	Selects which of the available custom fields is to be viewed or edited.
Enabled	Select the check box to enable the selected custom field.

Table 17-7 Personnel - Custom Fields (continued)

Field	Description
Custom field type	Displays the type of the custom field value (Example: Text, URL) to be associated with a custom field tab, and displays the selected type in the personnel and badges modules.
Custom field tab	Displays the custom field tab names in a drop-down list. To create more custom field tabs, refer to Custom Field Tabs, page 17-13.
Order	Displays custom personal fields in numerical order in the personnel module custom field.
Column header	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 such as the title of a book, for example: Driver's License Number.
Form label	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.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the **Options** menu).

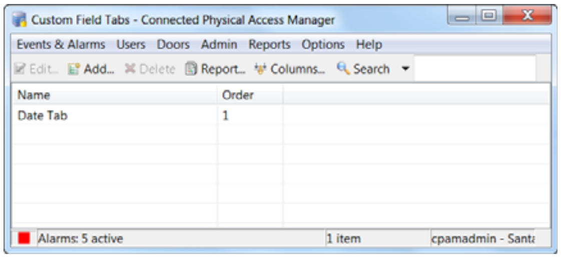
Custom Field Tabs

The Personnel - Custom window includes a 'Custom field tab' drop-down option list. This option list must be populated by tabs created by the Custom Field Tabs option.

To define new tabs, follow this procedure:

Step 1 From the **Admin** option, select **Custom Field Tabs**.

The Custom Field Tab window appears.

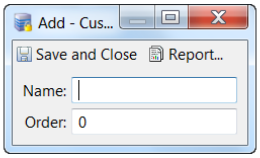

Custom Field Tabs - Connected Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add... Delete Report... Columns... Search

Name	Order
Date Tab	1

Alarms: 5 active 1 item cpamadmin - Santa

Step 2 Click **Add...**

The Add Custom Tab dialog box appears.



Name:
Order: 0

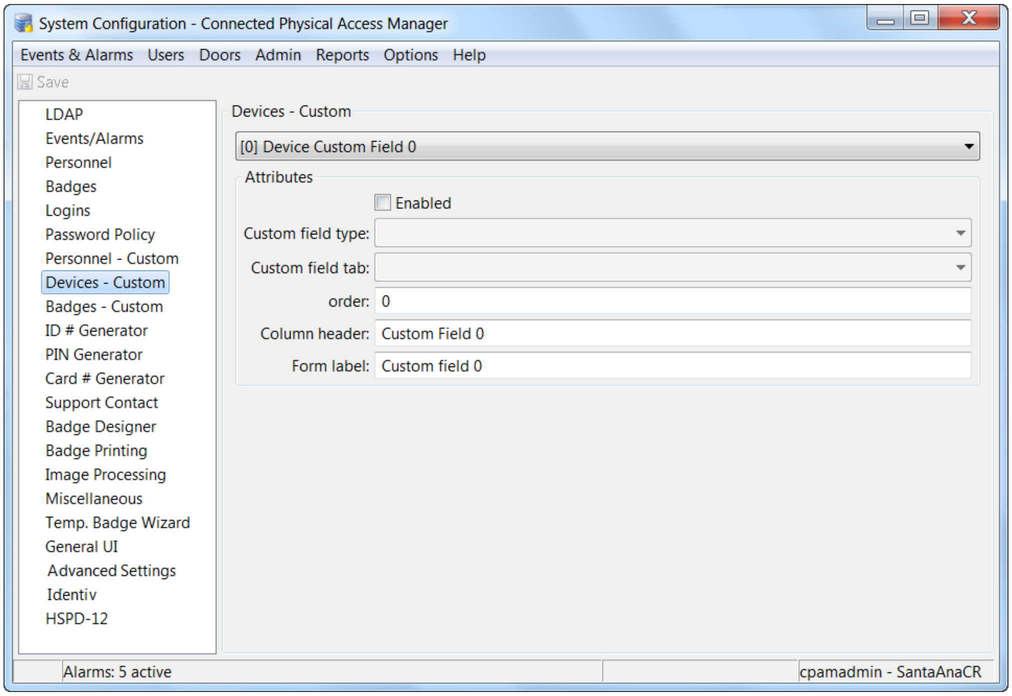
Step 3 Enter a name for this new tab and the order in which it is to be displayed in the option list (where 0 is the top of the list).

Step 4 Click **Save and Exit**.

Devices Custom Settings

This page determines which custom fields are available in the device detail window.

Figure 17-8 Custom Devices Fields



[0] Device Custom Field 0

□ Enabled

Custom field type:
Custom field tab:
order: 0
Column header: Custom Field 0
Form label: Custom field 0

Table 17-8 describes the Custom Device Fields settings.

Table 17-8 Custom Devices Fields Settings

Field	Description
Custom Device Fields	Selects which of the available custom fields is to be viewed or edited.
Enabled	Select the check box to enable the selected custom field.
Drop down	Select the check box to use a drop-down for entry the selected custom field.

Table 17-8 Custom Devices Fields Settings (continued)

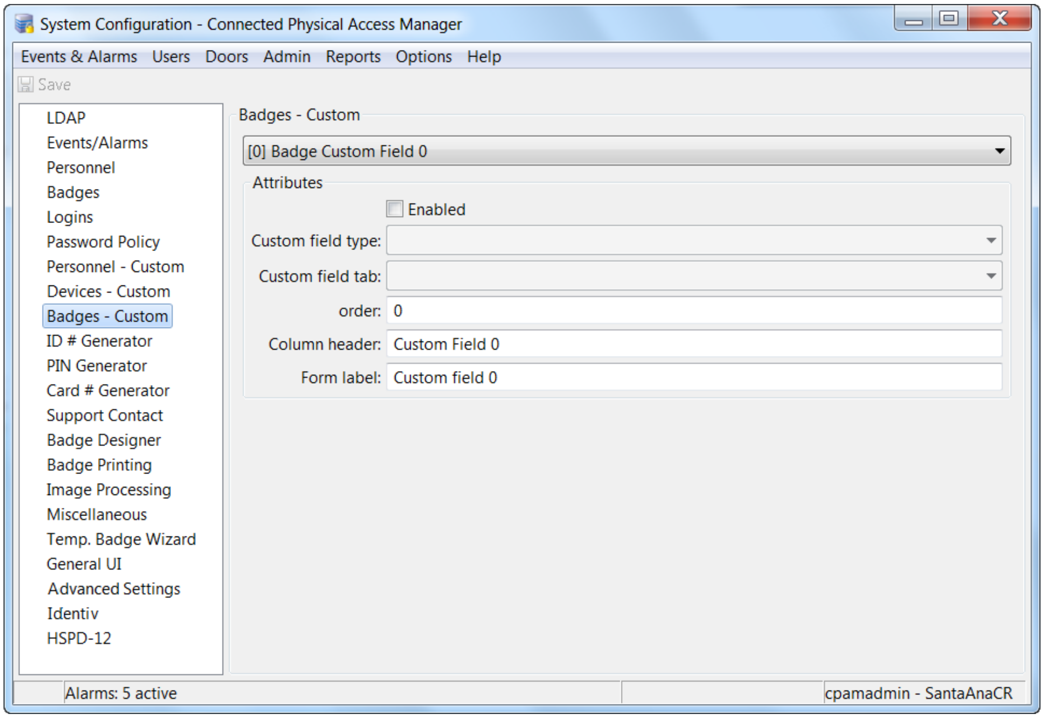
Field	Description
Column header	Change the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like the title of a book, for example, Serial Number.
Form label	Change 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.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Badges Custom Fields

This page determines which custom fields are available in the badge detail window.

Figure 17-9 Custom Badges Settings



Badges - Custom

[0] Badge Custom Field 0

Attributes

□ Enabled

Custom field type:

Custom field tab:

order: 0

Column header: Custom Field 0

Form label: Custom field 0

Alarms: 5 active

cpamadmin - SantaAnaCR

Table 17-9 Custom Badge Fields

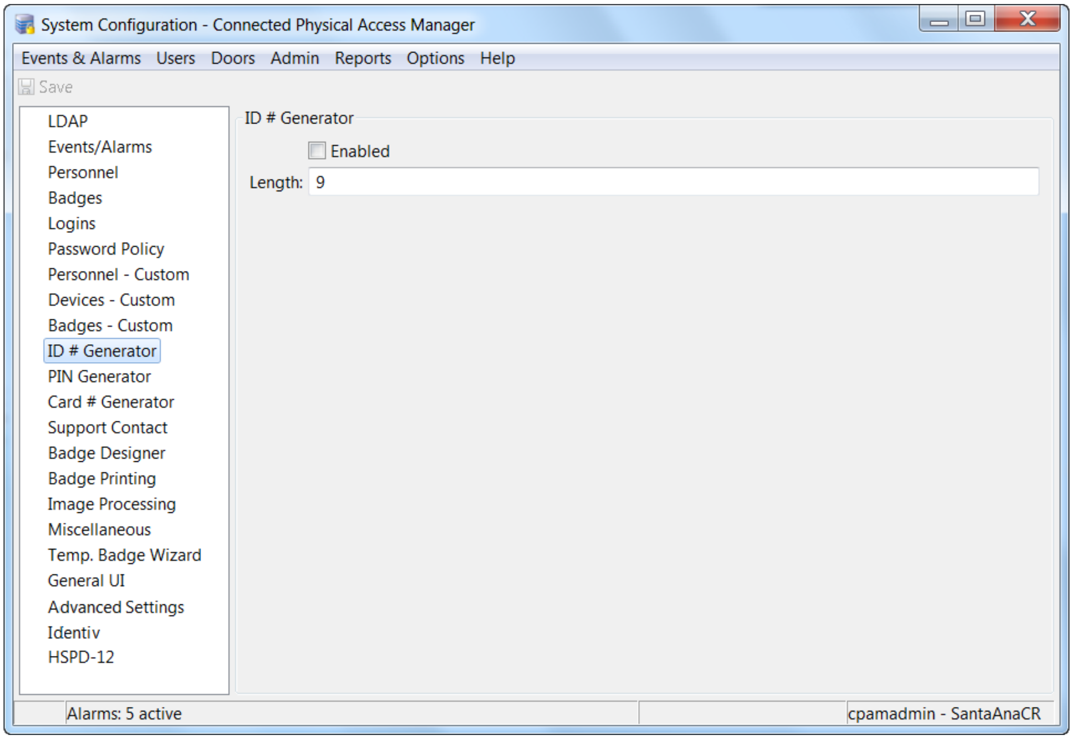
Field	Description
Custom Badge Fields	Selects which of the available custom fields is to be viewed or edited.
Enabled	Select the check box to enable the selected custom field.
Custom field type	Added custom field tab value is displayed in "custom field tab" drop down list of personal module and badge module.
Custom field tab	Add Custom field tabs value in custom field tabs window (Example: **Admin** > **Custom Field** tabs > **Add**) to display custom field tab value in personal module and badge module
Order	Displays custom personal fields in order in the personnel module custom field.
Column header	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.
Form label	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.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

ID Number Generator Settings

The 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 ID Number Generator Settings



ID # Generator

□ Enabled

Length: 9

Table 17-10 Personnel ID Number Generator Settings

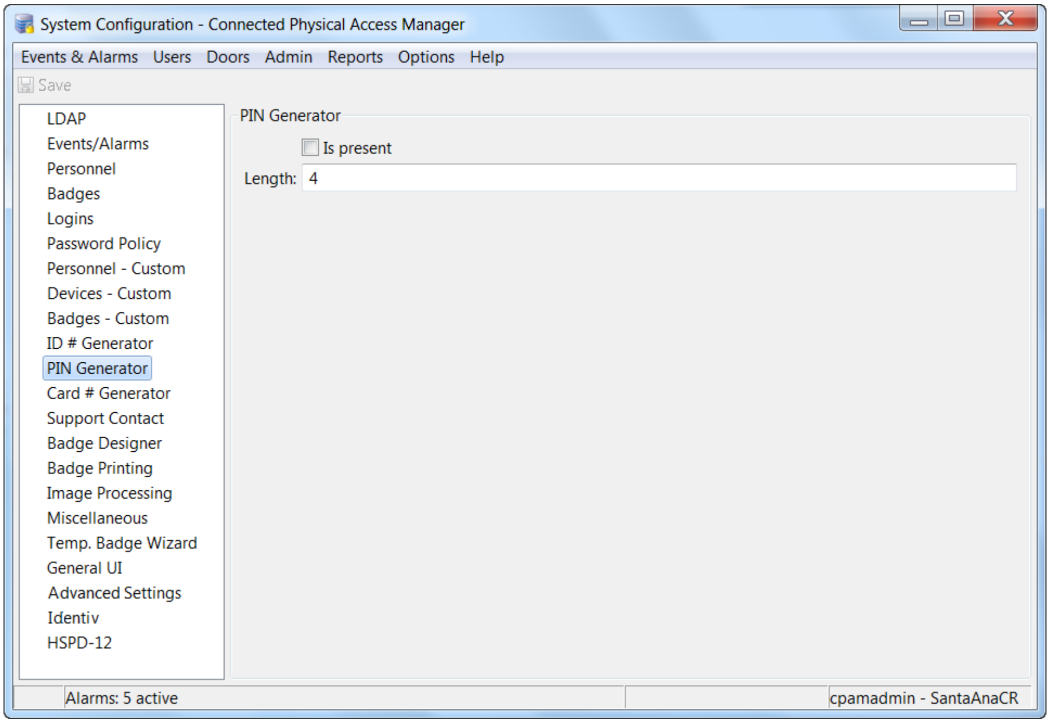
Field	Description
Enabled	Enables the personnel ID number generator. New personnel entries will have randomly generated ID numbers entered in the field.
Length	The digit length of generated IDs.

Note Changes to system configuration settings do not take effect until the ICPAM desktop application is restarted (exit and re-launch the application).

PIN Generator Settings

Use the PIN generator to generate random PIN numbers for badges.

Figure 17-11 PIN Generator Settings



PIN Generator

□ Is present

Length: 4

Alarms: 5 active

cpamadmin - SantaAnaCR

Table 17-11 PIN Generator Settings

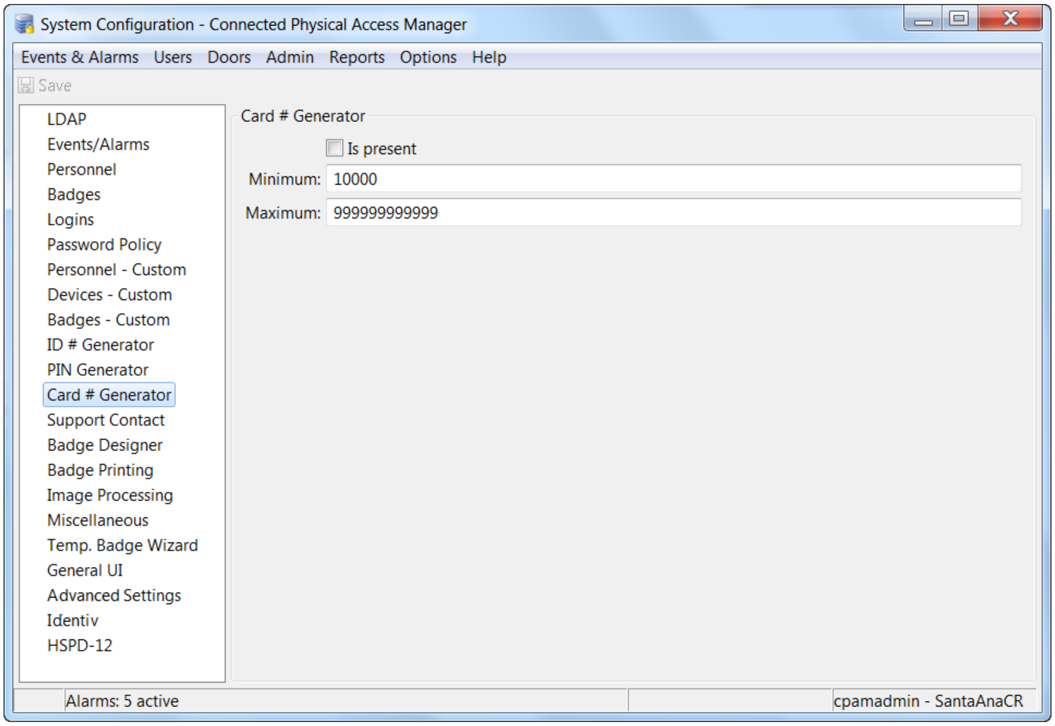
Field	Description
Is Present	Enable the personnel ID number generator. Adding new personnel will have randomly generated ID numbers entered in the field.
Length	The amount of digits in the generated PIN.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Card Number Generator Settings

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



□ Is present
Minimum: 10000
Maximum: 999999999999

Table 17-12 Card Number Generator Settings

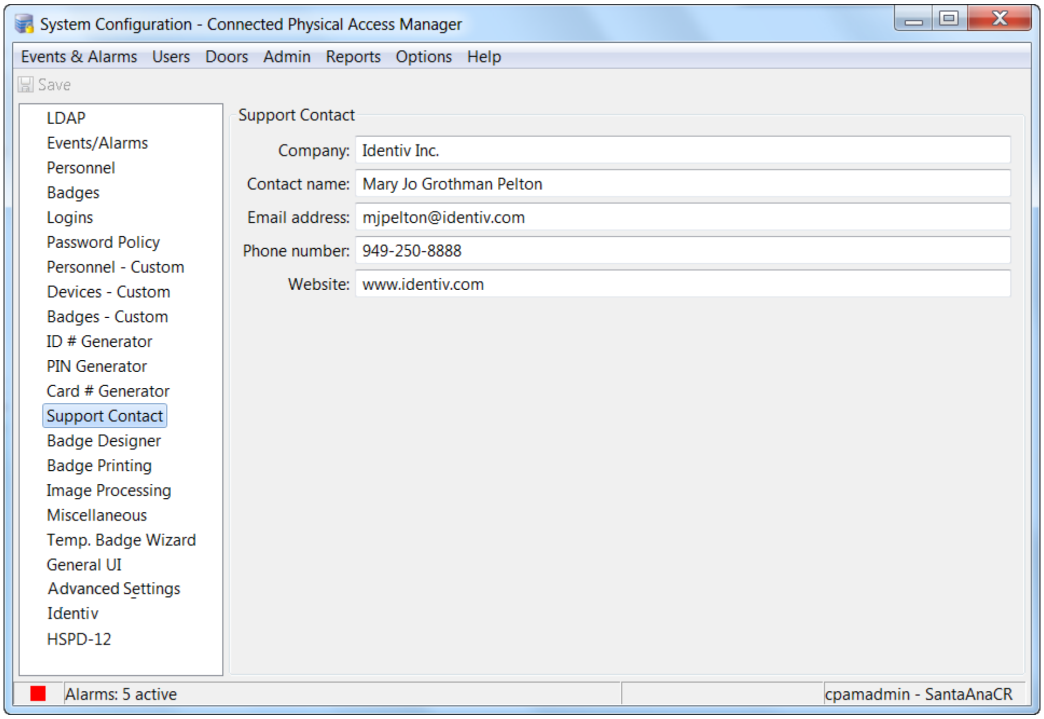
Field	Description
Is Present	Enables the card number generator. Adding new badges will have randomly generated card numbers entered in the **Card #** field.
Maximum	Maximum amount of card digits.
Minimum	Minimum amount of card digits.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Support Contact Information Settings

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



Company: Identiv Inc.
Contact name: Mary Jo Grothman Pelton
Email address: mjpelton@identiv.com
Phone number: 949-250-8888
Website: www.identiv.com

Table 17-13 Support Contact Information Settings

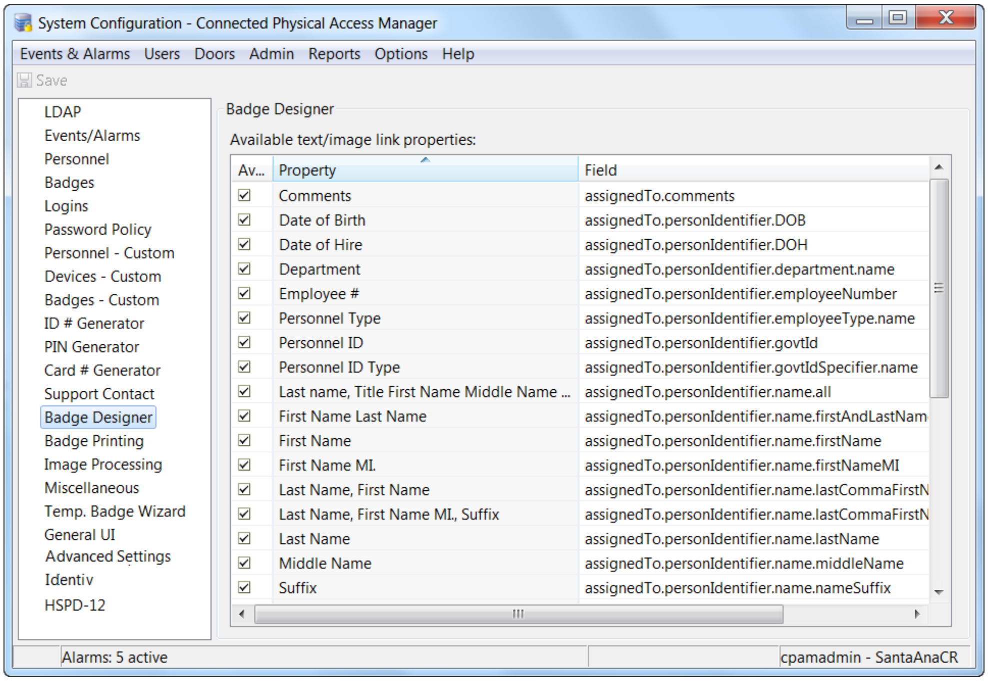
Field	Description
Company	Support company's name.
Contact name	The name of the contact person.
Contact person's email address	The contact person's email address.
Contact person's phone number	The contact person's phone number.
Company's website	Support company's company website address.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Badge Designer Settings

Figure 17-13 includes the fields on this tab.

Figure 17-14 Badge Designer Settings



Available text/image link properties:

Av...	Property	Field
☑	Comments	assignedTo.comments
☑	Date of Birth	assignedTo.personIdentifier.DOB
☑	Date of Hire	assignedTo.personIdentifier.DOH
☑	Department	assignedTo.personIdentifier.department.name
☑	Employee #	assignedTo.personIdentifier.employeeNumber
☑	Personnel Type	assignedTo.personIdentifier.employeeType.name
☑	Personnel ID	assignedTo.personIdentifier.govtId
☑	Personnel ID Type	assignedTo.personIdentifier.govtIdSpecifier.name
☑	Last name, Title First Name Middle Name ...	assignedTo.personIdentifier.name.all
☑	First Name Last Name	assignedTo.personIdentifier.name.firstAndLastNam
☑	First Name	assignedTo.personIdentifier.name.firstName
☑	First Name MI.	assignedTo.personIdentifier.name.firstNameMI
☑	Last Name, First Name	assignedTo.personIdentifier.name.lastCommaFirstN
☑	Last Name, First Name MI, Suffix	assignedTo.personIdentifier.name.lastCommaFirstN
☑	Last Name	assignedTo.personIdentifier.name.lastName
☑	Middle Name	assignedTo.personIdentifier.name.middleName
☑	Suffix	assignedTo.personIdentifier.name.nameSuffix

The fields on this screen include all of the fields included in the basic badge designer package. This page enables the user to include or exclude this field from the list of available fields when a badge is created. The three available columns are:

Table 17-14 Badge Designer Settings

Field	Description
Available	Check this property to include this option in the list of available field options in the badge designer. Uncheck this option to exclude this option from the list. The default value is all checked and included.
Property	The name of the option.
Field	The variables used to compute this field option.

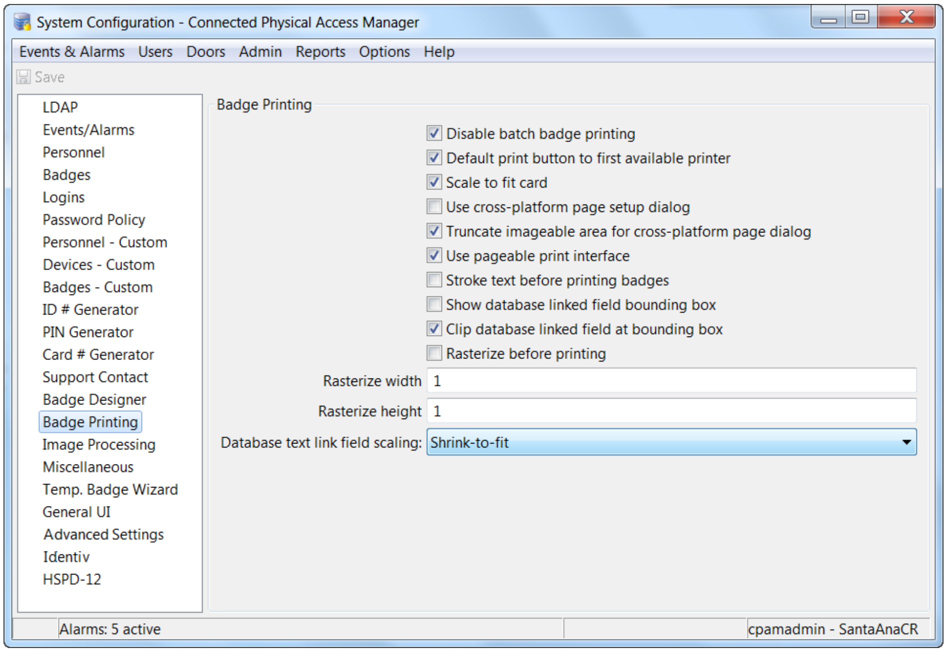
Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Badge Printing Settings

When you select the Badge Printing tab, a page like Figure 17-15 appears.

This page determines what features and fields appear during the badge printing operation.

Figure 17-15 Badge Printing Settings



Badge Printing

☑ Disable batch badge printing
☑ Default print button to first available printer
☑ Scale to fit card
☐ Use cross-platform page setup dialog
☑ Truncate imageable area for cross-platform page dialog
☑ Use pageable print interface
☐ Stroke text before printing badges
☐ Show database linked field bounding box
☑ Clip database linked field at bounding box
☐ Rasterize before printing

Rasterize width: 1
Rasterize height: 1
Database text link field scaling: Shrink-to-fit

The fields on this screen are described in Table 17-15.

Table 17-15 Badge Printing Settings

Field	Description
Disable batch badge printing	When checked, batch badge printing is not allowed.
Default print button to first available printer	When checked, the system defaults to the first available badge printer for printing a specified badge or badges.
Scale to fit card	When checked, the badge printer is instructed to scale the badge design and information to fit the size and dimensions of the card.
Use cross-platform page setup dialog	When checked, the program uses a cross-platform setup dialog box when printing is requested.
Truncate imageable area for cross-platform page dialog	When checked, the program will truncate the image area covered by the cross-platform page dialog box.
Use pageable print interface	When checked, the program is instructed to use a pageable print interface.
Stroke text before printing badges	When checked, the program is instructed to stroke the text before printing the badge.

Table 17-15 Badge Printing Settings

Field	Description
Show database linked field bounding box	When checked, the program displays the bounding box for any database link fields.
Clip database linked field at bounding box	When checked, the program will clip the database instruction field at the bounding box. Any instructions behind this box will be truncated.
Rasterize before printing	When checked, the program will rasterize any badge images before printing.
Rasterize width	When the 'Rasterize before printing' option is checked, the width of the rasterized field is specified here.
Rasterize height	When the 'Rasterize before printing' option is checked, the height of the rasterized field is specified here.
Database text link field scaling	Specify in this field the way in which the database text link field is scaled. The default is **Shrink-to-fit**.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Image Processing

Figure 17-16 displays an example of this page.

Figure 17-16 Image Processing Settings

\

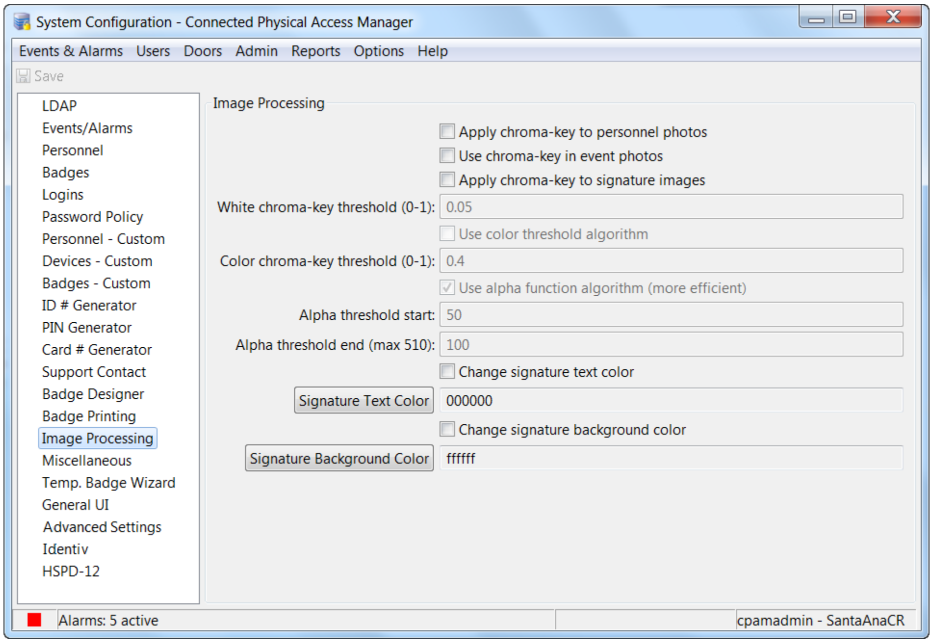


Image Processing

□ Apply chroma-key to personnel photos
□ Use chroma-key in event photos
□ Apply chroma-key to signature images

White chroma-key threshold (0-1): 0.05

□ Use color threshold algorithm

Color chroma-key threshold (0-1): 0.4

☑ Use alpha function algorithm (more efficient)

Alpha threshold start: 50

Alpha threshold end (max 510): 100

□ Change signature text color

Signature Text Color: 000000

□ Change signature background color

Signature Background Color: ffffff

The fields on this screen are described in Table 17-16.

Table 17-16 Image Processing Settings

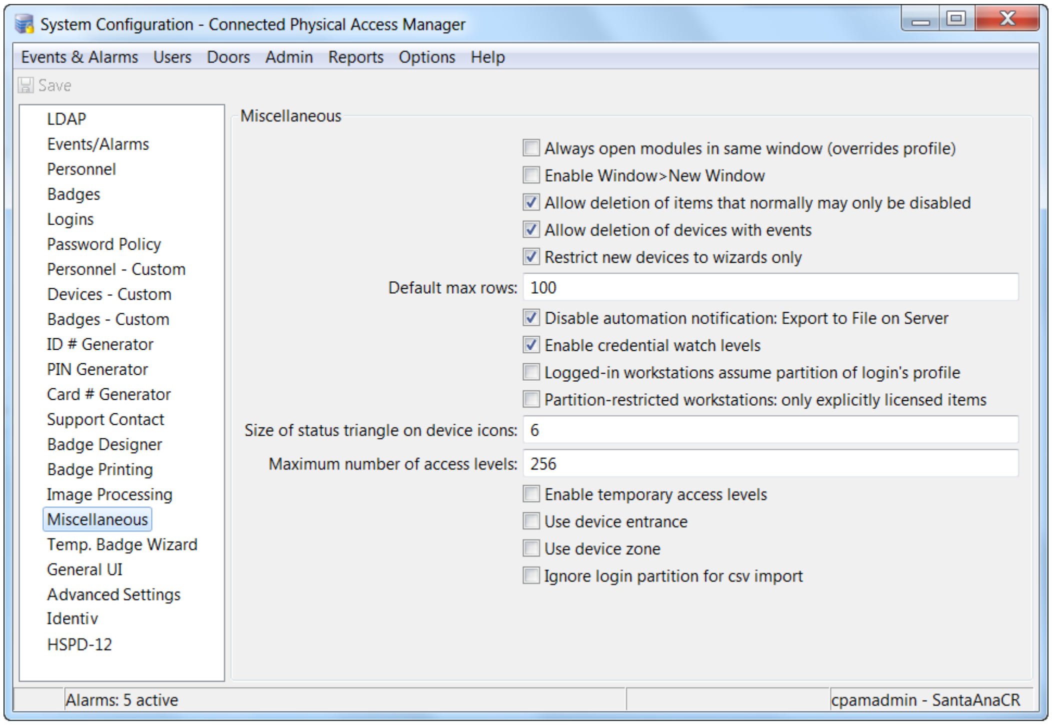
Field	Description
Apply chroma-key to personnel photos	When checked, the program applies chroma-key image processing to all personnel photos that are taken to the attached camera.
Use chroma-key in event photos	When checked, the program uses chroma-key image processing to massage any event photos that are taken.
Apply chroma-key to signature images	When checked, the program uses chroma-key to process all signatures that are captured.
White chroma-key threshold	Specify the threshold value applied to white when using chroma-key processing.
Color chroma-key threshold	Specify the threshold value applied to color when using chroma-key processing.
Alpha threshold start	Specify the alpha threshold start value applied to images.
Alpha threshold end	Specify the alpha threshold stop value applied to images.
Change signature text color	When checked, the color of the signature can be changed as specified in the following field.
Signature text color	Specify the color that will be substituted for the captured signature color.
Signature background color	Specify the color that will be substituted for the captured signature background color.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Miscellaneous Settings

When you select the Miscellaneous tab, a page (Figure 17-17) appears that includes settings described in Table 17-17.

Figure 17-17 Miscellaneous Settings



Miscellaneous

☐ Always open modules in same window (overrides profile)
☐ Enable Window>New Window
☑ Allow deletion of items that normally may only be disabled
☑ Allow deletion of devices with events
☑ Restrict new devices to wizards only
Default max rows: 100
☑ Disable automation notification: Export to File on Server
☑ Enable credential watch levels
☐ Logged-in workstations assume partition of login's profile
☐ Partition-restricted workstations: only explicitly licensed items
Size of status triangle on device icons: 6
Maximum number of access levels: 256
☐ Enable temporary access levels
☐ Use device entrance
☐ Use device zone
☐ Ignore login partition for csv import

Table 17-17 Miscellaneous Setting Fields

Field	Description
Always open new modules in same window	If checked, opening a new module simply replaces the module in the same window, rather than opening a new window.
Enable Window > New Window	Allows modules to be opened in multiple windows. Adds an additional **New Window** button to the toolbar.
Prevent force quit (Command-Q) on Mac OS X	Blocks the force quit command.
Allow deletion of items that normally may only be disabled	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.
Allow deletion of devices with events	Deletes events associated with a device when a device is deleted. **Note** Identiv recommends that you do not delete devices. Events that are associated with the device will be deleted if the device is deleted.
Restrict new devices to wizards only	All new devices added to the **Hardware - Tree** module will use an add wizard.

Table 17-17 Miscellaneous Setting Fields

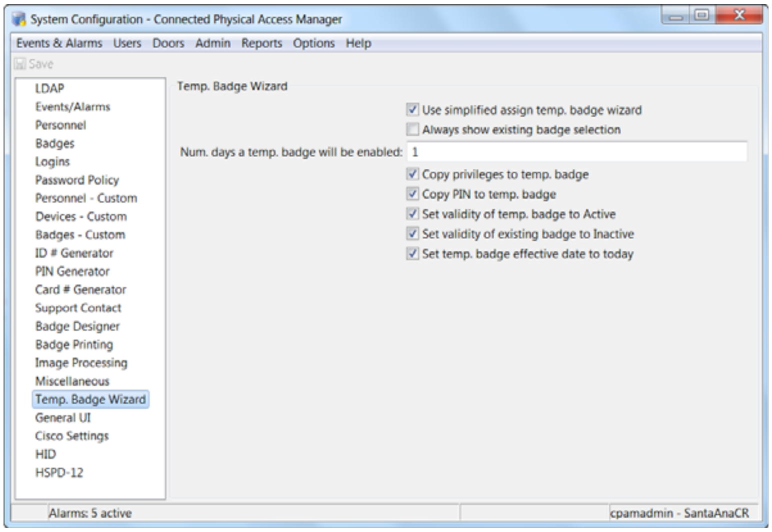
Field	Description
Default max rows	Limits the number of visible rows in list-based modules such as Events and Badges. For example, if the default max rows is set to 100, the badges module displays a maximum of 100 rows. Enter a number between 1 and 5000.
Change queue buffer size	Enter a new buffer size.
Logged in workstations assume partition of login's profile	not supported in 1.4.1, 1.5.0, or 2.1 versions.
Partition-restricted workstations only use explicitly assigned license items	not supported in 1.4.1, 1.5.0, or 2.1 versions.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Temporary Badge Wizard Settings

When you select the Temp. Badge Wizard tab, a page appears that includes fields that determine what features appear in the Temporary Badge Wizard.

Figure 17-18 Temporary Badge Wizard



Temp. Badge Wizard

☑ Use simplified assign temp. badge wizard

☐ Always show existing badge selection

Num. days a temp. badge will be enabled: 1

☑ Copy privileges to temp. badge

☑ Copy PIN to temp. badge

☑ Set validity of temp. badge to Active

☑ Set validity of existing badge to Inactive

☑ Set temp. badge effective date to today

The fields on this screen are described in Table 17-18.

Table 17-18 Temporary Badge Wizard Settings

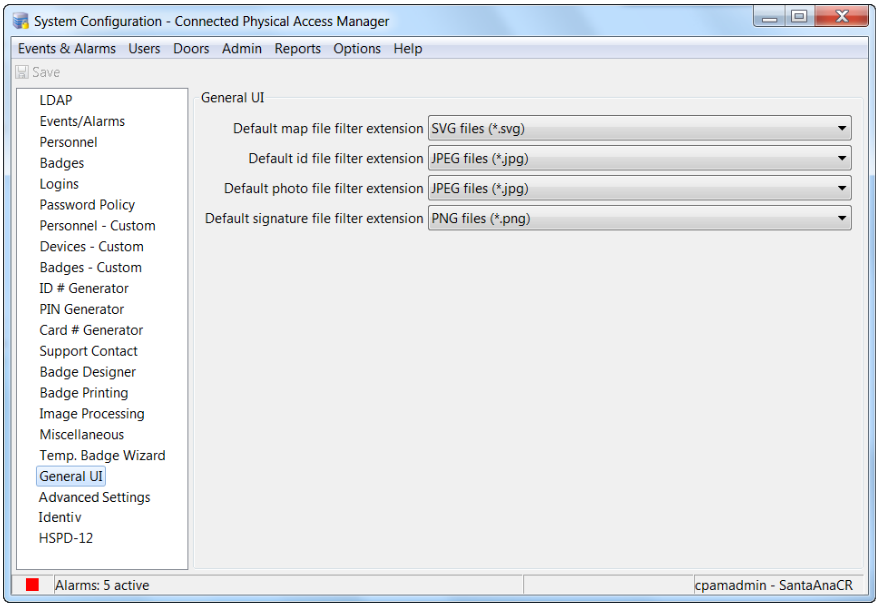
Field	Description
Use simplified assign temp. badge wizard	When checked, this program uses a shortened version of the temporary badge wizard.
Always shown existing badge selection	When checked, the wizard will always show the existing badge selection.
Number of days temp. badge is enabled	Specify the number of days the wizard assigns a temporary badge before the program invalidates it.
Copy privileges to temp. badge	When checked, the wizard allows privileges to be copied to a temporary badge.
Copy PIN to temp. badge	When checked, the wizard allows a PIN number to be copied to a temporary badge.
Set validity of temp. badge to Active	When checked, the wizard allows validity of a temporary badge to be set to active. Otherwise, the validity of the badge is inactive.
Set validity of existing badge to Active	When checked, the wizard allows the validity of an existing temporary badge to be set to active. Otherwise, the validity of the existing badge is inactive.
Set temp. badge effective date to today	When checked, the wizard assumes all temporary badges are valid from the moment they are created.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

General UI Settings

Figure 17-19 displays an example of the screen that appears when the General UI option is selected.

Figure 17-19 General UI Settings



Default map file filter extension: SVG files (*.svg)
Default id file filter extension: JPEG files (*.jpg)
Default photo file filter extension: JPEG files (*.jpg)
Default signature file filter extension: PNG files (*.png)

Alarms: 5 active
cpamadmin - SantaAnaCR

The fields on this screen are described in Table 17-19.

Table 17-19 General UI Settings

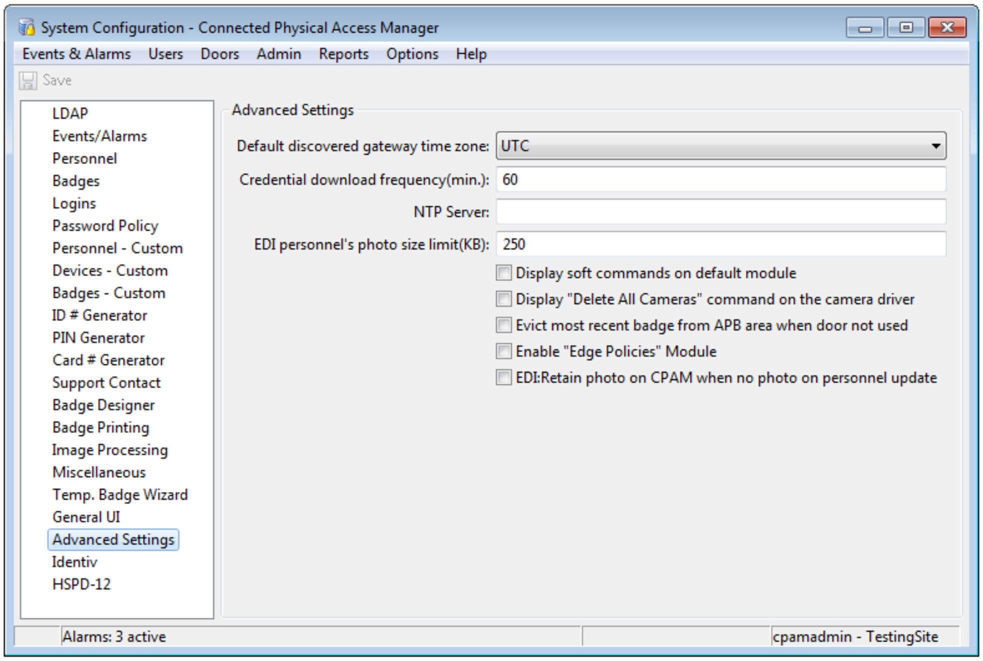
Field	Description
Default map file filter extension	Specify the extension applied to the map file filter by default.
Default ID file filter extension	Specify the extension applied to an ID file filter by default.
Default photo file filter extension	Specify the extension applied to a photo file filter by default.
Default signature file filter extension	Specify the extension applied to a signature file filter by default.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Advanced Settings

Figure 17-20 includes the settings described in Table 17-17.

Figure 17-20 Advanced Settings



Advanced Settings

Default discovered gateway time zone: UTC

Credential download frequency(min.): 60

NTP Server:

EDI personnel's photo size limit(KB): 250

□ Display soft commands on default module

□ Display "Delete All Cameras" command on the camera driver

□ Evict most recent badge from APB area when door not used

□ Enable "Edge Policies" Module

□ EDI:Retain photo on CPAM when no photo on personnel update

Alarms: 3 active

cpamadmin - TestingSite

Note To activate changes made to Advanced Settings, either log out and log back in, or restart the ICPAM appliance. To restart the appliance, see Using the Web Admin Menus, Commands and Options, page 2-18, or ask your system administrator for assistance.

Table 17-20 Advanced Settings Fields

Field	Description	To Activate Changes:
Default discovered gateway time zone	Defines the time zone for all discovered gateways. This time zone is configured on all discovered gateways.	Restart the ICPAM appliance.
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 - Tree** from the **Doors** menu, right-click on the **Access GW Driver**, and select **Apply Credential Changes**. See Configuring Personnel, page 9-1 for more information.	Restart the ICPAM appliance.

Table 17-20 Advanced Settings Fields (continued)

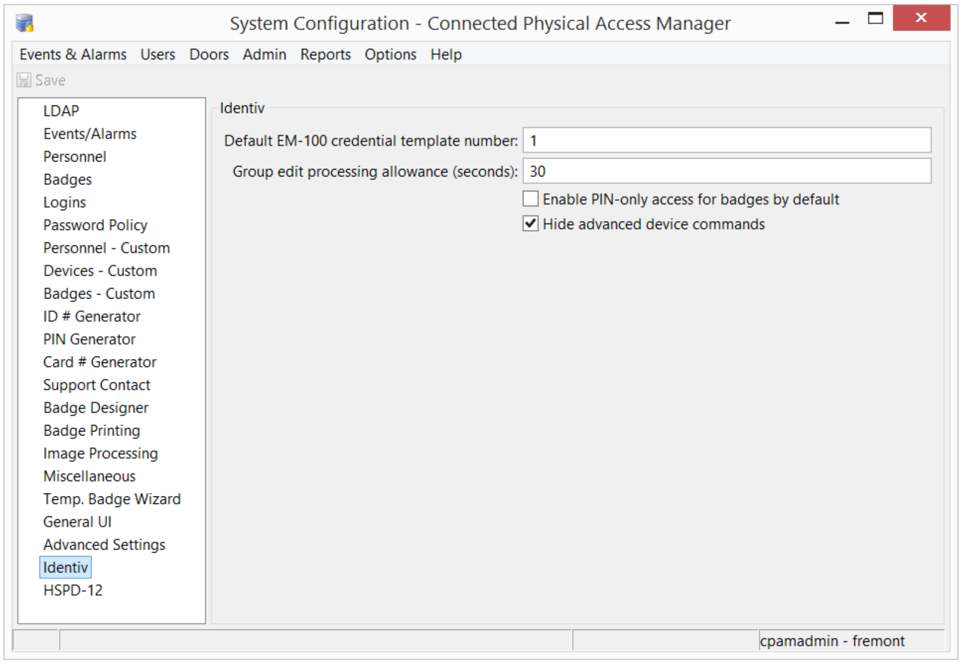
Field	Description	To Activate Changes:
NTP Server	Defines a default NTP server when updating multiple gateways. See the "Changing the NTP Setting for Multiple Gateways" section on page C-6.	Log out and log in.
EDI personnel's photo size limit	Defines the maximum file size for imported photo files using 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. • Enter a value, in kb, between 50 and 750. • The default value is 250 kb. See the "Understanding Photo File Compression When Importing Personnel Records" section on page 14-12.	Log out and log in.
Display soft commands on default module	Displays the soft commands for the default m01 gateway module.	Log out and log in.
Display "Delete All Cameras" command on the camera driver	Displays the **Delete All Cameras** command for the Cisco VSM Video Driver in the Hardware - Tree module. See Deleting the Cisco VSM Cameras, page 15-30.	Log out and log in.
Evict most recent badge from APB area when door not used	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 controller. 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**. See the "Evicting a Badge from APB if the User Does Not Enter the APB Area" section on page 11-24	Restart the ICPAM appliance.
Enable "Edge Policies" Module	Enables the Edge Policies module. See the "Configuring Edge Policies" section on page 13-9.	Log out and log in.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

Identiv Settings

When you select the **Identiv** option, a page like the following example (Figure 17-21) appears.

Figure 17-21 Identiv Settings



Identiv

Default EM-100 credential template number: 1

Group edit processing allowance (seconds): 30

☐ Enable PIN-only access for badges by default

☑ Hide advanced device commands

The fields on this screen are described in Table 17-21.

Table 17-21 Identiv Settings

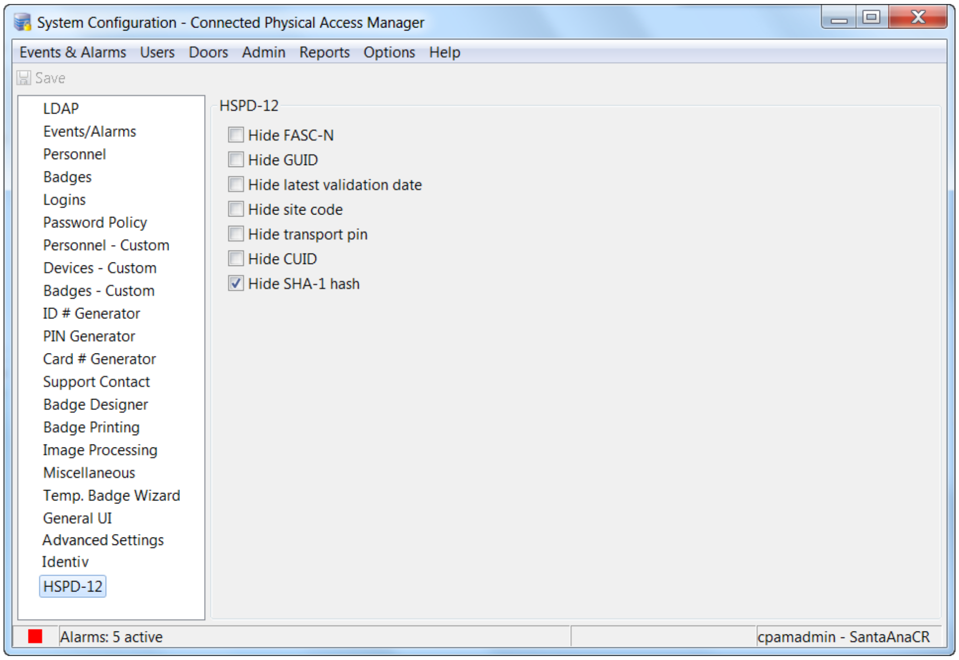
Field	Description
Default EM-100 credential template number	Enter the number of default credential templates.
Group edit processing allowance (seconds)	Enter the time in seconds the program allows for processing group edits.
Enable PIN-only access for badges by default	Check this option to enable PIN-only access for issued badges.
Hide advanced device commands	Check this option to hide all advanced device commands.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

HSPD-12 Settings

Figure 17-22 includes the settings described in Table 17-22.

Figure 17-22 HSPD-12 Settings



HSPD-12

- □ Hide FASC-N
- □ Hide GUID
- □ Hide latest validation date
- □ Hide site code
- □ Hide transport pin
- □ Hide CUID
- ☑ Hide SHA-1 hash

The fields on this screen are described in Table 17-22.

Table 17-22 HSPD-12 Settings

Field	Description
Hide FASC-N	Check this option to hide FASC-N-related fields
Hide GUID	Check this option to hide GUID-related fields
Hide latest validation date	Check this option to hide the latest validation date for personnel.
Hide site code	Check this option to hide the site code field.
Hide transport pin	Check this option to hide the transport PIN field.
Hide CUID	Check this option to hide CUID-related fields.
Hide SHA-1 hash	Check this option to hide any SHA-1 hashing from view.

Note Changes to system configuration settings do not take effect until you log out and log back in to the ICPAM application (select **Logout** from the Options menu).

APPENDIX **A**

Backing Up and Restoring Data

This appendix describes how to backup and restore the ICPAM 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 ICPAM Server Software from a Recovery CD, page B-21 for more information.

Contents

Backing up the ICPAM Database

Use the backup option in the ICPAM Server Administration utility to back up all ICPAM 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-5

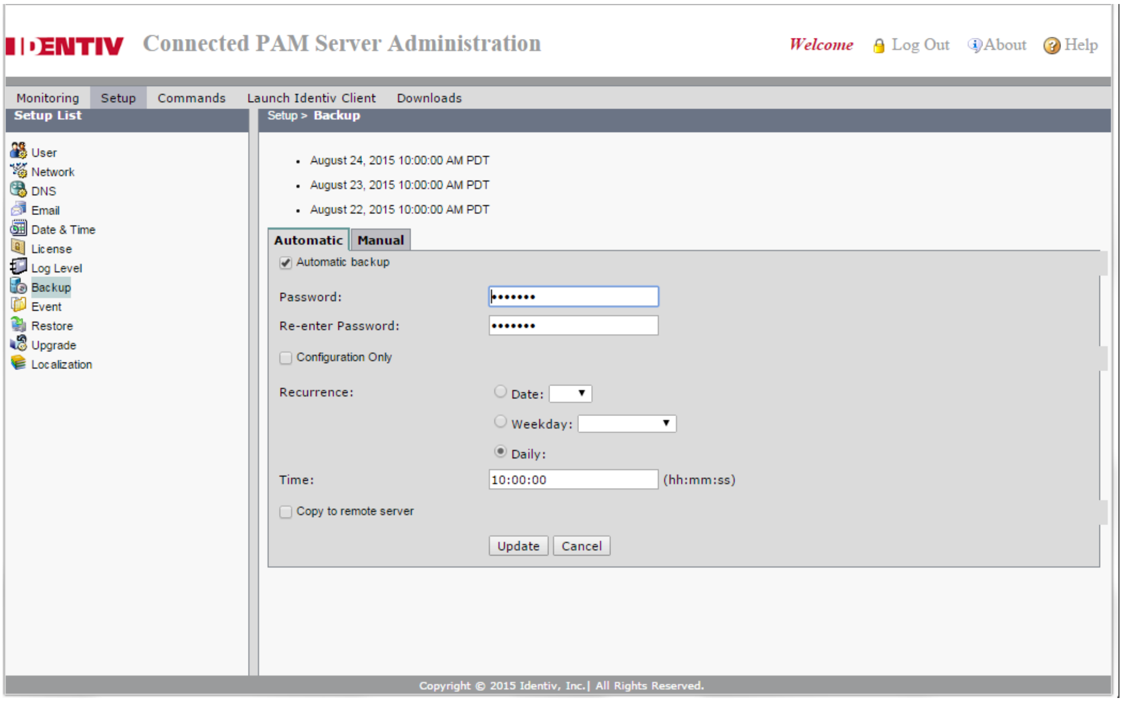
Backup Usage Notes

- 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-7 for more information. See the "Archiving Historical Events" section on page 2-25 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 ICPAM 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.

Figure A-1 Backup Window in the ICPAM Server Administration Utility



IDENTIV Connected PAM Server Administration

Welcome | Log Out | About | Help

Monitoring | Setup | Commands | Launch Identiv Client | Downloads

Setup List

- User
- Network
- DNS
- Email
- Date & Time
- License
- Log Level
- Backup
- Event
- Restore
- Upgrade
- Localization

Setup > Backup

- August 24, 2015 10:00:00 AM PDT
- August 23, 2015 10:00:00 AM PDT
- August 22, 2015 10:00:00 AM PDT

Automatic | Manual

☑ Automatic backup

Password: •••••••

Re-enter Password: •••••••

☐ Configuration Only

Recurrence: ○ Date: ○ Weekday: ● Daily:

Time: 10:00:00 (hh:mm:ss)

☐ Copy to remote server

Update | Cancel

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

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 ICPAM version number, and other information. For example: `bak-02062011-1422251.3.0_0.3.25.cpam-132`.

Procedure

To define automatic backups of the ICPAM data and configurations, do the following:

Step 1 Log on to the ICPAM appliance as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

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-7.
- 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 2-25.

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:

- **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 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 ICPAM server.

Step 8 Click **Update** to save the changes. Backups will occur according to the scheduled day(s) and time.

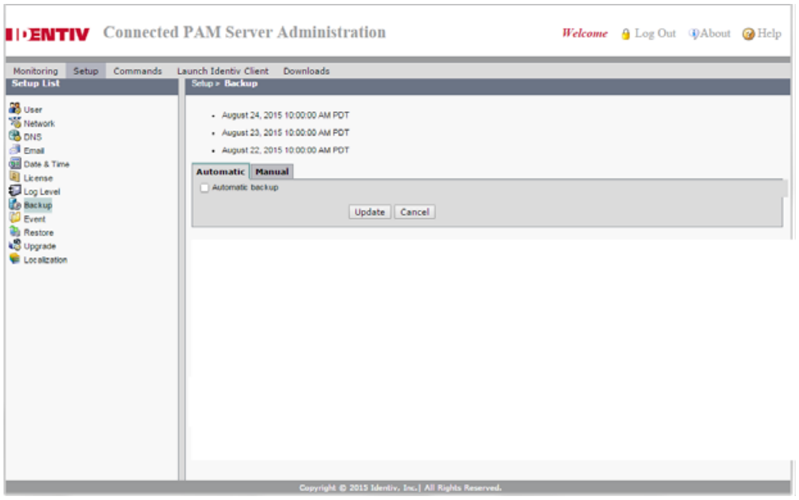
- When the backup is complete, the new backup file is added to the top of the screen, as shown in Figure A-1.
  - The backup name includes the date and the server software version number. For example: `February 06, 2011 02:22:25 PM PST`.
  - The three most recent backup files are saved to the ICPAM server. 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 ICPAM server even if the remote server in unavailable.

Disabling Automatic Backups

To disable automatic backups, deselect the Automatic backup check box (Figure A-2).

Figure A-2 Disabling Automatic Backups



- August 24, 2015 10:00:00 AM PDT
- August 23, 2015 10:00:00 AM PDT
- August 22, 2015 10:00:00 AM PDT

□ Automatic backup

Procedure

Step 1 Log on to the ICPAM appliance as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

Step 2 Select **Setup** and then **Backup**, as shown in Figure A-2.

Step 3 Select the **Automatic** tab.

Step 4 Deselect the **Automatic backup** check box.

Step 5 Click Update.

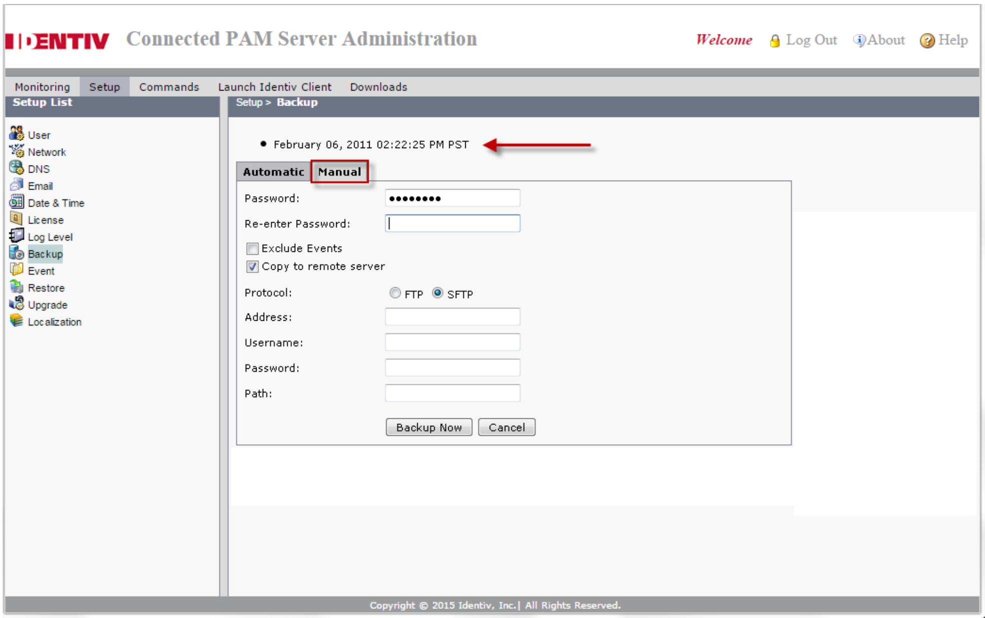
Step 6 (Optional) Perform a manual backup, if necessary. See the "Performing a One-Time Manual Backup" section on page A-5.

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 sever. 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



- February 06, 2011 02:22:25 PM PST

Password: ••••••••

Re-enter Password:

□ Exclude Events

☑ Copy to remote server

Protocol: ○ FTP ● SFTP

Address:

Username:

Password:

Path:

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 ICPAM 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 ICPAM appliance as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

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.

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-7.
- 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 2-25.

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 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 ICPAM 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 ICPAM 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 ICPAM server even if the remote server in unavailable.

Archiving the Historical Events Database

When you copy and prune old events (as described in "Archiving Historical Events" section on page 2-25) the events are moved to a separate ICPAM 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 2-25).

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 2-7 for instructions.

To modify these settings, use the ICPAM Server Administration utility, as described in the "Archiving Historical Events" section on page 2-25.

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 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 ICPAM 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-7 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 ICPAM 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 2-25 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 ICPAM Database, page A-1.

Step 2 Stop the Standby server, if installed.

Note

- For redundant HA configurations, ensure that both the Active and Standby servers are stopped (in **Down** state). Restoring a backup while either of the servers is up will result in unexpected behavior.
- If you are upgrading or reinstalling the server software, the Standby server should already be in the Down state.

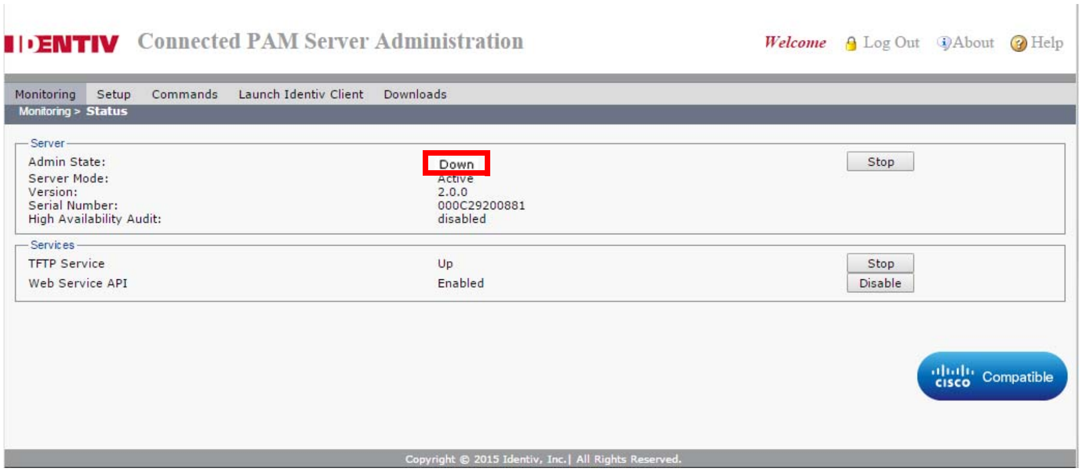
a. Log on to the Standby ICPAM appliance.

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.

Figure A-4 Server Admin State (Down) for the Active Server



Server

Admin State: Down

Server Mode: Active

Version: 2.0.0

Serial Number: 000C29200881

High Availability Audit: disabled

Services

TFTP Service Up

Web Service API Enabled

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Step 3 Stop the Active server.

Note

- For redundant HA configurations, ensure that both the Active and Standby servers are **Down** (Admin State). Restoring a backup while either of the servers is up will result in unexpected behavior.
- If you are upgrading or reinstalling the server software, the Standby server should already be in the Down state.

a. Log on to the Active ICPAM appliance.

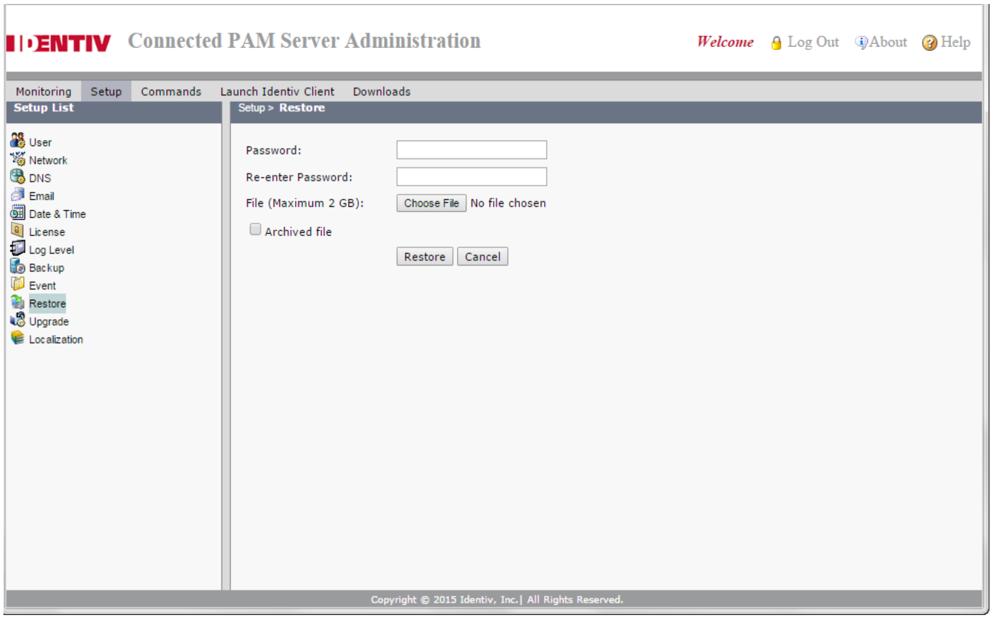
b. Select **Monitoring** and then select **Status**.

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 ICPAM Server Administration Utility



Password:

Re-enter Password:

File (Maximum 2 GB): No file chosen

□ Archived file

Step 5 Enter and re-enter the password for the backup file. This is the password entered when the backup file was created, as described in Backing up the ICPAM 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** check box.

See Archiving the Historical Events Database, page A-7 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 ICPAM 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.

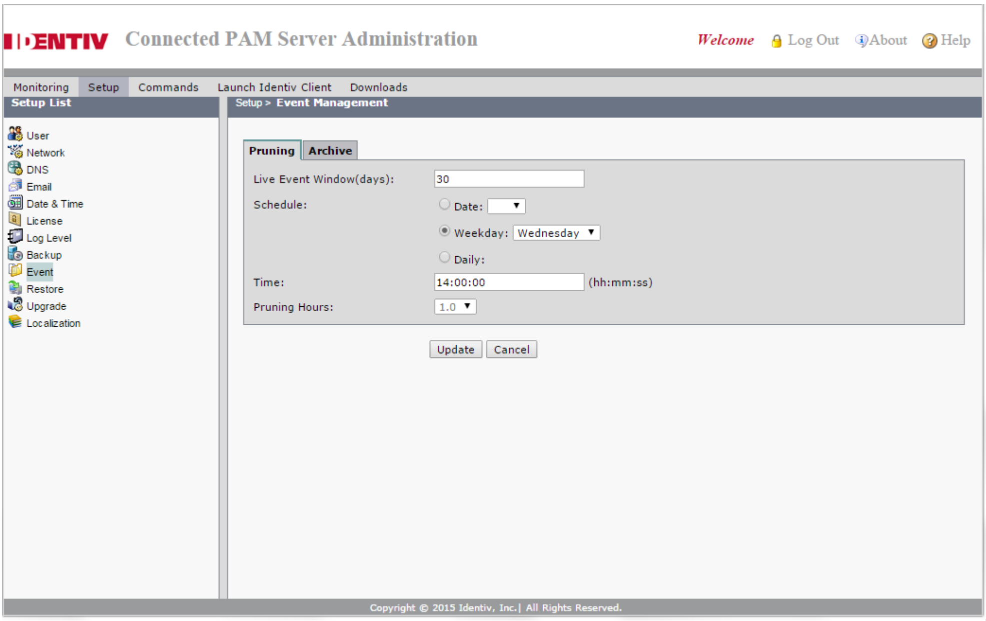
Step 10 If restoring a backup from Release 1.2.0 or earlier to Release 1.3.0 or higher, you must enter the event pruning and archive settings, as shown in Figure A-6.

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 ICPAM 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 ICPAM 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 2-25 for more information.

Figure A-6 Initial Setup: Event Pruning and Archiving



Live Event Window(days): 30

Schedule: ○ Date: ▼ ● Weekday: Wednesday ▼ ○ Daily:

Time: 14:00:00 (hh:mm:ss)

Pruning Hours: 1.0 ▼

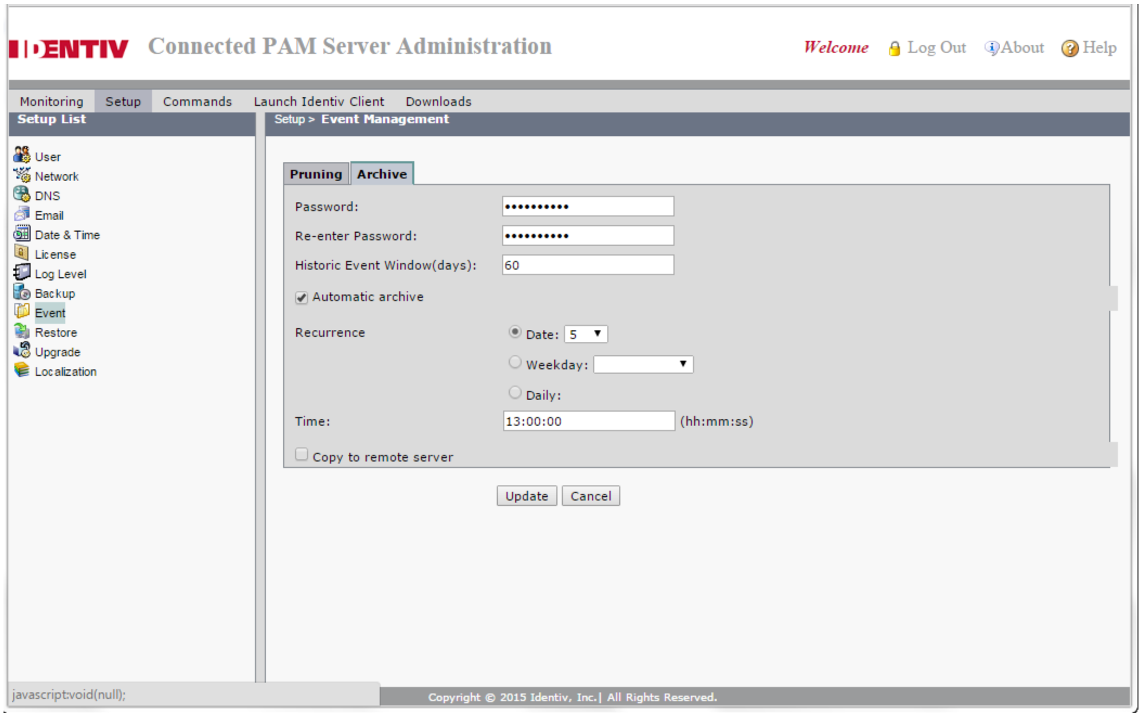
a. Select the **Pruning** tab (Figure A-6), and enter the following settings:

- **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).

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.

- **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`.

Figure A-7 Archiving Events


IDENTIV Connected PAM Server Administration
Welcome Log Out About Help
Monitoring Setup Commands Launch Identiv Client Downloads
Setup List
User
Network
DNS
Email
Date & Time
License
Log Level
Backup
Event
Restore
Upgrade
Localization
Setup > Event Management
Pruning Archive
Update Cancel
javascript:void(null);
Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Password: ••••••••••

Re-enter Password: ••••••••••

Historic Event Window(days): 60

☑ Automatic archive

Recurrence ● Date: 5 ○ Weekday: ○ Daily:

Time: 13:00:00 (hh:mm:ss)

□ Copy to remote server

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 2-25.

- 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 11 Verify that the Active server is up.

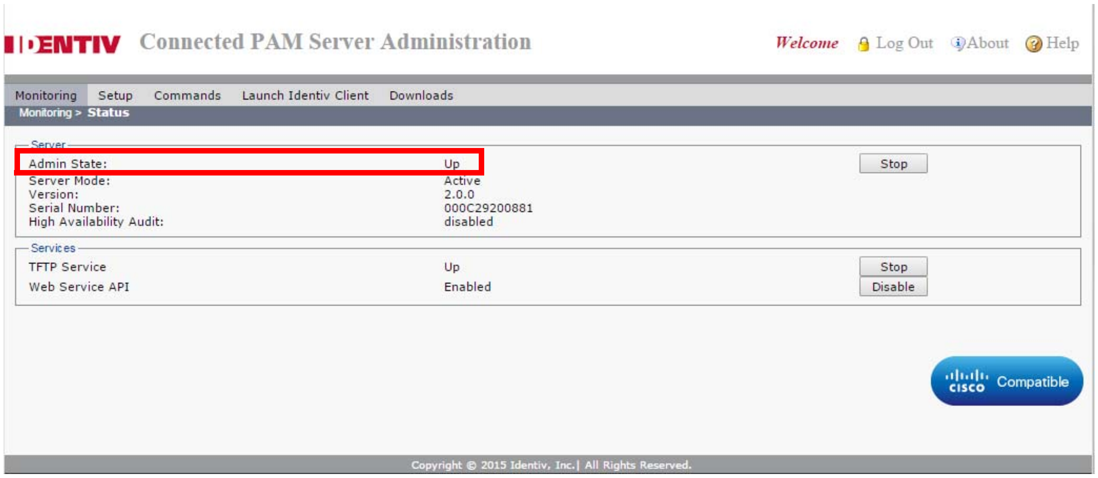
a. Log on to the Active ICPAM appliance.

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



Admin State: Up
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

TFTP Service Up
Web Service API Enabled

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 ICPAM 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**.

APPENDIX B

Upgrading the Server Software

This appendix describes how to upgrade or reinstall the ICPAM server software, desktop client software, and controller firmware.

Contents

Upgrade Notes for Release 2.1

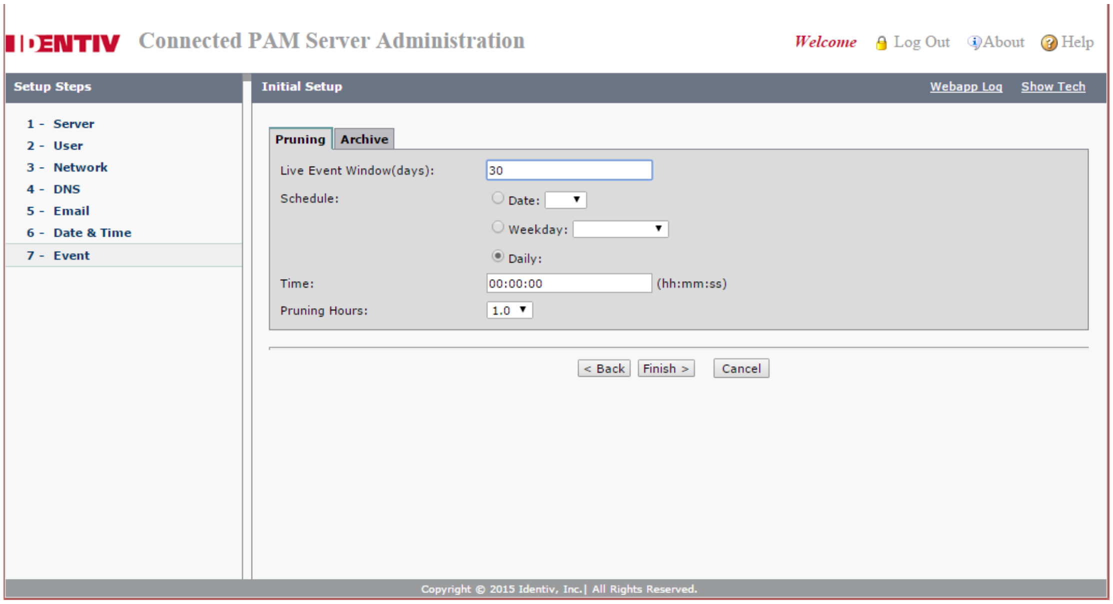
The upgrade topics and their associated notes are discussed in the following subsections.

- Event Archive Settings Are Required, page B-3
- Localization Feature Requires Database Upgrade, page B-4
- Controller Firmware Must Be the Same Version as ICPAM, page B-4
- Credential Download Frequency Must be 60 Minutes or Higher, page B-4
- Door Groups Feature Added to Device Groups, page B-5
- Enabling the Password Recovery Feature, page B-5
- Upgrading From Release 1.3.0 to Release 2.1, 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 ICPAM Desktop Client Software, page B-7
- Java Requirements, page B-7
- Stop EDI Projects Before Upgrading ICPAM, 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
- Controller Firmware Must Be the Same Version as ICPAM, 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 1.3.0 to Release 2.1, page B-5
- Split Holiday Schedule Configurations By Month, page B-5
- Browser Time-out, page B-7
- Upgrade the ICPAM Desktop Client Software, page B-7
- Java Requirements, page B-7
- Stop EDI Projects Before Upgrading ICPAM, 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 ICPAM Server Administration utility (Figure B-1).

Figure B-1 Initial Setup: Event Pruning and Archiving



Live Event Window(days): 30

Schedule:
○ Date:
○ Weekday:
● Daily:

Time: 00:00:00 (hh:mm:ss)

Pruning Hours: 1.0

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:

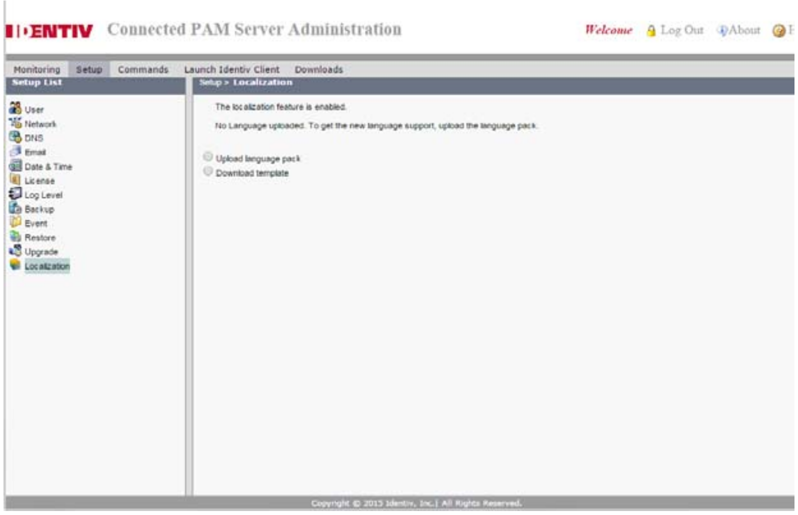
- If you are upgrading redundant HA servers, the historical event archive settings are only required on the primary appliance.
- If the appliance being upgraded has existing automation rules configured for historical events, the following occurs during the upgrade:
  - Commands to copy, prune or archive 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 2-25.

Localization Feature Requires Database Upgrade

If you upgrade the ICPAM appliance from release 1.4.1 or lower to release 1.5.0 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 (Figure B-2).

Figure B-2 Enabling Localization



The localization feature is enabled.

No Language uploaded. To get the new language support, upload the language pack.

○ Upload language pack
○ Download template

Copyright © 2013 Identiv, Inc.| All Rights Reserved.

Note

- 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 2-30.

Controller Firmware Must Be the Same Version as ICPAM

Controllers must have the same firmware version as the ICPAM appliance server software. This includes the major version, minor version, maintenance version, and the build number. If any difference in versions exists between the controller 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 controllers.

To access the **Credential download frequency** setting, see Advanced Settings, page 17-29.

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 ICPAM 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 1.3.0 to Release 2.1

To upgrade to Cisco PAM Release 2.1 from Release 1.3.0, you must first upgrade to ICPAM Release 1.5.0.

Post Upgrade:

- The doors without any location will be moved to the gateway or 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 for 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.

Select the Following Options When Upgrading Gateway Firmware

When upgrading gateway firmware images to ICPAM Release 2.1 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 ICPAM 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 ICPAM, page C-11 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 CPAM 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.

See *Cisco Physical Access Gateway User Guide* for more information on module and device wiring.

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:

Release 1.0.0 Command Name	Release 1.1.0 and Higher Command Name
Turn output off	Activate Relay
Turn output on	Deactivate Relay

The following generic output device event names were changed for Release 1.1.0. The functionality is the same:

Release 1.0.0 Event Name	Release 1.1.0 and Higher Event Name
Output Off	Output Deactivated
Output On	Output Activated

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 ICPAM Desktop Client Software

Always upgrade the ICPAM 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 ICPAM Desktop Software, page 3-2.

Java Requirements

Before installing the ICPAM client, ensure that your PC has Oracle Java Runtime Environment (JRE) 1.7 32-bit installed.

- To install Java 1.7, log on to the server administration console, select **Downloads**, and then select **JRE 1.7 (Windows)**.
- To download the latest Java, go to http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html.

Stop EDI Projects Before Upgrading ICPAM

Stop any running EDI projects before upgrading the ICPAM appliance software. After the upgrade, re-import the project to EDI Administration and start it again. See Importing, Starting, and Monitoring EDI Projects in ICPAM, page 14-37 for instructions to stop, start and import EDI projects.

If EDI projects are not stopped before a ICPAM upgrade, the project execution (or run) will not be successful. If this occurs, contact your Identiv 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 ICPAM 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

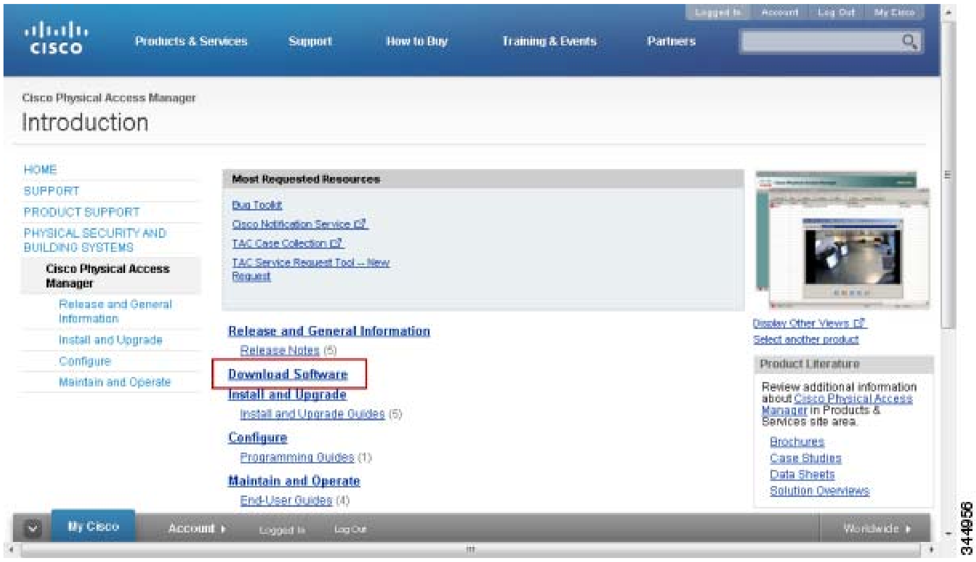
To access the self-service portal and obtain software, documents, and tools, do the following:

Step 1 Go to the following URL: http://www.identiv.com

Tip You can also log into the Identiv Support Center at http://www.identiv.com/support-icpam.

Step 2 Click the **Download Software** link (Figure B-3).

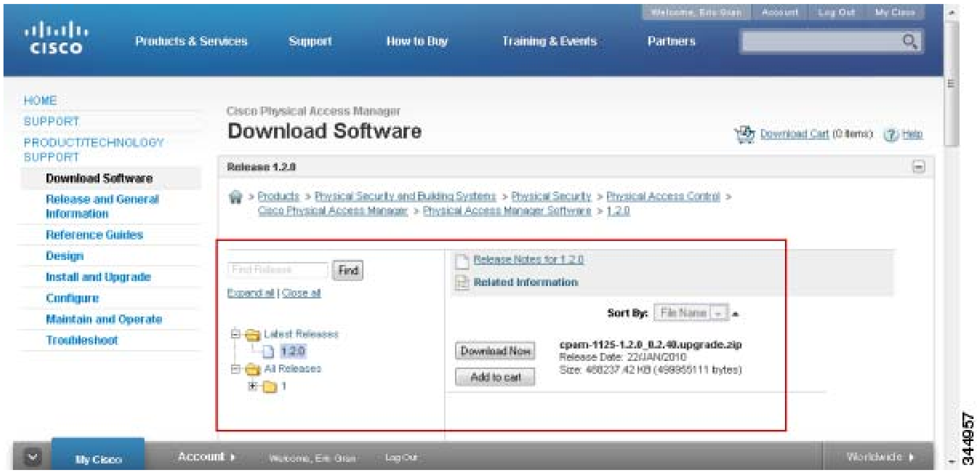
Figure B-3 Download ICPAM Software Updates



Review additional information about Cisco Physical Access Manager in Products & Services site area.

Step 3 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



cpam-1125-1.2.0_0.2.40.upgrade.zip
Release Date: 22/JAN/2010
Size: 488237.42 KB (499955111 bytes)

Step 4 Click **Download Now**.

Step 5 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 6 Locate and extract the compressed .zip file on your drive.

For example: cpam-2.1_0.1.10.upgrade.zip.

Step 7 Open the directory and verify that the file is correct.

The filename includes the release number and other details. For example: cpam-2.1_0.1.10.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:

- ICPAM Release Notes
  http://www.identiv.com/en/US/products/ps9688/prod_release_notes_list.html
- ICPAM Documentation
  http://www.identiv.com/en/US/products/ps9688/tsd_products_support_series_home.html
- Cisco Gateway Documentation
  http://www.cisco.com/en/US/products/ps9687/tsd_products_support_series_home.html

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 Identiv Connected 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 ICPAM Desktop Software

Always upgrade the ICPAM desktop client whenever 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 ICPAM Desktop Software, page 3-2 for instructions.

Upgrading the ICPAM Server Software

To upgrade the ICPAM 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 ICPAM 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 Gateways and other hardware devices may be dropped during the upgrade process. Identiv 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 2.1, page B-2
- Obtain the correct software image. See Obtaining Software Images, page B-8.

Tip The ICPAM 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 ICPAM server software, do the following:

Step 1 Review the notes in Before You Begin and Upgrade Notes for Release 2.1, page B-2

Step 2 Backup either the Active or Standby server, as described in Backing up the ICPAM 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:

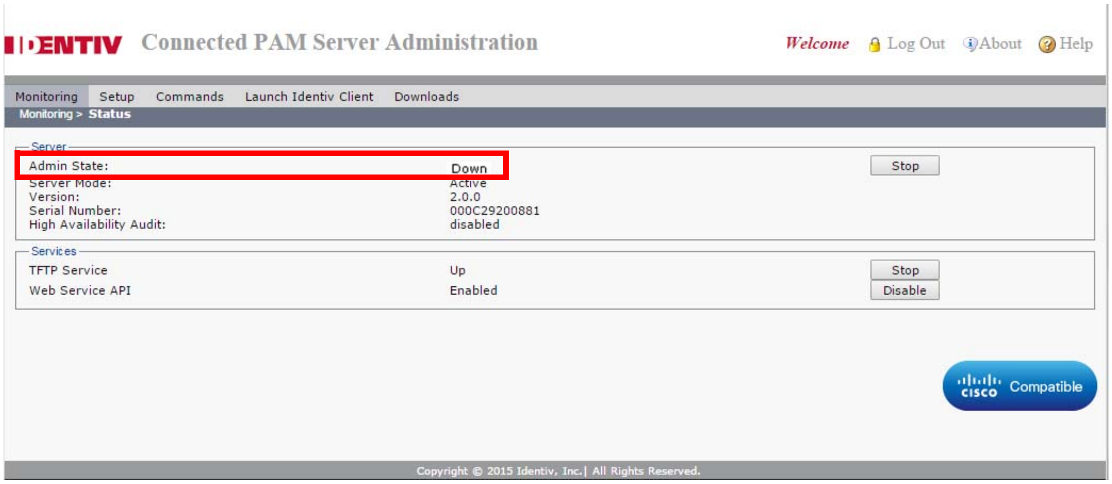
a. Log on to the Standby appliance, as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

b. Click the **Monitoring** tab and verify the Server Mode is *Standby* (Figure B-5).

c. Select the **Stop** button in the Admin entry.

d. Verify that the Admin State is *Down*.

Figure B-5 Monitoring Window in the ICPAM Server Administration Utility



Server

Admin State:	Down
Server Mode:	Active
Version:	2.0.0
Serial Number:	000C29200881
High Availability Audit:	disabled

Services

TFTP Service	Up
Web Service API	Enabled

Step 5 Stop the Active server.

a. Log on to the Active appliance.

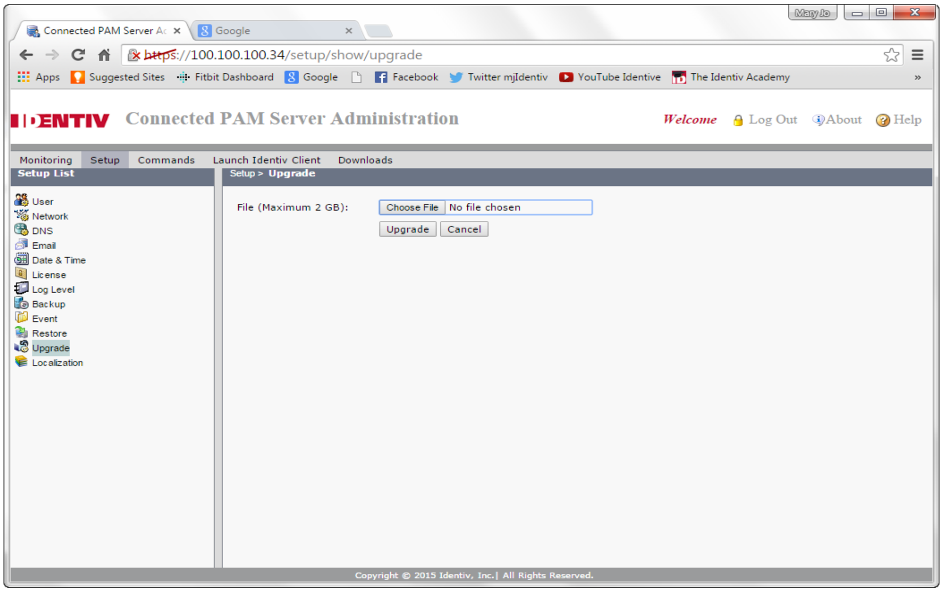
b. Click the **Monitoring** tab and verify the Server Mode is *Active* (Figure B-5).

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 ICPAM Server Administration Utility



~~https~~://100.100.100.34/setup/show/upgrade

File (Maximum 2 GB): No file chosen

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-2.1_0.1.10.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 ICPAM 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.

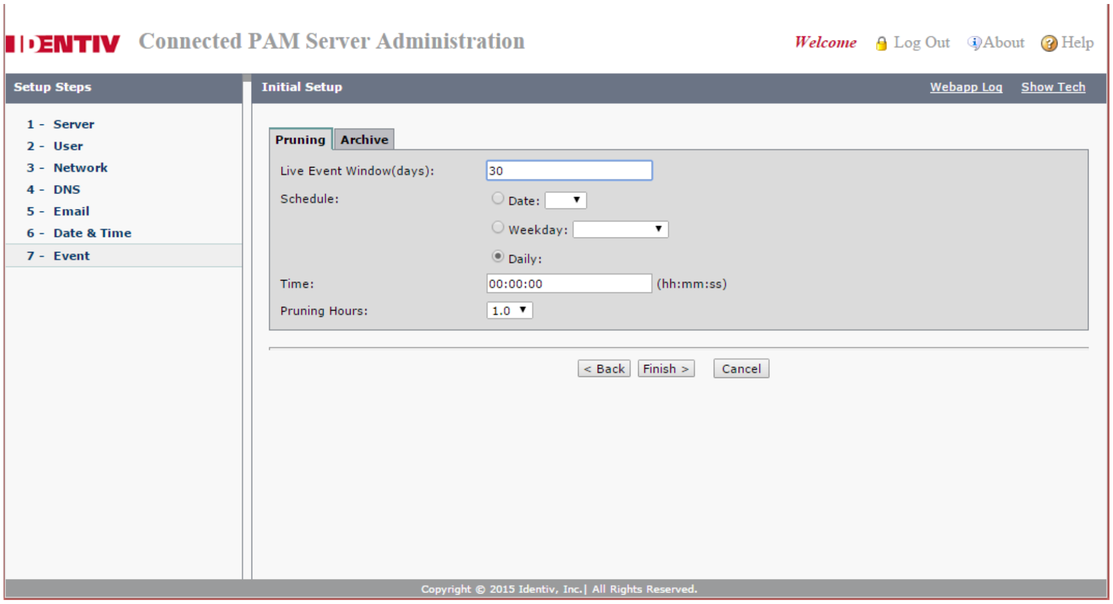
Step 11 If upgrading from Release 1.2.0 or earlier to Release 1.3.0 or higher, you must enter the event pruning and archive settings, as shown in Figure B-7.

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 ICPAM 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 ICPAM 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 2-25 for more information.

Figure B-7 Initial Setup: Event Pruning and Archiving



Live Event Window(days): 30

Schedule: ○ Date: ○ Weekday: ● Daily:

Time: 00:00:00 (hh:mm:ss)

Pruning Hours: 1.0

a. Select the **Pruning** tab (Figure B-7), and enter the following settings:

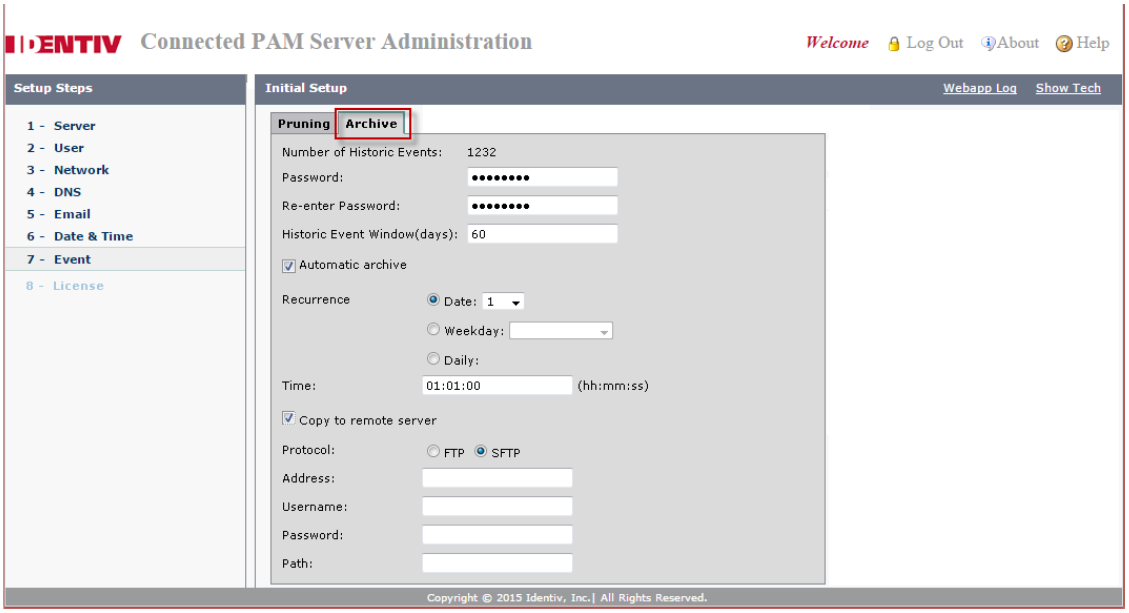
- **Live Events Window (days)**—Enter a value between 0 and 500 (inclusive). This is the number of days of events that will be available on live view. All the events older than the specified days will be removed at the pruning schedule time. For example, enter `30` to keep events in the live view for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

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`.
- **Pruning Hours**—This field is enabled only if Daily is selected in Schedule. The default value is 1.

Figure B-8 Archiving Events



Number of Historic Events: 1232

Password: ••••••••

Re-enter Password: ••••••••

Historic Event Window(days): 60

☑ Automatic archive

Recurrence ● Date: 1

○ Weekday:

○ Daily:

Time: 01:01:00 (hh:mm:ss)

☑ Copy to remote server

Protocol: ○ FTP ● SFTP

Address:

Username:

Password:

Path:

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

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 2-25.

- 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 ICPAM appliance.

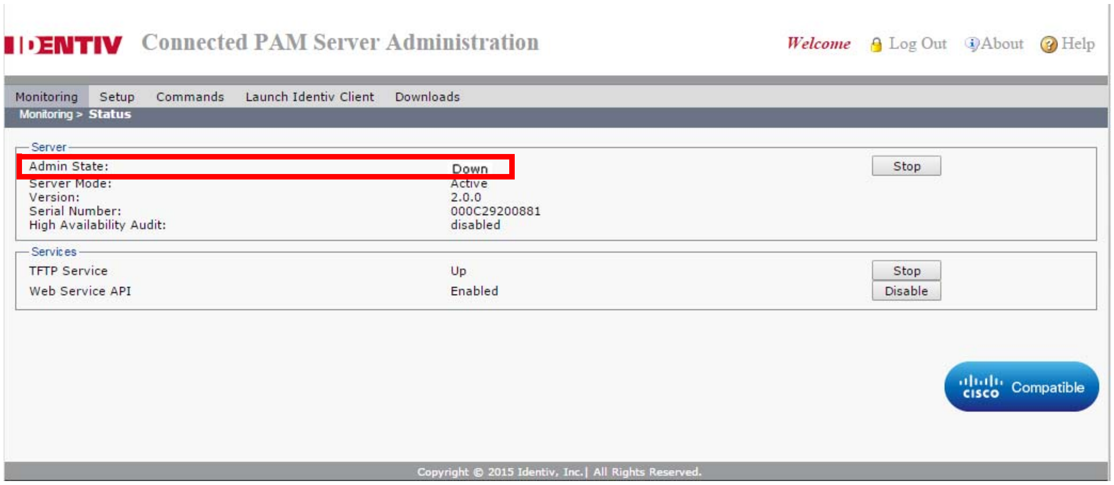
b. Select the **Monitoring** tab and then select **Status**.

c. Verify the Server Version is correct. For example: **`1.5.0`**

d. Verify the Admin State is *Down*.

e. Verify the Server Mode is **N/A**.

Figure B-9 Server Admin State for the Active Server



Server
Admin State: Down
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

Services
TFTP Service Up
Web Service API Enabled

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-11.

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.

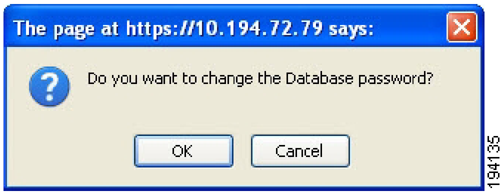
a. Log on to the Active ICPAM appliance, if necessary.

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,



The page at https://10.194.72.79 says:

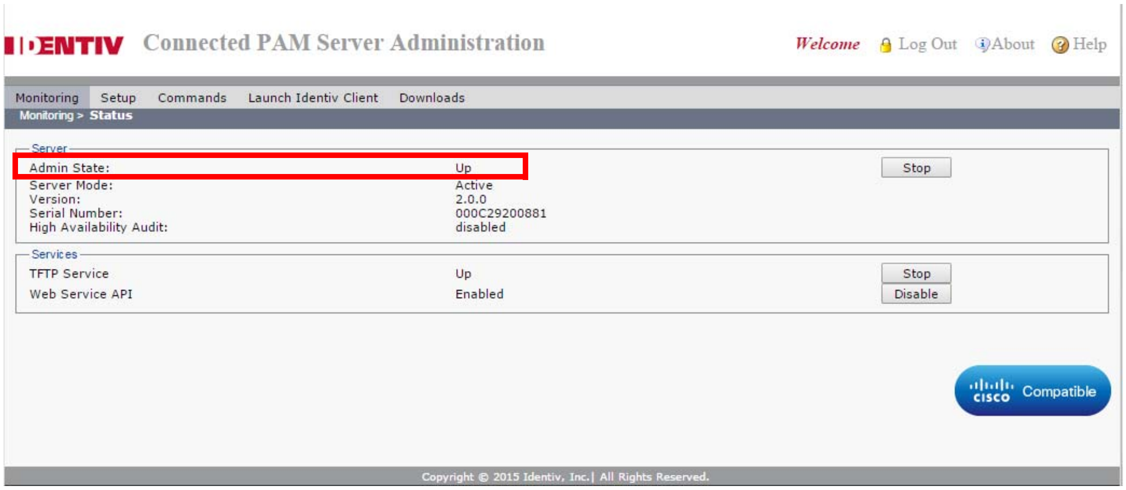
Do you want to change the Database password?

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: `2.1.0`
  - Verify the Admin State is *Up*.
  - Verify the Server Mode is *Active*.

Figure B-10 Server Admin State (Up) for the Active Server



Admin State:	Up	Stop
Server Mode:	Active	
Version:	2.0.0	
Serial Number:	000C29200881	
High Availability Audit:	disabled	
TFTP Service	Up	Stop
Web Service API	Enabled	Disable

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 ICPAM 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: **`2.1.0`**
  - 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 ICPAM desktop client, as described in Installing or Updating the ICPAM Desktop Software, page 3-2. 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-17
- Replacing Both Appliances in an HA Configuration, page B-18
- Replacing a Single Appliance in an HA Configuration, page B-19

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

Step 1 Backup the old appliance, as described in Backing up the ICPAM Database, page A-1. This backup is used to restore the system data to the new appliance.

Step 2 Copy the backup file to a local disk, as described in Backing up the ICPAM Database, page A-1.

Step 3 Stop the appliance.

a. Log on to the appliance, as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

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 2-7.

Step 6 Obtain and install new ICPAM licenses. See Obtaining and Installing Optional Feature Licenses, page 2-44 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 ICPAM 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 ICPAM Server Administration Utility, page 2-2.

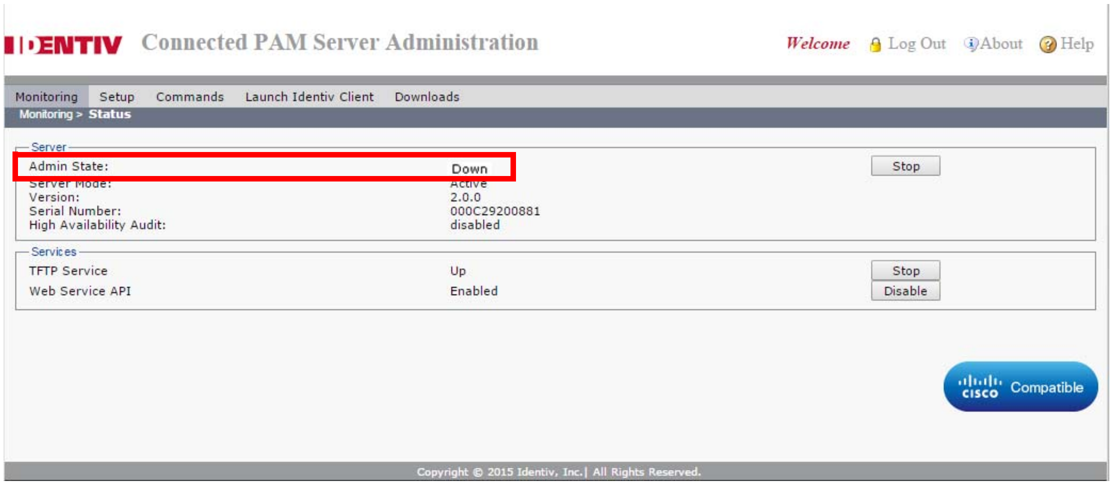
b. Select **Monitoring** and then select **Status** (Figure B-11).

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 Server in Admin State "Down"



Admin State: Down
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

TFTP Service Up
Web Service API Enabled

Step 3 Stop the Standby 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 ICPAM Server Administration Utility, page 2-2.

a. Select **Monitoring** and then select **Status**.

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 2-7.

- Enter a *Shared IP Address*.
- Obtain and install new ICPAM licenses, including the HA license. All optional licenses are installed on the Active server only. See Obtaining and Installing Optional Feature Licenses, page 2-44 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 2-7.
- Obtain and reinstall the HA license on the Standby server. See Obtaining and Installing Optional Feature Licenses, page 2-44 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.

If the HA servers are not in sync, see the "Monitoring" section on page 2-21 for a description of the HA messages that may appear.

Step 9 Restore the backup file to the Active server, as described in Restoring a Server Backup File, page A-8.

Replacing 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

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 ICPAM Database, page A-1.

c. Copy the backup file to a local disk.

Step 2 Stop the appliance to be replaced.

a. Log on to the appliance, as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

b. Select **Monitoring** and then select **Status**.

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-11.

Step 3 Power down and physically remove the old appliance.

Step 4 Install the replacement appliance, as described in the *Cisco Physical Security Multi Services Platform User Guide*.

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 2-7.
- Obtain and reinstall the HA license on the Standby appliance. See Obtaining and Installing Optional Feature Licenses, page 2-44 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.

If the HA servers are not in sync, see the "Monitoring" section on page 2-21 for a description of the HA messages that may appear.

Reinstalling the ICPAM Server Software from a Recovery CD

Use the recovery CD/DVD included with the ICPAM appliance to completely erase the server hard disk and re-install the ICPAM 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 "Backing up the ICPAM 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 2-7 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, "Backing Up and Restoring Data" for more information.

Caution Reinstalling the server software from a CD/DVD using these instructions permanently erases all data and configurations on the ICPAM appliance. You must have at least one backup to restore the server data. See Appendix A, "Backing Up and Restoring Data" for more information.

Step 2 Insert the ICPAM recovery CD into the server DVD-ROM drive.

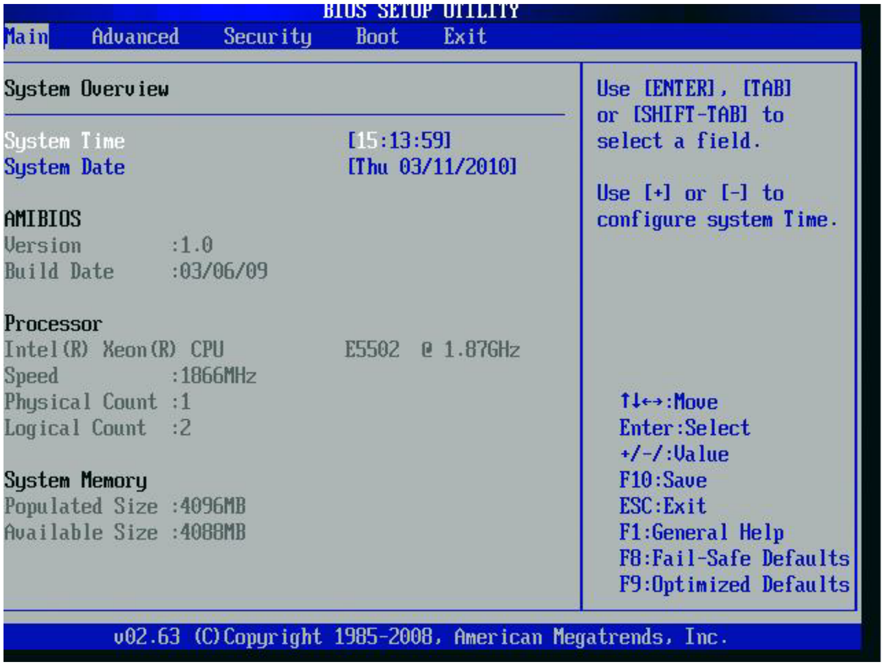
Step 3 Reboot the ICPAM appliance:

a. Log on to the ICPAM appliance, as described in Logging on to the ICPAM Server Administration Utility, page 2-2.

a. Select the **Commands** tab, and then select **Reboot**.

Step 4 Press and hold the **Delete** key while the appliance is restarting to open the BIOS setup utility, as shown in Figure B-12.

Figure B-12 BIOS Setup Utility



```
                                  BIOS SETUP UTILITY
Main    Advanced    Security    Boot    Exit

System Overview                                        Use [ENTER], [TAB]
                                                       or [SHIFT-TAB] to
System Time                  [15:13:59]                select a field.
System Date                  [Thu 03/11/2010]
                                                       Use [+] or [-] to
AMIBIOS                                                configure system Time.
Version         :1.0
Build Date      :03/06/09

Processor
Intel(R) Xeon(R) CPU         E5502  @ 1.87GHz
Speed           :1866MHz
Physical Count  :1                                       ↑↓↔:Move
Logical Count   :2                                       Enter:Select
                                                         +/-/:Value
System Memory                                            F10:Save
Populated Size  :4096MB                                  ESC:Exit
Available Size  :4088MB                                  F1:General Help
                                                         F8:Fail-Safe Defaults
                                                         F9:Optimized Defaults

          v02.63 (C)Copyright 1985-2008, American Megatrends, Inc.
```

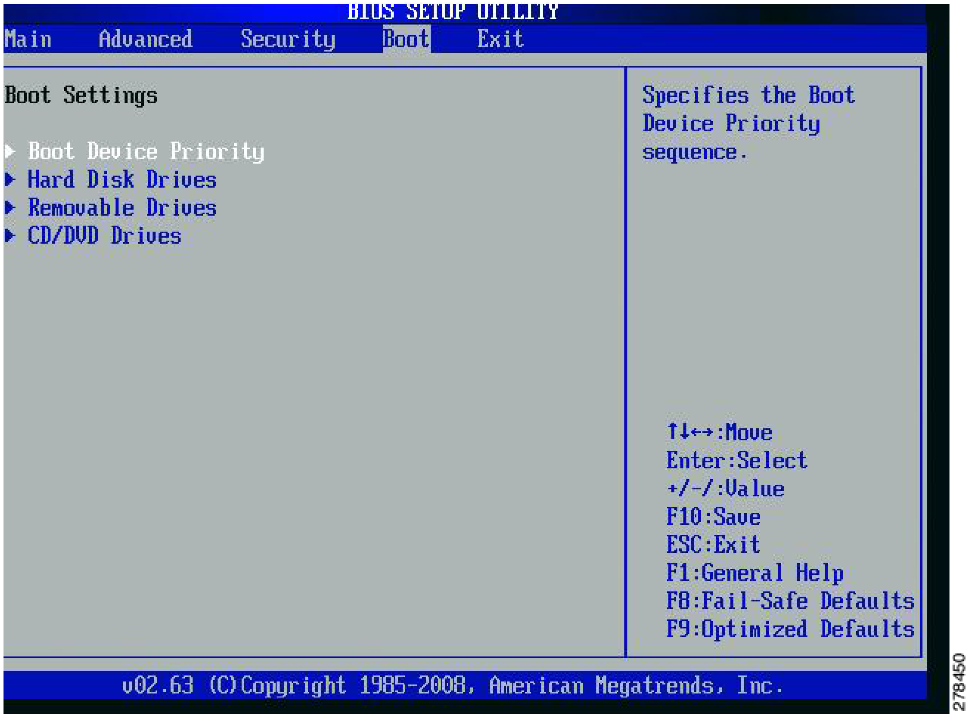
278451

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 ICPAM 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-13.

Figure B-13 BIOS Boot Settings



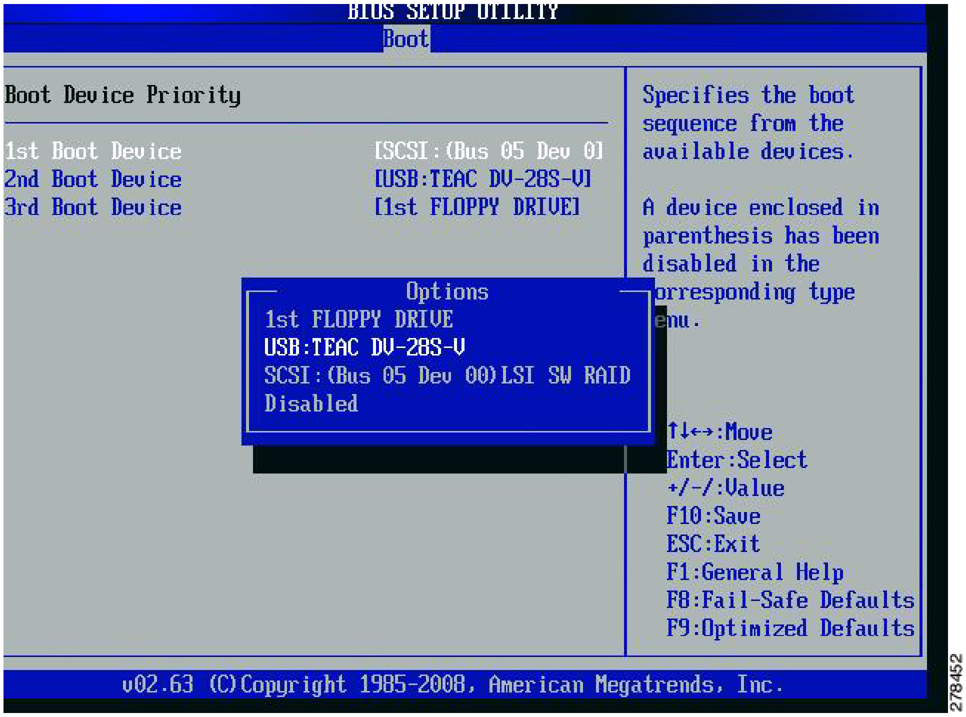
```
BIOS SETUP UTILITY
Main     Advanced     Security     Boot     Exit

Boot Settings                            Specifies the Boot
                                         Device Priority
▶ Boot Device Priority                   sequence.
▶ Hard Disk Drives
▶ Removable Drives
▶ CD/DVD Drives

                                           ↑↓←→:Move
                                           Enter:Select
                                           +/-/:Value
                                           F10:Save
                                           ESC:Exit
                                           F1:General Help
                                           F8:Fail-Safe Defaults
                                           F9:Optimized Defaults

        v02.63 (C)Copyright 1985-2008, American Megatrends, Inc.
```

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-14.

Figure B-14 Boot Device Priority Options

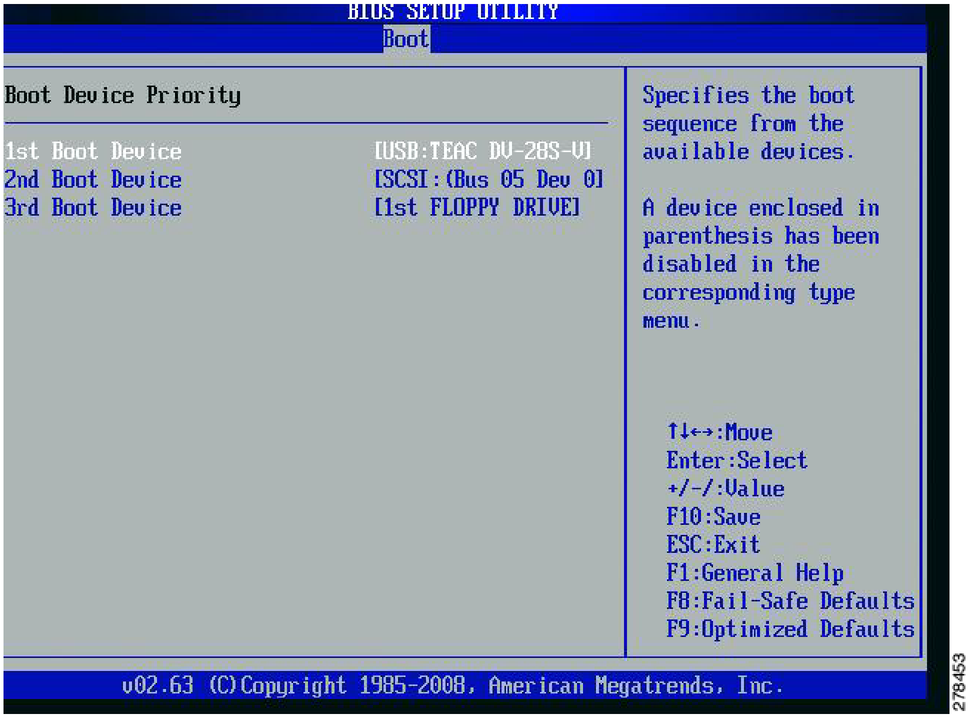


```
BIOS SETUP UTILITY
Boot

Boot Device Priority                              Specifies the boot
                                                  sequence from the
1st Boot Device          [SCSI:(Bus 05 Dev 0]     available devices.
2nd Boot Device          [USB:TEAC DV-28S-V]
3rd Boot Device          [1st FLOPPY DRIVE]       A device enclosed in
                                                  parenthesis has been
                                                  disabled in the
             Options                              orresponding type
             1st FLOPPY DRIVE                     enu.
             USB:TEAC DV-28S-V
             SCSI:(Bus 05 Dev 00)LSI SW RAID
             Disabled
                                                   ↑↓←→:Move
                                                   Enter:Select
                                                   +/-/:Value
                                                   F10:Save
                                                   ESC:Exit
                                                   F1:General Help
                                                   F8:Fail-Safe Defaults
                                                   F9:Optimized Defaults

        v02.63 (C)Copyright 1985-2008, American Megatrends, Inc.
```

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-15.

Figure B-15 1st Boot Device = CD/DVD



```
BIOS SETUP UTILITY
Boot

Boot Device Priority                              Specifies the boot
                                                  sequence from the
1st Boot Device          [USB:TEAC DV-28S-V]      available devices.
2nd Boot Device          [SCSI:(Bus 05 Dev 0]
3rd Boot Device          [1st FLOPPY DRIVE]       A device enclosed in
                                                  parenthesis has been
                                                  disabled in the
                                                  corresponding type
                                                  menu.

                                                   ↑↓←→:Move
                                                   Enter:Select
                                                   +/-/:Value
                                                   F10:Save
                                                   ESC:Exit
                                                   F1:General Help
                                                   F8:Fail-Safe Defaults
                                                   F9:Optimized Defaults

        v02.63 (C)Copyright 1985-2008, American Megatrends, Inc.
```

f. Press the **F10** function key to save the changes and exit the BIOS utility.

Step 6 Wait for the CD to install the ICPAM server software. When finished, the server will reboot again.

Step 7 After the server reboots, remove the ICPAM recovery CD from the server DVD-ROM drive.

Step 8 Configure the server as described in Initial Setup Instructions, page 2-7.

Step 9 Restore the system, as described in Restoring a Server Backup File, page A-8.

APPENDIX C

Upgrading and Configuring Gateways

Use the Hardware - Tree or Door/Location-based Hardware module to upgrade the firmware on one or more gateways, or change the network settings on the modules. You can also change the NTP settings on multiple gateways to ensure the time is synchronized on all devices.

Note

- We strongly recommend using NTP to synchronize the ICPAM appliance and gateway clocks to ensure correct event and messaging. See the "Change the NTP Setting for Multiple Gateways" section on page C-7 for instructions to set NTP on gateways.
- 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 ICPAM Installation Guide or, for Cisco Gateway support, refer to the Cisco Physical Access Gateway User Guide.
- This appendix applies only to Cisco Gateway installations. Identiv EM-100 controller installations are dealt with in a separate section.

Contents

This appendix includes the following information:

Displaying the Gateway Network and Firmware Configuration

The extended status area of the Hardware - Tree module displays the network configuration and firmware version for a gateway.

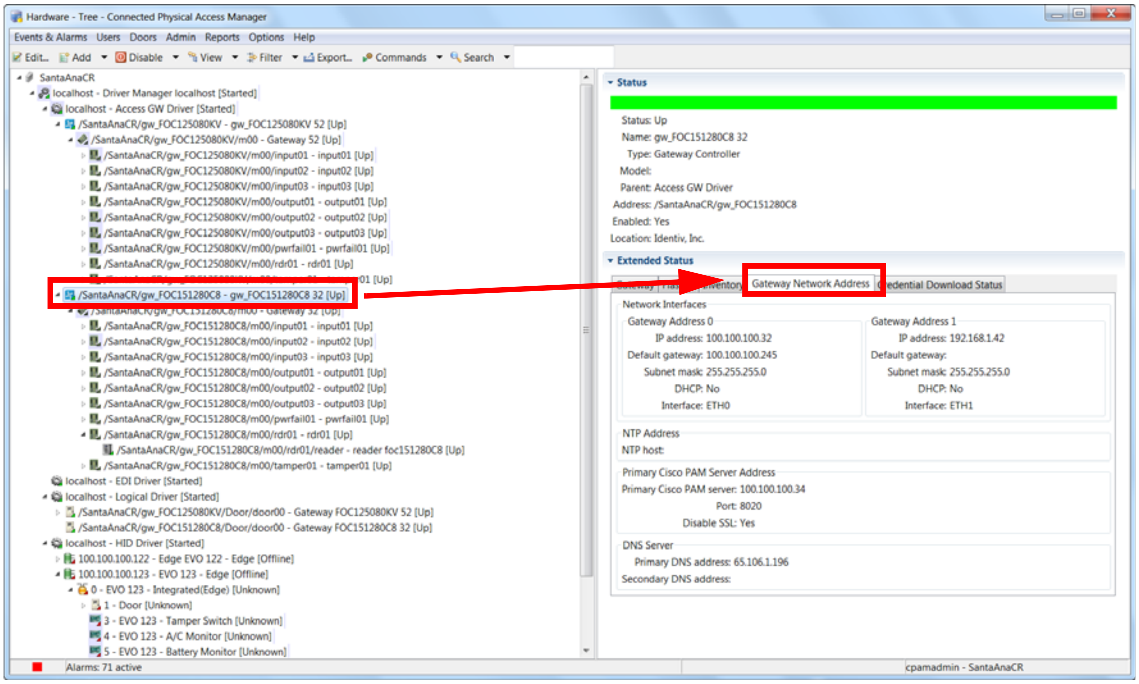
Step 1 Select the **Hardware - Tree** module from the **Doors** menu.

Tip You can also view the gateway settings from the Door/Location-based Hardware module. Filter the display to view the gateways and then select a gateway. See the "Using Door/Location-based Hardware to Change Gateway Network Settings" section on page C-10 for more information.

Step 2 Expand the **Access GW Driver** and click a gateway 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



```
SantaAnaCR
  localhost - Driver Manager localhost [Started]
    localhost - Access GW Driver [Started]
      /SantaAnaCR/gw_FOC125080KV - gw_FOC125080KV 52 [Up]
        /SantaAnaCR/gw_FOC125080KV/m00 - Gateway 52 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/input01 - input01 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/input02 - input02 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/input03 - input03 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/output01 - output01 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/output02 - output02 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/output03 - output03 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/pwrfail01 - pwrfail01 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/rdr01 - rdr01 [Up]
          /SantaAnaCR/gw_FOC125080KV/m00/tamper01 - tamper01 [Up]
      /SantaAnaCR/gw_FOC151280C8 - gw_FOC151280C8 32 [Up]
        /SantaAnaCR/gw_FOC151280C8/m00 - Gateway 32 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/input01 - input01 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/input02 - input02 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/input03 - input03 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/output01 - output01 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/output02 - output02 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/output03 - output03 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/pwrfail01 - pwrfail01 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/rdr01 - rdr01 [Up]
            /SantaAnaCR/gw_FOC151280C8/m00/rdr01/reader - reader foc151280C8 [Up]
          /SantaAnaCR/gw_FOC151280C8/m00/tamper01 - tamper01 [Up]
    localhost - EDI Driver [Started]
    localhost - Logical Driver [Started]
      /SantaAnaCR/gw_FOC125080KV/Door/door00 - Gateway FOC125080KV 52 [Up]
      /SantaAnaCR/gw_FOC151280C8/Door/door00 - Gateway FOC151280C8 32 [Up]
    localhost - HID Driver [Started]
      100.100.100.122 - Edge EVO 122 - Edge [Offline]
      100.100.100.123 - EVO 123 - Edge [Offline]
        0 - EVO 123 - Integrated(Edge) [Unknown]
          1 - Door [Unknown]
          3 - EVO 123 - Tamper Switch [Unknown]
          4 - EVO 123 - A/C Monitor [Unknown]
          5 - EVO 123 - Battery Monitor [Unknown]
```

Status: Up
Name: gw_FOC151280C8 32
Type: Gateway Controller
Model:
Parent: Access GW Driver
Address: /SantaAnaCR/gw_FOC151280C8
Enabled: Yes
Location: Identiv, Inc.

Network Interfaces

Gateway Address 0
IP address: 100.100.100.32
Default gateway: 100.100.100.245
Subnet mask: 255.255.255.0
DHCP: No
Interface: ETH0

Gateway Address 1
IP address: 192.168.1.42
Default gateway:
Subnet mask: 255.255.255.0
DHCP: No
Interface: ETH1

NTP Address
NTP host:

Primary Cisco PAM Server Address
Primary Cisco PAM server: 100.100.100.34
Port: 8020
Disable SSL: Yes

DNS Server
Primary DNS address: 65.106.1.196
Secondary DNS address:

Alarms: 71 active
cpamadmin - SantaAnaCR

Tip The IP address is the address configured on the gateway Eth0 port address, which provides IP network connectivity with the ICPAM appliance.

Step 3 Select the **Gateway Network Address** tab to display the module's network configuration.

Changing the Gateway Network Settings

To change network configuration settings for a gateway using ICPAM, right-click a gateway and select **Set Gateway Address**.

Procedure

Step 1 Select the **Hardware - Tree** module from the **Doors** menu.

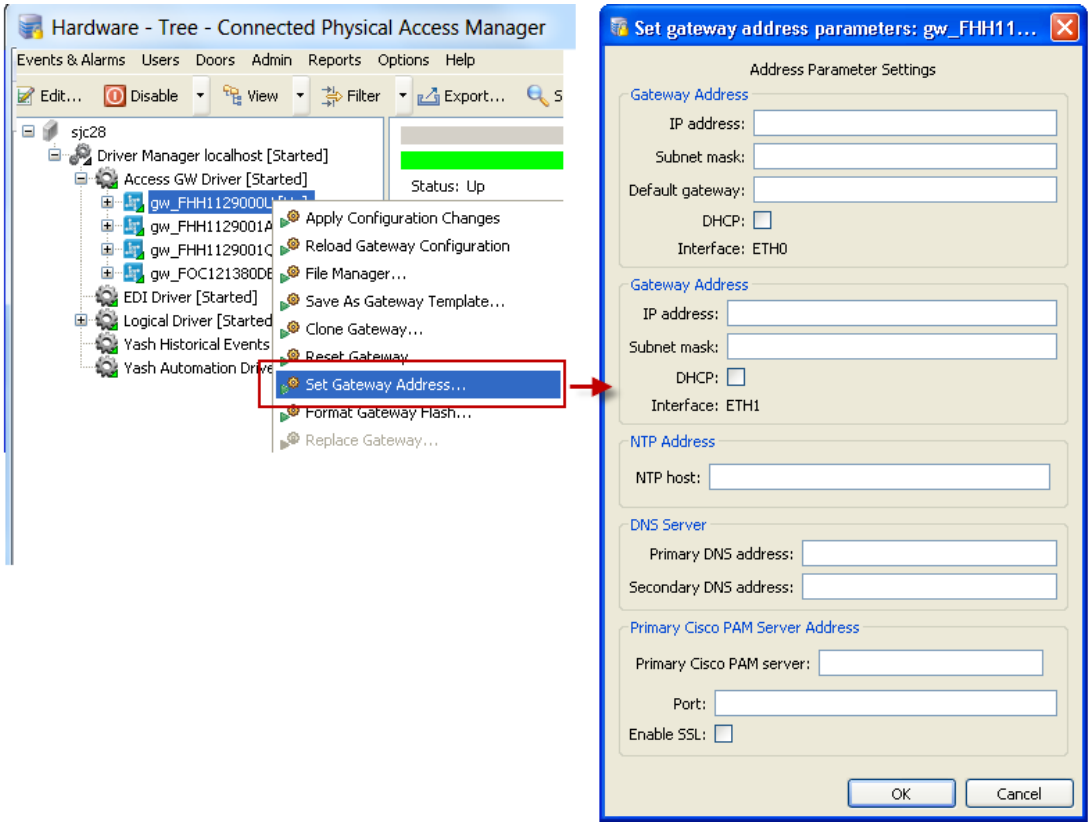
Step 2 Expand the **Access GW Driver**.

Step 3 Right-click a gateway and select **Set Gateway Address** (Figure C-2).

Tip You can also change the gateway settings from the Door/Location-based Hardware module. Filter the display to view the gateways and then right-click a gateway name. See the "Using Door/Location-based Hardware to Change Gateway Network Settings" section on page C-10 for more information.

Step 4 Modify the fields as described in the following table.

Figure C-2 Set Gateway Address



Field	Description
Gateway Address	
DHCP	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.
IP Address	IP address for the module Ethernet interfaces. • The ETH0 interface provides IP network connectivity with the ICPAM appliance. • The ETH1 interface is used for management connections, such as connecting a PC directly to the gateway. See the Cisco Physical Access Gateway User Guide for more information.
Subnet Mask	The subnet mask.
Default Gateway	The IP address of the default network gateway.
NTP Address	
NTP Host	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.
DNS Server	
Primary DNS Address	Enter the Primary DNS Address configuration if names (not IP addresses) are used for the NTP or ICPAM addresses.
Secondary DNS Address	Enter the Secondary DNS Address configuration if names (not IP addresses) are used for the NTP or ICPAM addresses
Primary ICPAM Server Address	
Primary ICPAM Server	Enter the ICPAM IP **Address** (IP address or name) to enable gateway communication with the appliance.

Port	Enter the **Port** number for the ICPAM appliance. The port number must be greater than 1024 and less 65535. The default is 8020.
Enable SSL	The secure socket layer (SSL) is enabled for secure communication between the gateway and ICPAM appliance by default. If necessary SSL can be disabled by deselecting the **Enable SSL** check box. **Note** SSL is enabled by default on all gateways and ICPAM appliances. If SSL is disabled for a gateway but enabled for ICPAM, the gateway will not be able to connect to the appliance. If the SSL settings are changed, reset all gateways and the ICPAM 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 5-13.

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.

Changing the NTP Setting for Multiple Gateways

You can set the network time protocol (NTP) server for all gateways, or for a selected gateway, 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 ICPAM appliance to ensure synchronized events and messaging. To set the server NTP address, see Chapter 2, "Configuring and Monitoring the ICPAM Server". Other systems that are integrated with ICPAM, 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-7.

Refer to the following topics:

- (Optional) Set a Default NTP Server, page C-6
- Change the NTP Setting for Multiple Gateways, page C-7

(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-7.

Procedure

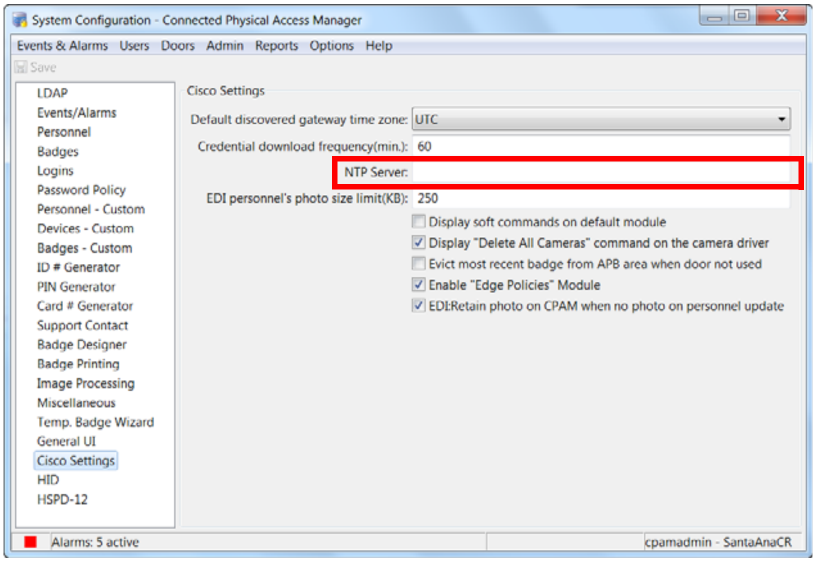
Step 1 Select **System Configuration** from the Admin menu.

Step 2 Select the **ICPAM 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.

Figure C-3 System Configuration: NTP Server IP Address



Cisco Settings

Default discovered gateway time zone: UTC

Credential download frequency(min.): 60

NTP Server:

EDI personnel's photo size limit(KB): 250

☐ Display soft commands on default module
☑ Display "Delete All Cameras" command on the camera driver
☐ Evict most recent badge from APB area when door not used
☑ Enable "Edge Policies" Module
☑ EDI:Retain photo on CPAM when no photo on personnel update

Alarms: 5 active

cpamadmin - SantaAnaCR

Step 4 Restart ICPAM (exit and relaunch the application).

Note Changes do not take effect until the ICPAM 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-7.

You must use the **Set NTP Server** command to apply the NTP server setting to one or more gateways.

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.

Note 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.

Procedure:

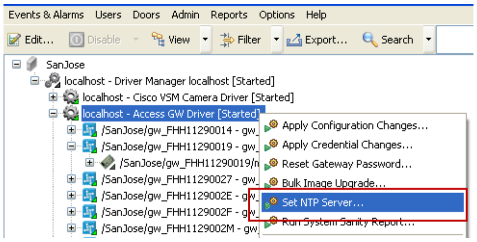
Step 1 (Optional) Enter a default NTP server setting to auto-populate the NTP Server field.

See the "(Optional) Set a Default NTP Server" section on page C-6 for more information.

Step 2 Select **Hardware - Tree** from the **Doors** menu.

Step 3 Right-click the **Access GW Driver** and select the **Set NTP Server** command (Figure C-4).

Figure C-4 ***Set NTP Server for Multiple Gateways***


Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Edit...
Disable
View
Filter
Export...
Search
SanJose
localhost - Driver Manager localhost [Started]
localhost - Cisco VSM Camera Driver [Started]
localhost - Access GW Driver [Started]
/SanJose/gw_FHH11290014 - gw_
/SanJose/gw_FHH11290019 - gw_
/SanJose/gw_FHH11290019/n
/SanJose/gw_FHH11290027 - gw_
/SanJose/gw_FHH1129002E - gw_
/SanJose/gw_FHH1129002F - gw_
/SanJose/gw_FHH1129002M - gw_
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Set NTP Server...
Run System Sanity Report...

Step 4 In the Set NTP Server window (Figure C-5), enter the following settings:

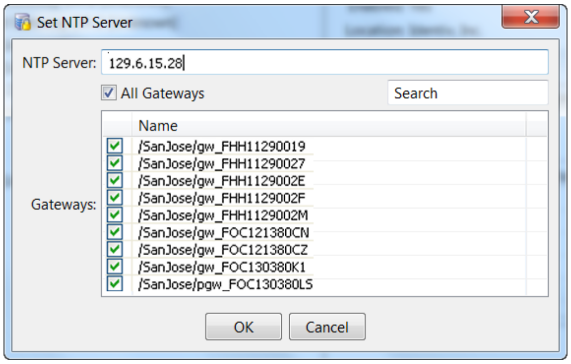
a. Enter the NTP server IP address.

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-6 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 deselect gateways in the list to include or exclude modules.

Figure C-5 ***Set NTP Server Configuration Window***



NTP Server: 129.6.15.28

☑ All Gateways

Gateways:

	Name
☑	/SanJose/gw_FHH11290019
☑	/SanJose/gw_FHH11290027
☑	/SanJose/gw_FHH1129002E
☑	/SanJose/gw_FHH1129002F
☑	/SanJose/gw_FHH1129002M
☑	/SanJose/gw_FOC121380CN
☑	/SanJose/gw_FOC121380CZ
☑	/SanJose/gw_FOC130380K1
☑	/SanJose/pgw_FOC130380LS

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.

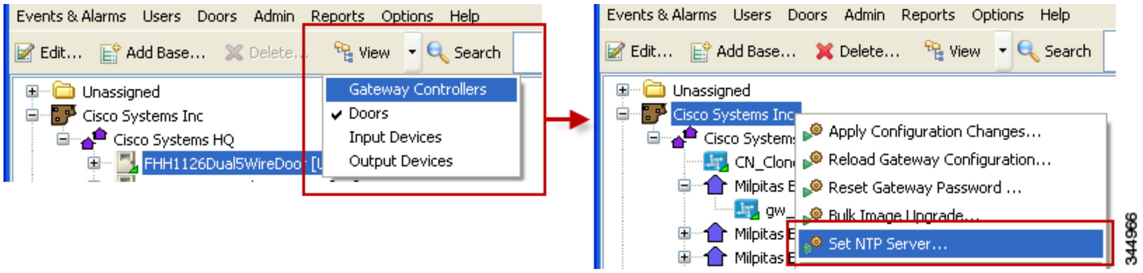
Note If the **Set NTP Server** command is already in progress for one or more gateways, you must wait for the summary event information to appear before you can use the command again.

Using Door/Location-based Hardware to Change Gateway Network Settings

You can use either the Hardware - Tree module or the Door/Location-based Hardware module to perform gateway configuration tasks such as changing the network settings or configuring an NTP server for multiple gateways.

To use the Door/Location-based Hardware 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 Door/Location-based Hardware Module


Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
Unassigned
Cisco Systems Inc
Cisco Systems HQ
FHH1126Dual5WireDoo
Gateway Controllers
Doors
Input Devices
Output Devices
Events & Alarms Users Doors Admin Reports Options Help
Edit... Add Base... Delete... View Search
Unassigned
Cisco Systems Inc
Cisco System
CN_Clon
Milpitas E
gw
Milpitas E
Milpitas E
Apply Configuration Changes...
Reload Gateway Configuration...
Reset Gateway Password ...
Bulk Image Upgrade...
Set NTP Server...
344966

- 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 Network Settings" section on page C-3 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 Gateways" section on page C-6 for additional instructions.

Upgrading Gateway Firmware Images Using ICPAM

Gateways must have the same firmware version as the ICPAM 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 ICPAM appliance is upgraded to Release 2.1, then all gateways must also be upgraded to firmware Release 2.1. If the firmware release is different than the ICPAM appliance release, the gateway will not operate and the gateway status in the ICPAM Hardware - Tree module will be **Mismatch**.

To ensure the gateway firmware is the same release as the ICPAM appliance software version, complete the instructions in this section. You can upgrade all the gateways at the same time, or one gateway at a time.

Firmware images must be located on a TFTP server (such as the built-in ICPAM 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. 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. See the *Cisco Physical Access Gateway User Guide* or *ICPAM Installation Guide* for more information.

This section includes the following information:

- Uploading Firmware Images to a TFTP Server, page C-11
- Updating the Firmware on All Gateways, page C-15
- Updating the Firmware on Individual Gateways, page C-21

Uploading Firmware Images to a TFTP Server

Firmware images used to update gateways must be located on a TFTP server. You can load the images to the built-in ICPAM 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 gateways, as described in Updating the Firmware on Individual Gateways, page C-21 and Updating the Firmware on All Gateways, page C-15.

Tip You can use the built-in ICPAM 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 ICPAM 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 ICPAM TFTP server, if necessary.

Note

- The ICPAM TFTP server is enabled by default. Complete these steps only if the server was manually disabled, as described in Disabling the ICPAM TFTP Server, page D-2.
- If you are using firmware images located on another TFTP server (not the ICPAM server), skip to Step 2.

a. Log in to the ICPAM Server Administration utility.

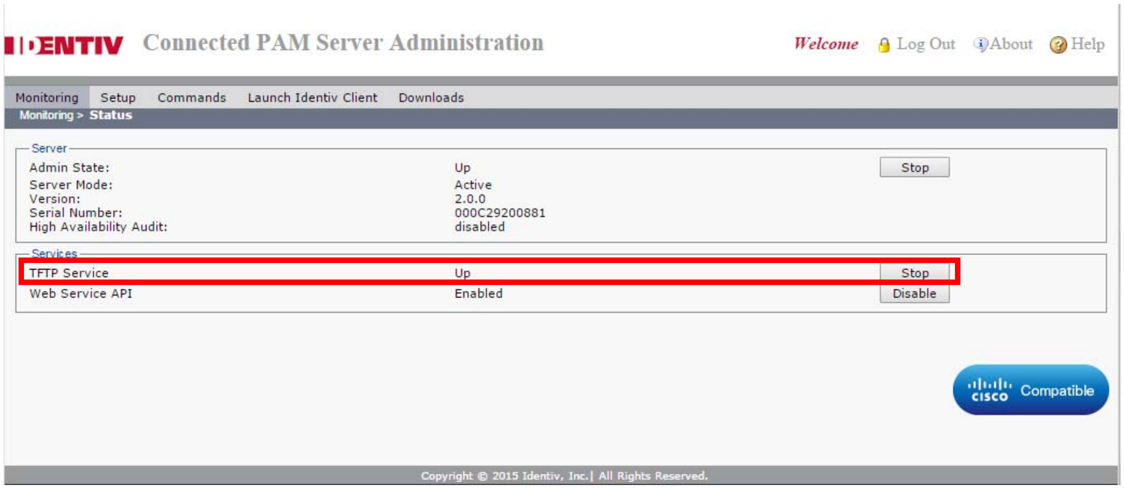
See Logging on to the ICPAM Server Administration Utility, page 2-2.

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



Server

Admin State: Up
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

Services

TFTP Service Up
Web Service API Enabled

Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Step 2 Log into the ICPAM desktop client.

See Logging on to the ICPAM Server Administration Utility, page 2-2.

Step 3 Select **Image Manager** from the Admin menu.

Figure C-8 shows the Image Manager window. Table C-1 on page C-13 describes each field.

Figure C-8 Image Manager with Callouts

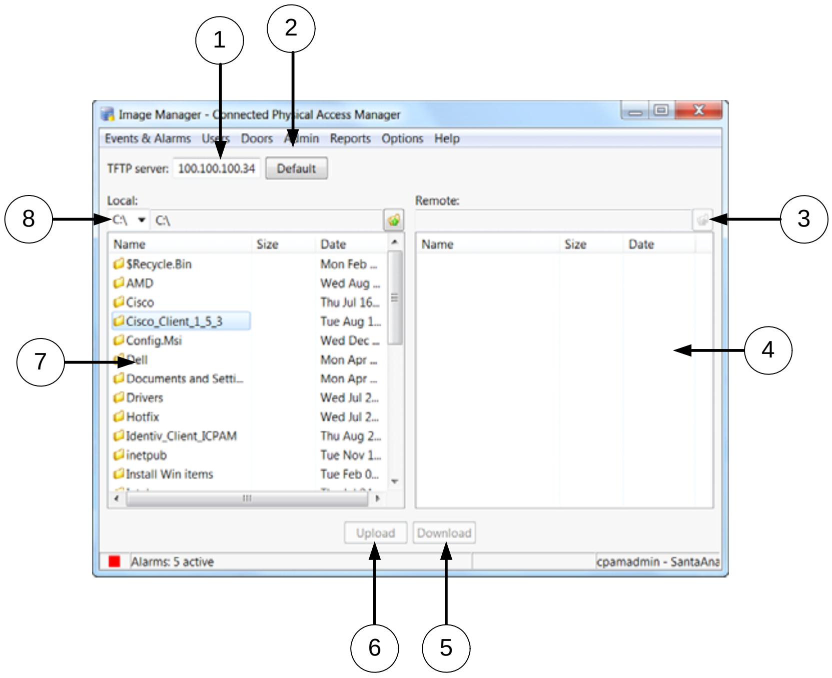


Table C-1 Image Manager Fields

	Field	Description
1	**TFTP server**	The IP address of the TFTP server to store image files.
2	**Default**	Click this button to IP address for the ICPAM TFTP server in the **TFTP server** field.
3	**Remote Directory Path**	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 ICPAM 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 ICPAM 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 ICPAM 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.
4	**Remote Browser**	Selects the directory where files will be uploaded on the built-in ICPAM TFTP server. This field is active only if you are using the build-in ICPAM 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

Table C-1 Image Manager Fields (continued)

	Field	Description
5	**Download Button**	Download a selected image on the TFTP server to the local drive.
6	**Upload Button**	Uploads the selected image file to the specified TFTP server and directory. This button is enabled only when a file is selected in the Local directory browser.
7	**Local Image Browser**	The **Local** directory browser specifies the file on a local drive for upload to the TFTP server. • Click the **Up** button to navigate one level up. • Double-click a folder to view the folder contents. • Select a file to enter the file name and directory path in the **Local Directory Path** field and enable the **Upload** button.
8	**Local Directory Path**	Read-only. Displays the directory path and filename for the file selected in the **Local** browser. This file will be uploaded to the specified TFTP server.

Step 4 Upload firmware images to either the ICPAM TFTP server, or another TFTP server:

Uploading images to the ICPAM TFTP Server:

a. Click **Default** to enter the ICPAM 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 ICPAM TFTP server where files will be uploaded. This field is inactive if you are using a TFTP server other than the build-in ICPAM server.

Right-click within the **Remote Browser** to select the following menu options:

– **Create Directory**: Creates a new directory on the ICPAM 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 ICPAM 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. ICPAM 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 Gateways, page C-21.

Tip To download an image from the TFTP server to a local directory, select the image and local directory, then click the **Download** button.

Updating the Firmware on All Gateways

This section describes how to upgrade or downgrade all the gateways configured in a ICPAM server.

Tip To upgrade the firmware for a single gateway, see Updating the Firmware on Individual Gateways, page C-21.

Before You Begin

Review the following before upgrading the gateways.

- This procedure loads the same firmware image to all gateways configured in ICPAM. 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 must have the same firmware version as the ICPAM 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 5-25 for more information.
- If you deselect the options **Set as active image** and **Reset Gateway**, then the firmware image is copied to the gateways, but is not made the *Active* or *Running* image. You must use the File Manager to manually activate the image on each gateway, as described in Step 9, and then reset the gateway as described in Step 10.
- Review the recommendations in the "Select the Following Options When Upgrading Gateway Firmware" section on page B-6.
- Gateways not configured in ICPAM 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 ICPAM. 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 gateways, complete the following steps.

Step 1 Complete the instructions in Uploading Firmware Images to a TFTP Server, page C-11

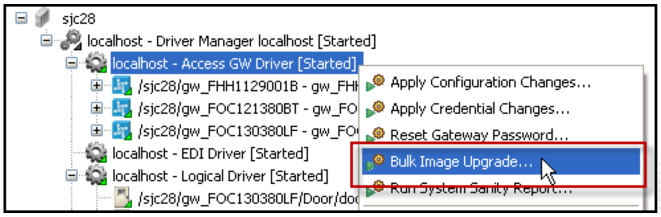
Step 2 Log in to the ICPAM desktop client.

See Logging into ICPAM Client, page 3-3.

Step 3 Select **Hardware - Tree** from the **Doors** menu.

Step 4 Right-click the **Access GW Driver** and select **Bulk Image Upgrade** (Figure C-9).

Figure C-9 Bulk Image Upgrade Menu


sjc28
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/sjc28/gw_FHH1129001B - gw_FHI
/sjc28/gw_FOC121380BT - gw_FO
/sjc28/gw_FOC130380LF - gw_FO
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
/sjc28/gw_FOC130380LF/Door/doo
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Run System Sanity Report...

Tip You can also access the **Bulk Image Upgrade** command using the **Door/Location-based Hardware** module. Select **Door/Location-based Hardware** 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 ICPAM TFTP server, click **Browse** to select a firmware image name.
- If the image is located on a different TFTP server, enter the filename manually.

Figure C-10 Bulk Image Upgrade Window

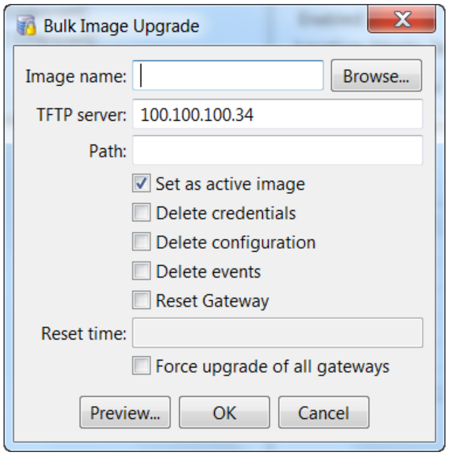

Bulk Image Upgrade

Image name: [Browse...]

TFTP server: 100.100.100.34

Path:

☑ Set as active image
□ Delete credentials
□ Delete configuration
□ Delete events
□ Reset Gateway

Reset time:

□ Force upgrade of all gateways

b. Enter the **TFTP Server** IP address.

The ICPAM 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 ICPAM 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 ICPAM 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 the "Select the Following Options When Upgrading Gateway Firmware" section on page B-6.

Step 6 Click **OK** to close the window and begin copying the firmware image to the gateways.

- 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.

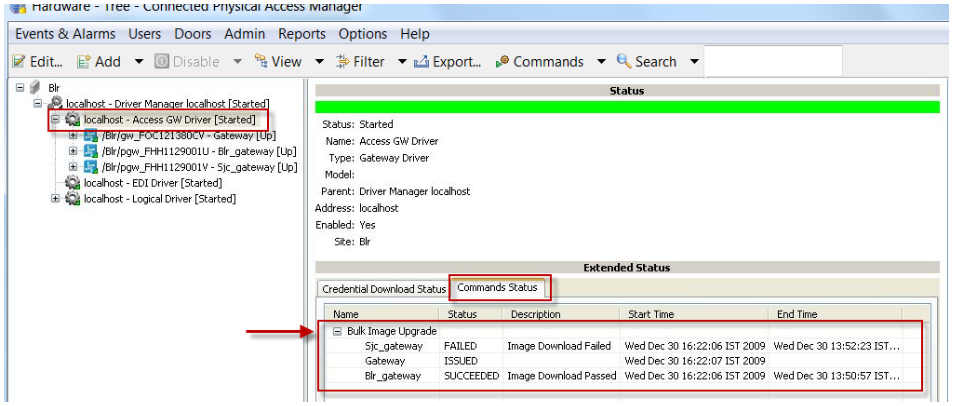
Note If you did not check the **Reset Gateway** option, the firmware image is copied to the gateways and defined as Active, but is not made the Running image. See Step 10 and Step 9 to manually activate the image and reset each gateway.

Step 7 Verify the upgrade status.

a. In the **Hardware - Tree** 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



Blr
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/Blr/gw_FOC121380CV - Gateway [Up]
/Blr/pgw_FHH1129001U - Blr_gateway [Up]
/Blr/pgw_FHH1129001V - Sjc_gateway [Up]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]

Status: Started
Name: Access GW Driver
Type: Gateway Driver
Model:
Parent: Driver Manager localhost
Address: localhost
Enabled: Yes
Site: Blr

Name	Status	Description	Start Time	End Time
Bulk Image Upgrade				
Sjc_gateway	FAILED	Image Download Failed	Wed Dec 30 16:22:06 IST 2009	Wed Dec 30 13:52:23 IST...
Gateway	ISSUED		Wed Dec 30 16:22:07 IST 2009	
Blr_gateway	SUCCEEDED	Image Download Passed	Wed Dec 30 16:22:06 IST 2009	Wed Dec 30 13:50:57 IST...

c. Expand the **Bulk Image Upgrade** entry to view the upgrade status for each gateway. The possible states include the following:

- **ISSUED**: The upgrade command was issued to the gateway.
- **SUCCEEDED**: The gateway image upgrade was successfully completed.
- **FAILED**: The gateway image upgrade Failed for the reason in the description.
- **COMPLETED**: ICPAM 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.

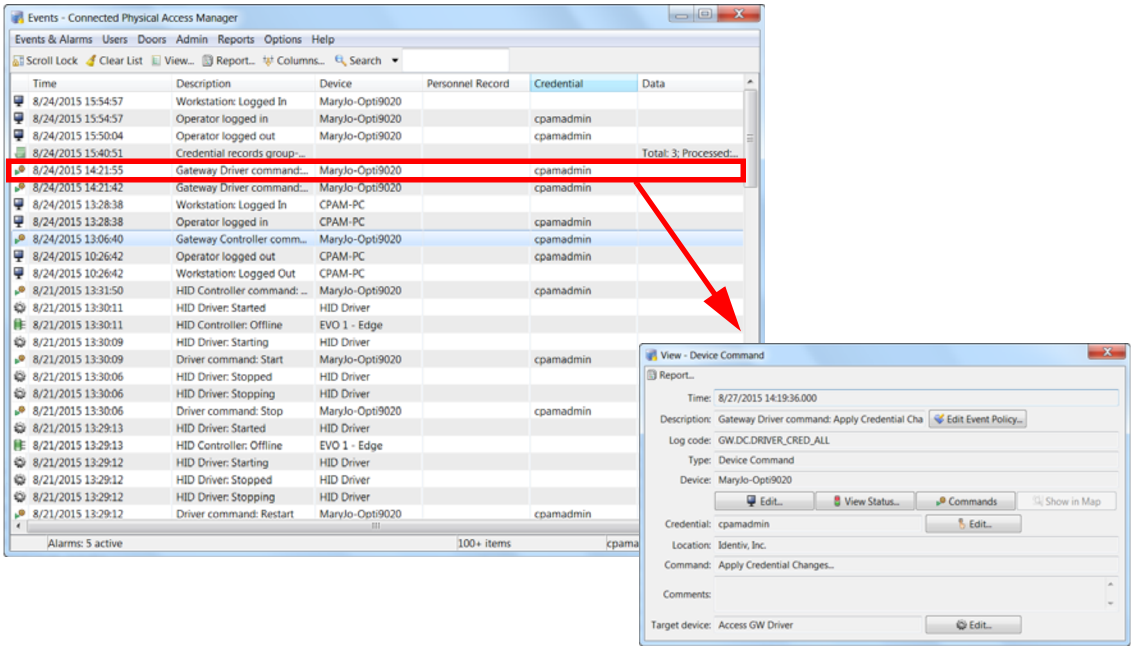
Note The status is shown as COMPLETED if the gateway reboots, and the status is still ISSUED. This can happen if the gateway has a large number of events in its queue when the module reboots, so the final status is not reported. Right-click the gateway icon in the Hardware - Tree module and select **File Manager** to view the status of the loaded firmware images.

Step 8 Review the summary event posted to the ICPAM Events module.

a. Select **Events** from the **Events & Alarms** menu, under the **Monitoring** submenu.

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



Time	Description	Device	Personnel Record	Credential	Data
8/24/2015 15:54:57	Workstation: Logged In	MaryJo-Opti9020			
8/24/2015 15:54:57	Operator logged in	MaryJo-Opti9020		cpamadmin	
8/24/2015 15:50:04	Operator logged out	MaryJo-Opti9020		cpamadmin	
8/24/2015 15:40:51	Credential records group-...				Total: 3; Processed:...
8/24/2015 14:21:55	Gateway Driver command:...	MaryJo-Opti9020		cpamadmin	
8/24/2015 14:21:42	Gateway Driver command:...	MaryJo-Opti9020		cpamadmin	
8/24/2015 13:28:38	Workstation: Logged In	CPAM-PC			
8/24/2015 13:28:38	Operator logged in	CPAM-PC		cpamadmin	
8/24/2015 13:06:40	Gateway Controller comm...	MaryJo-Opti9020		cpamadmin	
8/24/2015 10:26:42	Operator logged out	CPAM-PC		cpamadmin	
8/24/2015 10:26:42	Workstation: Logged Out	CPAM-PC			
8/21/2015 13:31:50	HID Controller command: ...	MaryJo-Opti9020		cpamadmin	
8/21/2015 13:30:11	HID Driver: Started	HID Driver			
8/21/2015 13:30:11	HID Controller: Offline	EVO 1 - Edge			
8/21/2015 13:30:09	HID Driver: Starting	HID Driver			
8/21/2015 13:30:09	Driver command: Start	MaryJo-Opti9020		cpamadmin	
8/21/2015 13:30:06	HID Driver: Stopped	HID Driver			
8/21/2015 13:30:06	HID Driver: Stopping	HID Driver			
8/21/2015 13:30:06	Driver command: Stop	MaryJo-Opti9020		cpamadmin	
8/21/2015 13:29:13	HID Driver: Started	HID Driver			
8/21/2015 13:29:13	HID Controller: Offline	EVO 1 - Edge			
8/21/2015 13:29:12	HID Driver: Starting	HID Driver			
8/21/2015 13:29:12	HID Driver: Stopped	HID Driver			
8/21/2015 13:29:12	HID Driver: Stopping	HID Driver			
8/21/2015 13:29:12	Driver command: Restart	MaryJo-Opti9020		cpamadmin	

Alarms: 5 active 100+ items cpama

Time: 8/27/2015 14:19:36.000
Description: Gateway Driver command: Apply Credential Cha
Log code: GW.DC.DRIVER_CRED_ALL
Type: Device Command
Device: MaryJo-Opti9020
Credential: cpamadmin
Location: Identiv, Inc.
Command: Apply Credential Changes...
Comments:
Target device: Access GW Driver

Note

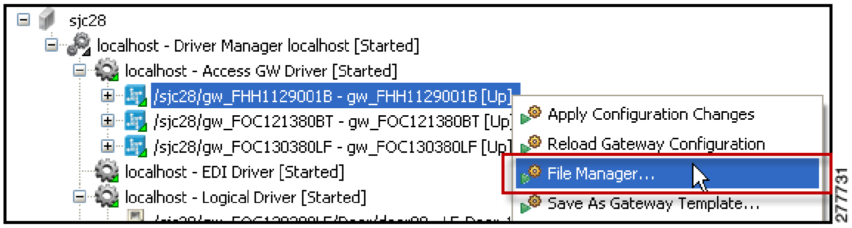
- The summary event is posted 10 minutes after all the gateways are updated.
- Any gateways that are still in the **Issued** state are shown as **Upgrade in progress** in the Data field.
- You cannot issue another **Bulk Image Upgrade** command until all the summary event is posted.

Step 9 (Optional) Use the File Manager to verify the active and running firmware image for a gateway.

Tip You can also change the active image using the File Manager.

a. Right-click a gateway (blue icon) and select **File Manager**, as shown in Figure C-13.

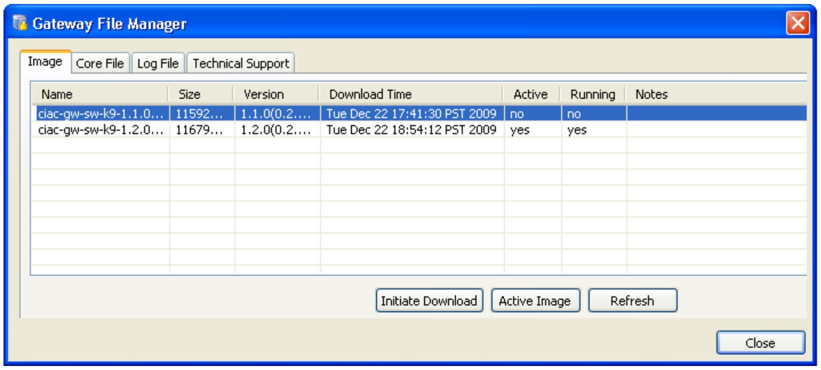
Figure C-13 File Manager Menu


Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
277731

sjc28
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/sjc28/gw_FHH1129001B - gw_FHH1129001B [Up]
/sjc28/gw_FOC121380BT - gw_FOC121380BT [Up]
/sjc28/gw_FOC130380LF - gw_FOC130380LF [Up]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]

b. Select the **Image** tab to display a list of the firmware images currently loaded on the gateway, as shown in Figure C-14.

Figure C-14 File Manager Window: Image Tab



Name	Size	Version	Download Time	Active	Running	Notes
ciac-gw-sw-k9-1.1.0...	11592...	1.1.0(0.2....	Tue Dec 22 17:41:30 PST 2009	no	no	
ciac-gw-sw-k9-1.2.0...	11679...	1.2.0(0.2....	Tue Dec 22 18:54:12 PST 2009	yes	yes	

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.
- **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.

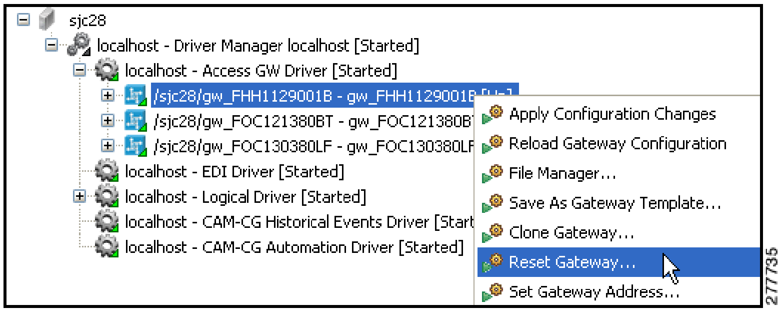
This step is necessary if you did not select the option to **Reset Gateway** in Step 5d. The *Active* image becomes the running image only after the gateway is reset.

To reset the gateway, do the following:

a. In the **Hardware - Tree** module, right-click a gateway (blue icon).

b. Select **Reset Gateway**, as shown in Figure C-15.

Figure C-15 Reset Gateway Command


sjc28
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/sjc28/gw_FHH1129001B - gw_FHH1129001B
/sjc28/gw_FOC121380BT - gw_FOC121380B
/sjc28/gw_FOC130380LF - gw_FOC130380LF
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - CAM-CG Historical Events Driver [Start
localhost - CAM-CG Automation Driver [Started]
Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
Clone Gateway...
Reset Gateway...
Set Gateway Address...
277735

Updating the Firmware on Individual Gateways

You can load more than one firmware image to a gateway, 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 Gateways, page C-15.

Before You Begin

Review the following before using the instructions to upgrading an individual gateway.

- This procedure loads the same firmware image to all gateways configured in ICPAM. If you check the options **Set as active image** and **Reset Gateway**, the gateways will reset with the new image as the active *running* image.
- An *Active* image is the image that will be operational when the gateway is reset. A *Running* image is the firmware image currently used to operate the gateway.
- Gateways operate normally while the firmware image is being copied from the TFTP server, but are out of service while being reset. When a gateway is down, the doors for that gateway remain locked if the lock is fail-secure, and unlocked otherwise. See Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 5-25 for more information.
- If you deselect the options **Set as active image** and **Reset Gateway**, then the firmware image is copied to the gateway, but is not made the *Active* or *Running* image. You must use the File Manager to manually activate the image on each gateway, as described in Step 8, and then reset the gateway, as described in Step 9.
- Review the recommendations in the “Select the Following Options When Upgrading Gateway Firmware” section on page B-6.

Procedure

Step 1 Complete the instructions in Uploading Firmware Images to a TFTP Server, page C-11

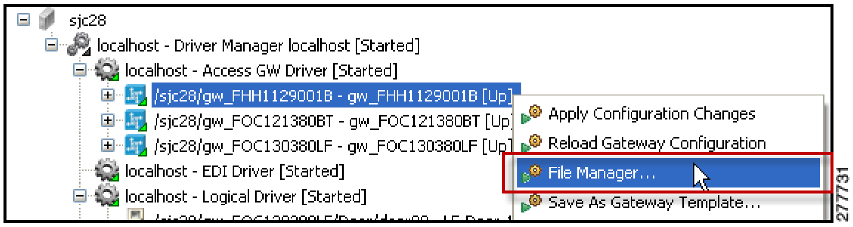
Step 2 Log in to the ICPAM desktop client.

See Logging into ICPAM Client, page 3-3.

Step 3 Select **Hardware - Tree** from the **Doors** menu.

Step 4 Right-click a gateway (blue icon) and select **File Manager** (Figure C-16).

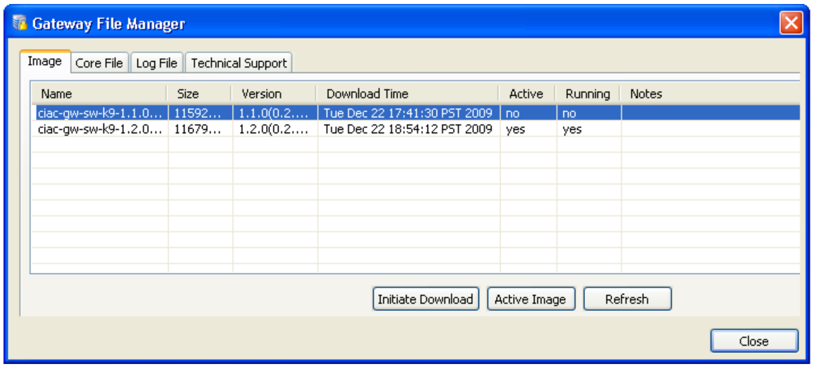
Figure C-16 File Manager Menu


sjc28
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/sjc28/gw_FHH1129001B - gw_FHH1129001B [Up]
/sjc28/gw_FOC121380BT - gw_FOC121380BT [Up]
/sjc28/gw_FOC130380LF - gw_FOC130380LF [Up]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
277731

Tip You can also access the **File Manager** using the **Door/Location-based Hardware** module. Select **Door/Location-based Hardware** 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 (Figure C-17).

Figure C-17 File Manager Window: Image Tab



Name	Size	Version	Download Time	Active	Running	Notes
ciac-gw-sw-k9-1.1.0...	11592...	1.1.0(0.2....	Tue Dec 22 17:41:30 PST 2009	no	no	
ciac-gw-sw-k9-1.2.0...	11679...	1.2.0(0.2....	Tue Dec 22 18:54:12 PST 2009	yes	yes	

Each row displays information about the firmware image:

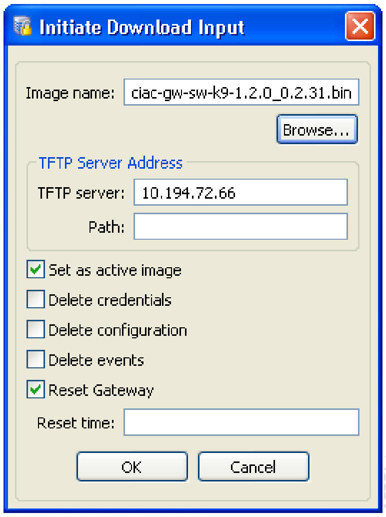
- **Name:** the image filename.
- **Version**: the firmware version number.
- **Download Time**: the time and date when the image was downloaded to the gateway.
- **Active**: The Active image will become the Running image when the gateway is reset. The image marked **Yes** is the active image on the 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



Initiate Download Input

Image name: ciac-gw-sw-k9-1.2.0_0.2.31.bin

Browse...

TFTP Server Address

TFTP server: 10.194.72.66

Path:

☑ Set as active image

☐ Delete credentials

☐ Delete configuration

☐ Delete events

☑ Reset Gateway

Reset time:

OK Cancel

b. Enter the **Image Name**:

- If the image is located on the ICPAM 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 ICPAM 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 ICPAM 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 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. 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 ICPAM 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.

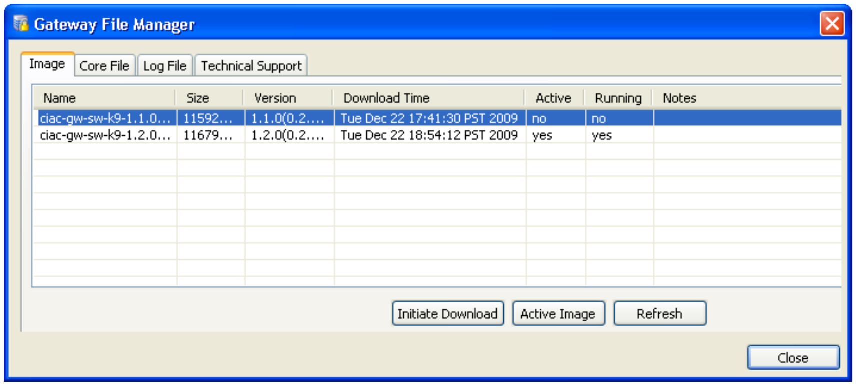
Note See the "Select the Following Options When Upgrading Gateway Firmware" section on page B-6.

Step 7 Click **OK** to close the window and copy the firmware image to the gateway.

- Any actions selected in Step 6e are initiated. For example, the new active image is set and the gateway 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



Name	Size	Version	Download Time	Active	Running	Notes
ciac-gw-sw-k9-1.1.0...	11592...	1.1.0(0.2....	Tue Dec 22 17:41:30 PST 2009	no	no	
ciac-gw-sw-k9-1.2.0...	11679...	1.2.0(0.2....	Tue Dec 22 18:54:12 PST 2009	yes	yes	

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.
- **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.

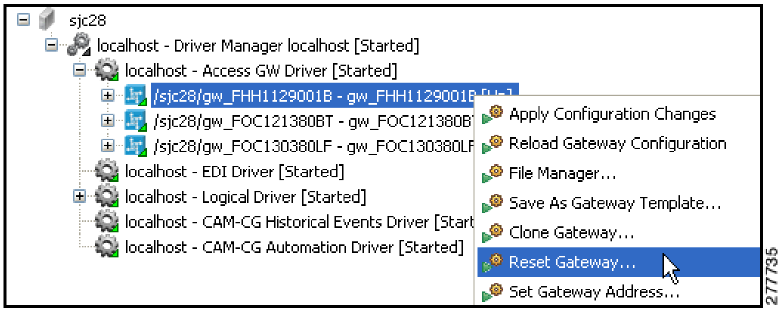
This step is necessary if you did not select the option to **Reset Gateway** in Step 6e, or want to change the Running image. The *Active* image becomes the *Running* image only after the gateway is reset.

To reset the gateway, do the following:

a. In the **Hardware - Tree** module, right-click the gateway (blue icon).

b. Select **Reset Gateway**, as shown in Figure C-20.

Figure C-20 Reset Gateway Command


sjc28
localhost - Driver Manager localhost [Started]
localhost - Access GW Driver [Started]
/sjc28/gw_FHH1129001B - gw_FHH1129001B [Up]
/sjc28/gw_FOC121380BT - gw_FOC121380B
/sjc28/gw_FOC130380LF - gw_FOC130380LF
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - CAM-CG Historical Events Driver [Start
localhost - CAM-CG Automation Driver [Started]
Apply Configuration Changes
Reload Gateway Configuration
File Manager...
Save As Gateway Template...
Clone Gateway...
Reset Gateway...
Set Gateway Address...
277735

Gateway Firmware Backward Compatibility

The ICPAM Release 2.1 is backward compatible with the Cisco PAM 1.5.1. Users using earlier versions of Cisco PAM should upgrade to version 1.3.2 and then to 1.5.1. The services that worked with Cisco PAM 1.5.0 continue to work with ICPAM 2.1.

ICPAM version 2.1 is backward compatible with gateways running firmware version 1.5.1 and earlier. gateways with version 1.5.1 work on ICPAM version 2.1 without upgrading the gateway's firmware. However, gateways running older firmware versions (1.3.2 to 1.4.1) have to be upgraded to 1.5.0 or 1.5.1 before working properly.

Note In ICPAM 2.1, CSV import of 500 records in MSP 1-RU platform and CSV import of 1000 records in OVA platform are recommended.

Note The gateway can be upgraded through web admin in Internet Explorer 8.0 or above only if TLS 1.1 is enabled in the IE browser's settings. To enable TLS 1.1, choose **Tools** > **Internet Options** > **Advanced**> **Security**, uncheck the **Use TLS 1.0** check box, and check **Use TLS 1.1** check box.

APPENDIX D

Security

This appendix includes information used to ensure the security of your ICPAM appliance.

Contents

ICPAM TCP Port Requirements for Firewall Connections

Table D-1 lists the TCP ports used by the ICPAM appliance. ICPAM desktop clients require access to these ports when connecting to a ICPAM appliance that is behind a firewall.

Table D-1 ICPAM Appliance Ports: Firewall Requirements

Port	Description
TCP 80	HTTP for video and redirect to HTTPS
TCP 443	HTTPS
TCP 1236	Fixed port for ICPAM client to server communications.
TCP 3306	MYSQL
TCP 8020	Default port for Gateway to ICPAM communication.
UDP 69	TFTP

Related Security Documentation

Refer to the following documentation for security information related to ICPAM.

- *Red Hat Enterprise Linux 6.4 Security Guide*
  https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html
- Security in MySQL
  http://dev.mysql.com/doc/mysql-security-excerpt/5.5/en/

Disabling the ICPAM TFTP Server

The ICPAM appliance includes a TFTP server that is enabled by default. This TFTP server is used primarily to store firmware images for upgrading controllers, as described in Upgrading Gateway Firmware Images Using ICPAM, page C-11.

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 ICPAM, page C-11 for more information.

Step 1 Log in to the ICPAM Server Administration utility.

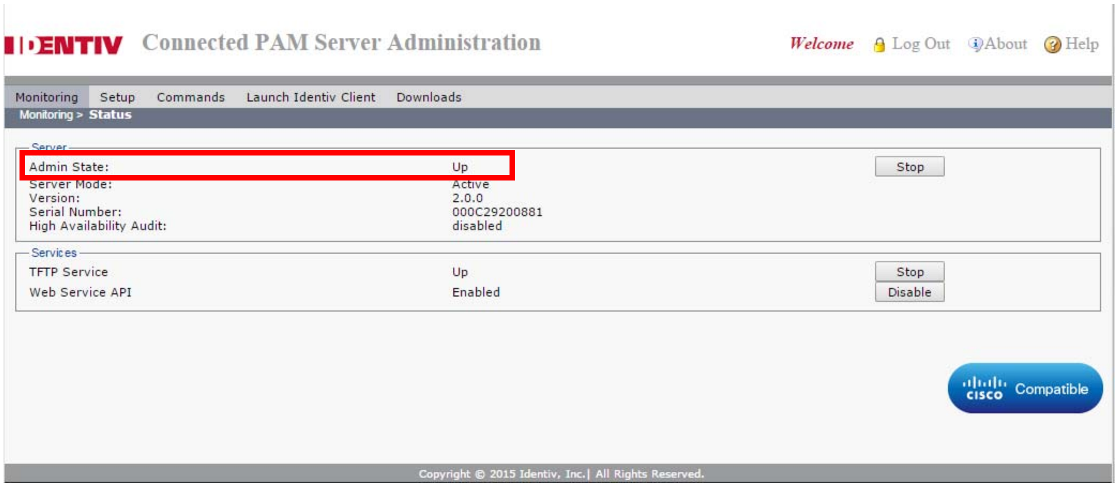
See Logging on to the ICPAM Server Administration Utility, page 2-2.

Step 2 Select the **Monitoring** tab and then select **Status**.

Step 3 Verify that the TFTP Service is **Up**, click **Stop**, as shown in Figure D-1.

Step 4 After the confirmation message appears, verify that TFTP Service is **Down**.

Figure D-1 TFTP Service in "Up" State



Server

Admin State: Up
Server Mode: Active
Version: 2.0.0
Serial Number: 000C29200881
High Availability Audit: disabled

Services

TFTP Service Up
Web Service API Enabled

Tip Once the TFTP Service is **Down**, the button changes to **Start**. Click **Start** to enable the TFTP server.

APPENDIX E

Troubleshooting

If your ICPAM 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

This section provides answers to common licensing questions. For more information, see “Obtaining and Installing Optional Feature Licenses” section on page 2-44.

Table E-1 Licensing: Frequently Asked Questions

Question	Answer
What does the ICPAM base license cover?	The base license includes these services and modules: • All hardware modules • Web services • Badge designer
What additional license SKUs are available for added modules?	None. All module licenses are purchases bundled with the hardware. New hardware does not require additional license installation.

Table E-1 Licensing: Frequently Asked Questions

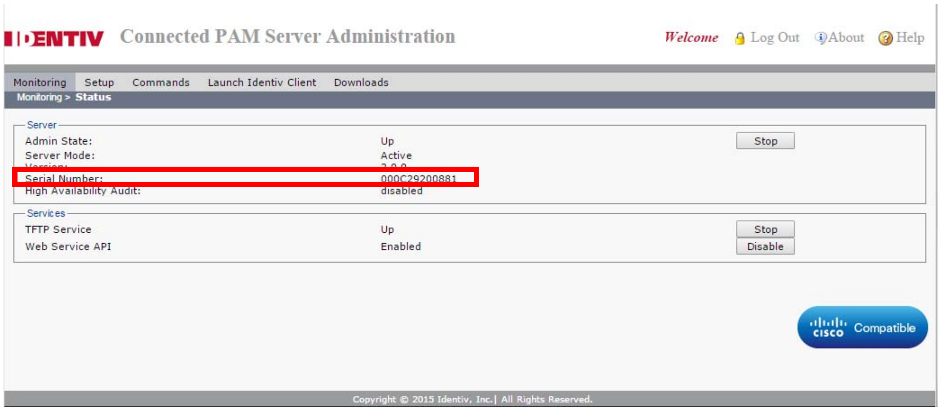
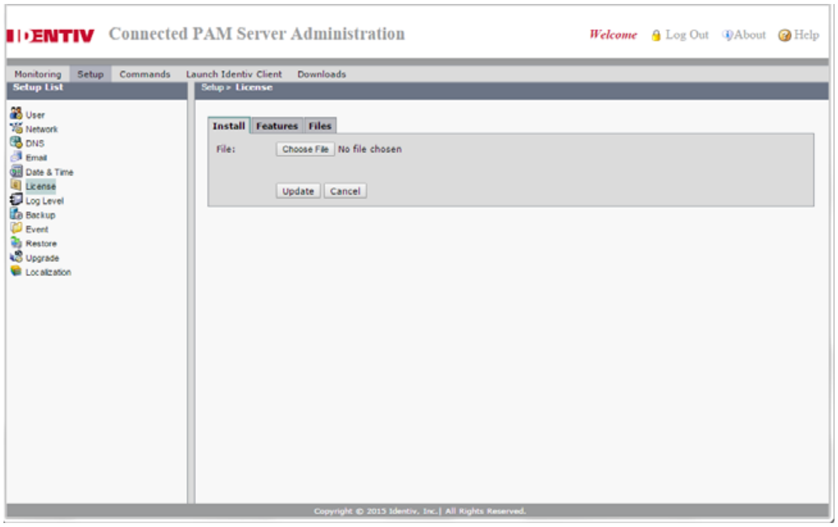
Question	Answer
How are licenses keyed to the specific server?	By the ICPAM software serial number that is obtained using the ICPAM admin web interface. The serial number is 16 digits in the range of 0-F. The server hardware serial number is not used.  IDENTIV Connected PAM Server Administration Welcome Log Out About Help Monitoring Setup Commands Launch Identiv Client Downloads Monitoring > Status Server Admin State: Up Stop Server Mode: Active Version: 2.0.0 Serial Number: 000C29200881 High Availability Audit: disabled Services TFTP Service Up Stop Web Service API Enabled Disable Compatible Copyright © 2015 Identiv, Inc.| All Rights Reserved.
If the ICPAM is in an HA (high availability) configuration with two servers, do I need two copies of each license?	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.
What is the SKU for the HA feature?	CIAC-CPAME-HA= is the SKU for the HA license.
Can a license be moved to another ICPAM server?	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.
Who handles licensing issues for the ICPAM server?	Identiv customer support can assist with installing a license but cannot generate licenses. If you have a problem with the license file itself you can email licensing@identiv.com and seek additional assistance. You should include the ICPAM serial number and the purchase or sales order number as well.
What software features require a license?	• The Enterprise Data Integration feature requires SKU CIAC-EDI= • The HA feature requires CIAC-PAME-HA= • The EAI feature requires CIAC-PAME-EAI=

Table E-1 Licensing: Frequently Asked Questions

Question	Answer
What is the process to acquire additional licenses?	Identiv or our partner generates a sales order and the licensing team then generates a PAK (Product Authorization Key). The PAK is entered into the Identiv.com licensing portal, and a license file is generated. The file can be downloaded at this point. The file is then installed onto the ICPAM 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 2-44.  IDENTIV Connected PAM Server Administration Welcome Log Out About Help Monitoring Setup Commands Launch Identiv Client Downloads Setup List User Network DNS Email Date & Time License Log Level Backup Event Restore Upgrade Localization Setup > License Install Features Files File: Choose File No file chosen Update Cancel Copyright © 2013 Identiv, Inc.| All Rights Reserved.
What are controller conversion licenses for?	These are for supporting non-ICPAM access panels.

APPENDIX F

Related Documentation

Refer to the following documentation for additional information and instructions for the features and subjects discussed in this guide:

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

Physical Access Control User Documentation

- Identiv Connected Access Control API Reference Guide
- Identiv Connected Physical Access Manager User Guide
- Identiv Connected Physical Access Manager Quick Start Guide
- Cisco Physical Access Gateway Quick Start Guide
- Cisco Physical Access Gateway User Guide
- Cisco Physical Security Multiservices Platform Series User Guide
- Release Notes for ICPAM

Cisco Video Surveillance Manager (Cisco VSM) User Documentation

- Cisco Video Surveillance Manager User Guide, Release 6.3
- 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 ICPAM.

- *Red Hat Enterprise Linux 6.4 Security Guide*
https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html
- Security in MySQL
http://dev.mysql.com/doc/mysql-security-excerpt/5.5/en/

GLOSSARY

A

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

Access policy

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

ADA

ADA is an abbreviation for the Americans with Disabilities Act.

ADA strike time

ADA strike time refers to the ability of ICPAM 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 ICPAM refers to a type of credential used for biometric verification.

C

Calendar A calendar defines a set of holidays. The holidays within the calendars are then used in conjunction with access policies to control access during holiday periods.

Camera Cameras record digital video files to be stored on the DVR.

See also: Closed Circuit Television

CAN (Controller Area Network) bus A 3 wire parallel communication bus that runs between the Gateway and up to a total of 15 additional modules. These additional modules can be any combination of Reader, Input, or Output modules.

The distance limit on the CAN bus is 1320 feet. The last module on the CAN bus must be set to terminate the Can bus.

Card See Badge.

Card format The bit structure of a particular card. The average card format includes the card number, facility code, and parity bits. The two types of card formats supported by ICPAM are Wiegand and magstripe.

Card format type The type of a card format, which may be Wiegand or magstripe.

See also: Wiegand

See also: Magnetic Stripe

Card number The card number encoded within the badge, often on the magnetic stripe or internally for proximity cards.

See also: Badge

CCTV Closed Circuit Television

CHUID/CUID Card Holder Unique Identity Model.

Closed Circuit Television A collection of surveillance cameras conducting video surveillance. Each camera is viewable on a monitor.

Controller

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 via Ethernet. It also communicates up to 15 additional reader, input, or output modules over a 3-wire CAN bus. The gateway can be powered using either PoE or 12V or 24V DC.

The controller can download badge access credentials and store them locally permitting access control even without network connectivity to the ICPAM server. Events that occur while the connection to the server is down are stored locally and uploaded to the ICPAM server once the network connection resumes.

Two types of controllers are offered by Identiv: Cisco Gateway and EM-100 Edge Controller.

Credential

A general category that includes login, badge, and biometric; something that isused to gain access to a physical or logical resource.

See also: Login

See also: Badge

See also: Biometric

D

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 controller to the ICPAM server and TCP port to use for the Gateway to ICPAM server TCP/IP session. The Gateway can also have a static IP address. The ICPAM 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

E

EDI

EDI (Electronic Data Interchange) is the transfer of data from one computer system to another by standardized message formatting without the need for human intervention. EDI permits multiple companies -- possibly in different countries -- to exchange documents electronically. Data can be exchanged through serial links and peer-to-peer networks, though most exchanges currently rely on the Internet for connectivity.

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 controller are encrypted.

ICPAM 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

F

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

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 graphic maps.

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

HA High availability. In the event of physical server failure, affected virtual machines are automatically restarted on other production servers with spare capacity. In the case of operating system failure, VMware HA restarts the affected virtual machine on the same physical server.

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 - Tree module and the graphics. 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 The Homeland Security Presidential Directive 12. A a policy for a common identification standard for federal employees and contractors.

HTTPS Hypertext Transfer Protocol Secure. A combination of the Hypertext Transfer Protocol and a network security protocol. Gateway and ICPAM HTTP access is via HTTPS.

See also SSL.

I

ICPAM client A Java applet that runs on a Windows client PC or workstation that is used to manage the ICPAM 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 ICPAM server and the access modules.

ICPAM server An appliance used to manager and monitor a physical access infrastructure comprised of 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.

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 ICPAM server via the CAN bus and the controller. The module requires an external 12V to 24V DC source and can not be powered via POE.

IP address The Internet Protocol address. The ICPAM 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 controller to the ICPAM server and TCP port to use for the gateway to ICPAM server TCP/IP session. The Gateway can also have a static IP address. The ICPAM 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 ICPAM 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 ICPAM server via the CAN bus and the controller. 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

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 policies and profiles.

See also: Credential

See also: Profile

See also: Access policy

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 controller to facilitate communication with a ICPAM 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 ICPAM 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 ICPAM 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 an ICPAM 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 ICPAM server can utilize SSL for the connection. All gateways and ICPAM server must be configured for SSL, or for no SSL. A mix of SSL and non-SSL is not supported.

Gateway and ICPAM 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, ICPAM can determine if a wire is cut or shorted.

See also input and Input module. See Device Configuration Properties for more information.

T

TCP/IP communications A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

Telnet An Internet communications protocol that enables a computer to function as a terminal working from a remote computer.

Time interval 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.

Time received The time an event or alarm was actually received by the access-control system and stored in the database.

Time schedule A defined set of time intervals used to make access-control, triggering, and other decisions. See also: Time interval

Time zone 24 longitudinal divisions of the globe, nominally 15 degrees wide, in which clocks show the same time.

TM input This input is used to detect if a component box is being tampered with. It acts like a normal input and would be in the normally closed position indicating that the component box access door is closed. Once opened, this input would alert and administrator that the component access door is, or was, opened. The TM input has 2 pins marked + and -. This input can be re-allocated to act as an unsupervised input.

Top alarm The most important alarm present at a given device. Based on alarm state, time, and priority. See also: Alarm and Alarm state

Top alarm state The state of the top alarm at a given device. Possible states include active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity. Not to be confused with device status, which is independent of operator actions in the application. For example, if a door is forced open, and then shut again, the status will go from forced open to secure, butthe top alarm state will reflect the forced open state until an operator clears it. See also: Device Status and Alarm state

Trigger A trigger waits for an operator-defined combination of events, addresses, properties, and time schedules to occur, then executes a procedure. See also: Procedure

TTR Triple Technology Reader. A reader which combines three devices in one: a magnetic card reader, HID proximity card reader, and piezoelectric keypad.

U

Use limit An option which can restrict a badge to a certain number of uses. The default is 0 (off). See also: Badge

Username A sequence of characters used as identification when logging onto the application.

V

View query An option within the filter tools, giving operators the capability to view the actual filter definition as an SQL-like expression string. See also: Filter

VIN pins Voltage input. This is where you can use +12 to +24 volts DC to power the module.

W

Wiegand card format Wiegand card format stores card data using binary values. The information includes parity error detection, facility code and the card ID. Each card has a particular format that must be configured in the access-control panel to permit the panel to correctly interpret the card data. A very common Wiegand card format is a 26 bit format, with the first and last bit for parity, 8 bits for the facility code and 16 bits for the card number.

When configuring the Credential Template on the ICPAM 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