



## **Identiv Connected Physical Access Manager 2.2 Installation Guide**

June 22, 2016

**Identiv, Inc.**  
[www.identiv.com](http://www.identiv.com)

Copyright © 2015-2016 Identiv, Inc. All rights reserved.

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

Phone: (949) 250-8888  
Fax: (949) 250-7372  
Web: [www.identiv.com](http://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)

## Revision History

| <b>Text Part Number</b> | <b>Date Published</b> | <b>Description</b>   |
|-------------------------|-----------------------|--|
| IC02-02                 | June 22, 2016         | Corresponds to the ICPAM 2.2 release, which includes bug fixes and adds support for: the optional Exit Reader Expansion Module for EM-100 controllers; anti-passback for EM-100 controllers; and the "Reset All Card Holder Status" right-click command for the Identiv EM-100 Driver. |
| IC02-01                 | January 7, 2016       | Corresponds to the ICPAM 2.1 release, which adds support for Identiv's EM-100 single-door controller.  |

# Contents

|   |     |
|---|-----|
| Revision History .....  | ii  |
| Contents .....  | iii |
| List of Figures .....   | v   |
| List of Tables .....  | vii |
| Introduction .....  | 1   |
| What is ICPAM? .....  | 1   |
| Upgrade Paths .....   | 2   |
| System Requirements .....   | 3   |
| Network Design Requirements and Recommendations .....                                       | 4   |
| Static IP Addresses versus DHCP .....   | 4   |
| Firewall Configuration .....  | 4   |
| Default Services and Ports for the EM-100 Controller .....                                  | 5   |
| Using a Separate Virtual LAN for Your Security System .....                                 | 6   |
| Using a Network Time Protocol (NTP) Server .....  | 6   |
| Installing and Configuring the ICPAM Server Software .....                                  | 7   |
| Prerequisites for Installing the ICPAM Server Software .....                                | 7   |
| Installing VMware .....   | 7   |
| Deploying the OVA File for ICPAM and Editing the Virtual Machine Settings .....             | 8   |
| Launching the ICPAM Server Virtual Machine for the First Time .....                         | 9   |
| Obtaining Super-user Privilege .....  | 12  |
| Configuring the ICPAM Server's Network Settings .....                                       | 13  |
| Launching the ICPAM Server Administration Program .....                                     | 17  |
| Configuring the ICPAM Server Software .....   | 18  |
| Installing the Necessary Version of the Java Runtime Environment and the ICPAM Client ..... | 29  |
| Upgrading a High Availability Pair of ICPAM Servers .....                                   | 34  |
| Installing and Configuring Door Controllers .....   | 35  |
| Cisco Physical Access Gateways .....  | 35  |
| Overview of a Gateway .....   | 35  |
| Installing a Gateway .....  | 39  |
| Configuring a Gateway .....   | 46  |
| Identiv EM-100 Controllers .....  | 48  |
| Overview of an EM-100 Controller .....  | 48  |
| Installing an EM-100 Controller .....   | 51  |
| Configuring an EM-100 Controller .....  | 56  |
| Optical Tamper Feature of an EM-100 Controller .....  | 61  |
| Beep Patterns of an EM-100 Controller .....   | 61  |
| Resetting an EM-100 Controller's Password and IP Address .....                              | 62  |
| Connecting an Exit Reader Expansion Module .....  | 64  |



## List of Figures

|   |    |
|---|----|
| Figure 1: Major Components of an ICPAM Security System .....                                | 1  |
| Figure 2: VMware Settings for the ICPAM OVA File.....                                       | 8  |
| Figure 3: VMware vSphere Client Login Dialog .....  | 9  |
| Figure 4: VMware Console Window.....  | 10 |
| Figure 5: Username Field for VMware Login.....  | 10 |
| Figure 6: Password Field for VMware Login.....  | 11 |
| Figure 7: Red Hat Enterprise Linux (RHEL) Console Screen .....                              | 11 |
| Figure 8: Terminal Command Line Dialog .....  | 12 |
| Figure 9: Super-User Permissions Command Line .....   | 12 |
| Figure 10: Root Authority Prompt Command Line.....  | 13 |
| Figure 11: Root Prompt Commands .....   | 13 |
| Figure 12: vi Text Editor ifcfg-eth0 File Example .....                                     | 14 |
| Figure 13: vi Text Editor Insert Mode Indicator .....                                       | 15 |
| Figure 14: Running service network restart.....   | 16 |
| Figure 15: Running service immortal restart.....  | 16 |
| Figure 16: ICPAM Server Administration - Login Page.....                                    | 17 |
| Figure 17: ICPAM Server Administration - Server Page.....                                   | 18 |
| Figure 18: ICPAM Server Administration - User Page.....                                     | 19 |
| Figure 19: ICPAM Server Administration - Network Page .....                                 | 20 |
| Figure 20: ICPAM Server Administration - DNS Page .....                                     | 22 |
| Figure 21: ICPAM Server Administration - Email6 Page.....                                   | 22 |
| Figure 22: ICPAM Server Administration - Date & Time Page .....                             | 23 |
| Figure 23: ICPAM Server Administration - Event Page (Pruning Subpage).....                  | 24 |
| Figure 24: ICPAM Server Administration - Event Page (Archive Subpage).....                  | 25 |
| Figure 25: ICPAM Server Administration - License Page.....                                  | 27 |
| Figure 26: ICPAM Server Administration Login Page - with Link to Launch ICPAM Client.....   | 29 |
| Figure 27: ICPAM Server Administration - Downloads Page .....                               | 30 |
| Figure 28: ICPAM Client Installation - Welcome Page.....                                    | 31 |
| Figure 29: ICPAM Client Installation - Target Path Page.....                                | 31 |
| Figure 30: ICPAM Client Installation - Installation page .....                              | 32 |
| Figure 31: Log In Dialog for the ICPAM Client .....   | 32 |
| Figure 32: Welcome Page of the ICPAM Client.....  | 33 |
| Figure 33: Cisco Physical Access Gateway.....   | 35 |
| Figure 34: Cisco Physical Access Gateway - Back and Top Views (with Labels) .....           | 36 |
| Figure 35: Three Options for Installing a Gateway's Wall Brackets .....                     | 39 |
| Figure 36: Gateway Power Connections .....  | 40 |
| Figure 37: Wiegand Interface Connections on Gateway and Reader Modules.....                 | 42 |
| Figure 38: Wiring of Termination Resistors for Supervised Input Connections.....            | 43 |
| Figure 39: Input Connections on the Cisco Physical Access Gateway .....                     | 43 |
| Figure 40: Output Connections on the Cisco Physical Access Gateway.....                     | 45 |
| Figure 41: ETH 0 (and ETH1) Ethernet Connections on the Cisco Physical Access Gateway ..... | 45 |
| Figure 42: Configuring the Cisco Access Control Gateway - Network Setup Page .....          | 46 |
| Figure 43: Installing the Mounting Plate for an EM-100 Controller.....                      | 51 |
| Figure 44: Commonly Used Connections on the EM-100 Controller.....                          | 52 |
| Figure 45: Wiring Connections on the EM-100 Controller.....                                 | 52 |
| Figure 46: Example Wiring Diagram for an EM-100 Controller .....                            | 55 |

Figure 47: EM-100 Configuration - Warning that Connection Is Not Private ..... 56

Figure 48: EM-100 Configuration - Authentication Required Dialog..... 57

Figure 49: EM-100 Configuration - Basic Network Setup Page ..... 57

Figure 50: EM-100 Configuration - Advanced Network Setup Page (Part 1)..... 58

Figure 51: EM-100 Configuration - Advanced Network Setup Page (Part 2)..... 59

Figure 52: EM-100 Configuration - System Status Page..... 60

Figure 53: Debug Port Jumper Pins on an EM-100 Controller..... 62

Figure 54: Wiring Connections on the Exit Reader Expansion Module (for an EM-100 Controller)..... 64

---

## List of Tables

|   |    |
|---|----|
| Table 1: Minimum Requirements for an ICPAM System .....                               | 3  |
| Table 2: Network Ports of the ICPAM Server .....                                      | 4  |
| Table 3: Security Recommendations for an EM-100 controller's Services and Ports ..... | 5  |
| Table 4: EM-100 Controller: General Specifications .....                              | 48 |
| Table 5: EM-100 Controller: Power Specifications .....                                | 49 |
| Table 6: Function of the Pins on an EM-100 Controller .....                           | 53 |
| Table 7: Beep Patterns of an EM-100 Controller .....                                  | 61 |
| Table 8: Function of the Pins on an Exit Reader Expansion Module .....                | 64 |





## Introduction

This document explains how to install and configure the major components of an ICPAM security system, including:

- VMware and the ICPAM Server software
- the ICPAM Desktop Client (and the necessary version of the Java Runtime Environment)
- Cisco Physical Access Gateways and expansion modules
- Identiv EM-100 Controllers and expansion modules

### What is ICPAM?

ICPAM is an acronym for the Identiv Connected Physical Access Manager software, which is the successor to the Cisco Physical Access Manager (CPAM) software. This server-level software is operated using desktop client software, and manages a network of controllers which enforce physical access control for a collection of secured doors and other devices. The controllers are initially configured using a built-in utility program.

The following diagram shows the major components of a security system based on ICPAM.

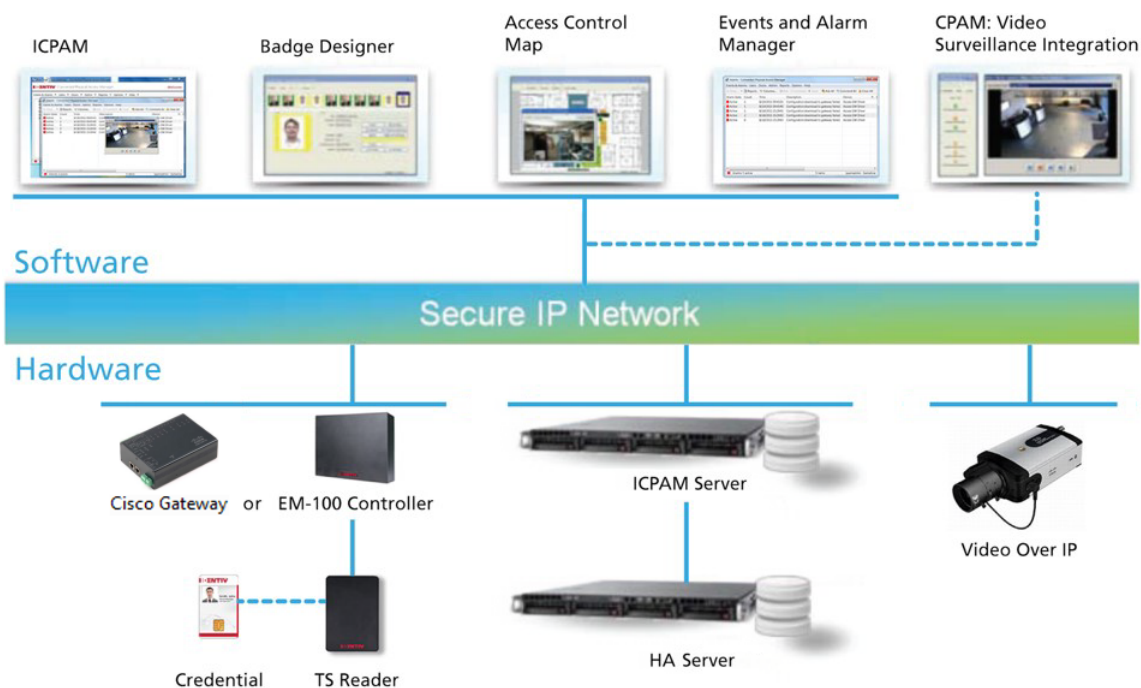


Figure 1: Major Components of an ICPAM Security System

CPAM supported the Cisco Physical Access Gateway (CIAC-GW-K9) controller, which can manage two doors per controller. ICPAM supports both the Cisco Physical Access Gateway controller and the Identiv EM-100 controller. The EM-100 controller can manage one door.

NOTE: Cisco's Physical Access Gateway is no longer being manufactured or sold.

In the ICPAM 2.1 and 2.1.1 releases, the EM-100 controller supported only one (entry) reader. In the ICPAM 2.2 release, the EM-100 controller supports an Exit Reader Expansion Module which adds a second (exit) reader to the door. Having an exit reader makes it possible to better track a person's location or movements, and provides more flexibility when defining and enforcing anti-passback areas.

For additional information about the software components of an ICPAM security system, see the **ICPAM Software Overview** section in Chapter 1 of the **ICPAM User Guide**.

## Upgrade Paths

ICPAM 2.2 is a **required** upgrade for:

- existing CPAM customers who need to add EM-100 controllers to their security system (because the Cisco Physical Access Gateway is no longer being sold)
- existing ICPAM 2.1 or 2.1.1 customers (whose security system includes any mixture of Cisco Physical Access Gateways and EM-100 controllers) who need to add the optional Exit Reader Expansion Module to an EM-100 controller

ICPAM 2.2 is a **recommended** upgrade for:

- existing CPAM customers who need certain bug fixes available only in ICPAM
- existing ICPAM 2.1 or 2.1.1 customers who need certain bug fixes available only in the 2.2 release

In-place upgrades from existing customer deployments of CPAM 1.5.3 are supported. There is no need to make configuration changes or replace current UCS, gateway, or desktop hardware, on operating systems that meet the minimum system requirements. Cisco Physical Access Gateways must be upgraded to v1.5.3 firmware, before upgrading from CPAM to ICPAM.

The following upgrade paths to ICPAM 2.2 are supported:

- ICPAM 2.1.1 to ICPAM 2.2
- ICPAM 2.1.0 to ICPAM 2.2
- CPAM 1.5.3 to ICPAM 2.2



*System configuration checks are performed as part of the upgrade process. The upgrade process will gracefully exit, leaving the system in its original state, if either of the following conditions is detected:*

- *A CPAM version earlier than v1.5.3*
- *A VSM 6.x (or earlier) driver is installed*

Customers using an older version of CPAM (versions 1.5.2 and below) will need to first upgrade to CPAM 1.5.3 before upgrading to ICPAM 2.2. Customers using VSM 6.x (or earlier) will need to first upgrade to VSM 7.x before upgrading to ICPAM 2.2.

You might also need to upgrade some other components of your existing CPAM system, so it meets the minimum requirements for an ICPAM system. For example:

- The Cisco CPS-MSP server is not supported by ICPAM, because it does not meet the minimum requirements.
- Upgrades of existing CPAM installs on bare metal USC C-Series servers with at least 16GB of RAM are supported.
- New installs of ICPAM require VMware.

## System Requirements

The following table lists the minimum requirements for an ICPAM system.

**Table 1: Minimum Requirements for an ICPAM System**

| <b>Category</b>                   | <b>List of Requirements</b>   |
|-----------------------------------|---|
| ICPAM Server Hardware             | <ul style="list-style-type: none"> <li>• 4 virtual processors</li> <li>• at least 16GB of RAM</li> <li>• sufficient hard drive capacity (at least 500GB) to accommodate the database and software</li> </ul> <p>NOTE: The actual capacity needed will vary with event archival strategy, user count, controller count, event rates, etc.</p>  |
| ICPAM Server Software             | <ul style="list-style-type: none"> <li>• ICPAM 2.1.0, ICPAM 2.1.1, or ICPAM 2.2</li> <li>• VMware vSphere 5.x or 6.x (because an ICPAM server runs as a Linux Virtual Appliance)</li> </ul> <p>NOTE: Other virtualization products (such as Oracle VirtualBox, Microsoft HyperV, Xen, etc.) are not supported.</p>  |
| ICPAM Client Workstation Hardware | <ul style="list-style-type: none"> <li>• modern Intel or AMD multi-core processor</li> <li>• 4GB RAM</li> <li>• 250MB hard disk space available for the application</li> </ul>  |
| ICPAM Client Workstation Software | <ul style="list-style-type: none"> <li>• Operating System: Windows 7 or Windows 8</li> <li>• User account with administrative privileges</li> <li>• Web browser: Internet Explorer versions 8 through 11</li> <li>• Java Runtime Environment (JRE): 32-bit version 1.6 (release 27) or 32-bit version 1.7 (release 79), for both installation and normal use.</li> </ul> <p>NOTE: Auto-updating of the JRE must be disabled.</p>  |
| Door Controller Firmware          | <ul style="list-style-type: none"> <li>• Identiv EM-100 Controllers: firmware release 3.5.1 is required. (Firmware release 3.5.1 is installed on each EM-100 controller at the factory.)</li> <li>• Cisco Physical Access Gateways: firmware release 1.5.3 is required. You might need to upgrade the firmware on some older Physical Access Gateways. (For information about how to upgrade the firmware, see the <b>Cisco Physical Access Gateway User Guide</b>.)</li> </ul> |

## Network Design Requirements and Recommendations

The following set of topics provide information about designing the network for your security system.

### Static IP Addresses versus DHCP

The ICPAM Server must know the network address of every door controller that it manages. Acceptable addressing options for the door controllers include:

- Static IP addresses
- Dynamic Host Control Protocol (DHCP) with reserved addresses
- DHCP linked to a Domain Name System (DNS), where the door controllers are identified by hostnames

Static IP address is the recommended way to configure the EM-100 controller network settings. After modifying the EM-100 controller's network configuration, the controller re-initializes the network interface and attempts to connect to the Host.

An EM-100 controller can utilize DHCP to obtain an IP address. If the controller cannot obtain an IP address from a DHCP server within approximately 60 seconds after powering up, it defaults to an IP address of 169.254.242.121. But this Alias IP address is only accessible through a direct connection, because it is in a non-routable range of IP addresses.

A Dynamic Host Control Protocol (DHCP) network can be used only if the addresses designated for the attached EM-100 controllers have been reserved in advance. (Most DHCP-enabled routers provide a section on reservations that allow the configurator to set up one or more static addresses for assignment to those devices that require it.) Otherwise, static IP addresses are recommended.

### Firewall Configuration

When the ICPAM appliance is behind a firewall, you must open the network ports listed in the following table, so the ICPAM Server software can communicate with Gateways and ICPAM Desktop Clients.

**Table 2: Network Ports of the ICPAM Server**

| Network Port | Description  |
|--------------|--|
| TCP 80       | HTTP for video and redirect to HTTPS                             |
| TCP 443      | HTTPS  |
| TCP 1236     | Communication between the ICPAM Clients and the ICPAM Server     |
| TCP 3306     | MYSQL  |
| TCP 4070     | Default port for EM-100 Controller to ICPAM Server communication |
| TCP 8020     | Default port for Gateway to ICPAM Server communication           |
| UDP 69       | TFTP   |

For more information, see **Appendix D: Security** in the **ICPAM User Guide**.

When installing the EM-100 controller to communicate through a firewall, the firewall must allow TCP data transfer to the ICPAM server on the specified port and UDP data transfer from the ICPAM server out through the firewall.

For server/host-originated communication, firewall configuration may be required. Open the following ports on the firewall for EM-100 controller communication:

- ICPAM initiated EM-100 inbound UDP port (4050 default)
- EM-100 initiated outbound TCP port (4070 default)

The connection port is utilized by the server/host to contact an EM-100 controller. Use the connection port as an inbound connection for the EM-100.

The listen port is utilized by the EM-100 controller to communicate with the server/host. Use the listen port as an outbound connection for the EM-100.

If unfamiliar with configuring a network firewall, contact the Network/IT Administrator, or consult your firewall user/installation manual.

For more information about the default port values available for the EM-100 controller, refer to the following table.

**CAUTION** *Unless the firewall is properly configured, the controller cannot communicate with the ICPAM Server.*

### Default Services and Ports for the EM-100 Controller

The EM-100 controller uses standard TCP and UDP packets to send and receive data between the ICPAM server and other EM-100 controllers. The default network ports used by ICPAM are:

- TCP port 4050, from the ICPAM Server to EM-100 controllers
- TCP port 4070, from EM-100 controllers to the ICPAM Server
- UDP port 9000, from an EM-100 controller to other EM-100 controllers

Out of the box, an EM-100 controller has the following ports open. You can modify or shut off some of these ports to make the controller more secure. To make the controller more secure, follow the recommendations in the following table.

**Table 3: Security Recommendations for an EM-100 controller's Services and Ports**

| Port or Service | Purpose  | Security Recommendation  |
|-----------------|--|--|
| TCP 20/21       | File Transfer Protocol (FTP)                             | Disable through the Advanced Setup Web pages built into the controller, and enable only when a firmware update occurs. |
| TCP 22          | Secure Shell (SSH/SCP) only on R2.3.1 units              | Disable through the Advanced Setup Web pages built into the controller, and enable only when a firmware update occurs. |
| TCP 23          | Telnet   | Disable through the Advanced Setup Web pages built into the controller, and enable only when a firmware update occurs. |
| TCP 80/443      | Web Server/SSL Web Server (R2.2.7.145+ and R2.3.1 units) | Set the Administrator password appropriately, per the 6-10 character requirement built into the Web pages.             |

|                    |  |   |
|--------------------|--|---|
| TCP 4050           | EM-100 Controller Listening Port   | Modify the port value using the Advanced Setup Web pages built into the controller. If utilized for primary communications with the controller, then you should also enable encryption (as explained on page 60). |
| TCP 4070           | EM-100 Controller Connection Port  | Modify the port value using the Advanced Setup Web pages built into the controller. If utilized for primary communications with the controller, then you should also enable encryption (as explained on page 60). |
| UDP 4070           | Discovery GUI Communication Port; from the EM-100 Controller to the ICPAM Server | Limit the use of the Discovery GUI to the controller's initial installation.  |
| UDP 9000           | Peer to Peer Communication between EM-100 Controllers                            | The data is already protected, and the use of this port is only enabled when the Peer to Peer capability is enabled.  |
| IP 169.254.242.121 | Alias IP Address used for Direct Connect Configuration                           | After configuring the controller, disable this IP address through the Advanced Setup Web pages built into the controller. This non-routable IP address is limited to use with a Direct Connection.                |
| Linux root Login   | For Web (R227 only), telnet, FTP, and SSH (R231 only)                            | Modify the default password.  |

### Using a Separate Virtual LAN for Your Security System

As a best practice, you should use a separate Virtual LAN (with an exclusive dedicated subnet) for the networked devices which are part of your security system. Those devices include the ICPAM Servers, the Cisco Physical Access Gateways, and the Identiv EM-100 Controllers.

Using a Virtual LAN helps ensure that the communication between the ICPAM Server and the door controllers is not delayed by other traffic on the network. This is especially important on a network which is also used for voice data (VOIP) or video data (VSOM).

### Using a Network Time Protocol (NTP) Server

To prevent inconsistent system behavior, you should use a Network Time Protocol (NTP) server to synchronize the date and time on the ICPAM server appliance and on each Cisco Physical Access Gateway. The same NTP server should be used for all components of your security system, including an optional High Availability server and any optional integrations such as the Video Surveillance Manager.

---

# Installing and Configuring the ICPAM Server Software

The following sections provide detailed instructions on setting up the ICPAM server software platform, including VMware.

## Prerequisites for Installing the ICPAM Server Software

Before you start installing the ICPAM server and client, make sure you have done the following:

- Ensure that the components of your ICPAM system meet the minimum requirements, as listed in "System Requirements" on page 3.
- Ensure that the BIOS on your ICPAM server is enabled for virtualization (called 'virtualization technology' or 'Intel VT').
- Specify a fixed IP address for your ICPAM server and make sure that there are two IP addresses available for the VMware server and the ICPAM server. If you are running Dynamic Host Configuration Protocol (DHCP) on your router or switch, reserve two IP addresses for this purpose.
- Ensure the ICPAM server is connected to the network and has proper connectivity.
- Connect at least one EM-100 controller or Cisco gateway via Ethernet or USB to the server.
- Download the necessary software components (such as drivers and upgrades) for the controller(s) and other attached components.

## Installing VMware

An ICPAM server runs as a Linux Virtual Appliance within a native Windows environment. This means that in order to run the ICPAM server on a PC, you need to install VMware. (Other virtualization products, such as Virtual Box or HyperV, are not supported.) The recommended version of VMware is version 5.1 or 6.x.

There are several products in the VMware family. Although there is a free product called VMware Player, it is not supported for use with ICPAM. The ESXi vSphere or VMware Workstation products require licenses and must be paid for after a brief evaluation period.

- **VMware Workstation** might be sufficient for small testing environments, but it is not supported for use with an ICPAM production system. It can be downloaded from:

<http://www.vmware.com/products/player/playerpro-evaluation.html>

- **VMware ESXi vSphere** 6.x is the required version of VMware for an ICPAM production system, and it includes the vSphere Hypervisor as virtualization manager and user interface. It can be downloaded from:

<https://my.vmware.com/web/vmware/evalcenter?p=free-esxi6>

Obtain the appropriate VMware product for your system's requirements, and install it according to the instructions provided by the VMware installation wizard.

## Deploying the OVA File for ICPAM and Editing the Virtual Machine Settings

An OVA file is a pre-configured virtual appliance that can be deployed to your VMware environment to enable one or more guest operating systems to reside on your host operating system. The ICPAM OVA file contains a Linux environment pre-configured for the ICPAM server software.

- To download the current OVA, go to **www.identiv.com/icpam-support**. Follow the instructions for registering and downloading the latest ICPAM OVA.
- In the VMware software, perform one of the following tasks (according to which product you have installed):
  - For vSphere client, select **Deploy OVF Template...** from the **File** menu.
  - For VMware Workstation (which is supported only for a small testing environment), select **File > Open**.
- Browse to the location where you downloaded the ICPAM OVA file and select it.
- Click **Import** or **Open**.
- After the OVA file is available, either click the **Edit virtual machine settings** option, or right-click on the file and select **Edit Settings** from the pop-up menu. A configuration window appears.

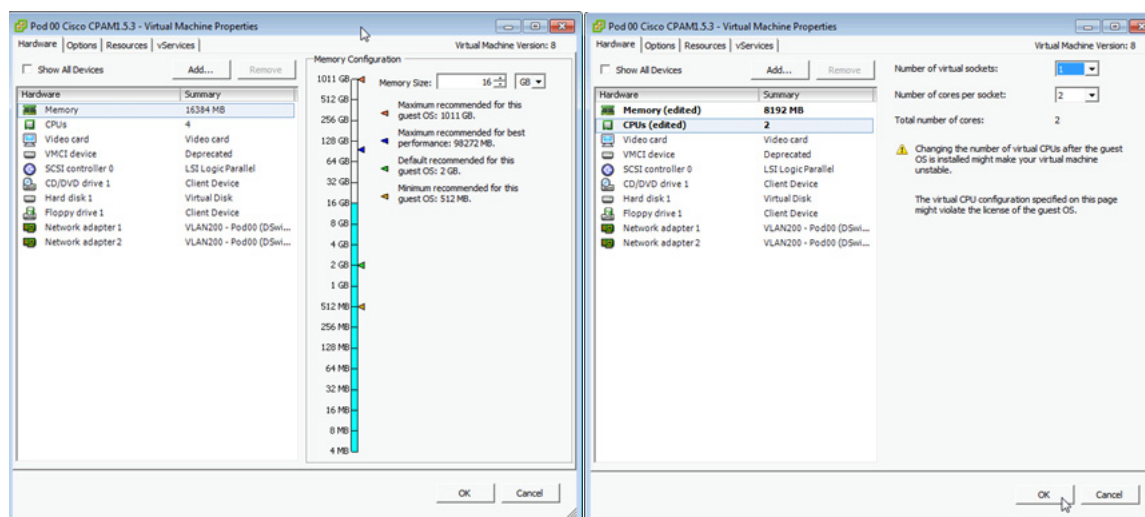


Figure 2: VMware Settings for the ICPAM OVA File

- Edit the virtual machine settings as required. Minimally, the settings should include these values:
  - 16GB of RAM
  - 4 processor cores
 Change any other values required for your system.



## Launching the ICPAM Server Virtual Machine for the First Time

1. Do the following steps for whichever VMware product you are using:

**Hint** Customers often cause themselves problems by closing a virtual machine when it is loading. While the virtual machine is booting, you can press **ESC** to see what files are currently loading. If you think your system is locked up during this process, press **ESC** to verify the system is still loading.

If you need to move your cursor from the Virtual Machine Console window, press the **CTRL** and **ALT** keys at the same time. This releases your mouse.

- For VMware ESXi, launch the VMware vSphere Client using this procedure:
  - Enter the User name and Password (which was established when VMware ESXi was installed on the server), then click **Login**.



Figure 3: VMware vSphere Client Login Dialog

- Click on **VMs and Templates**.
- Locate your virtual appliance in the left window tree and right-click on it.
- Select the **Open Console** option.
- For VMware Workstation (which is supported only for a small testing environment), use this procedure:
  - Select **File > Open > Virtual Machine**.
  - Navigate to the ICPAM virtual machine and select **Open**.

The Red Hat Enterprise Linux console window appears.

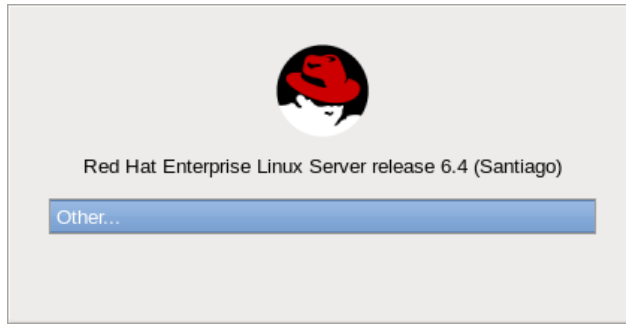


Figure 4: VMware Console Window

- 1. *The ICPAM OVA includes Red Hat Enterprise Linux (RHEL) as its default virtual appliance operating system.*
- 2. Double-click the **Other...** field.
- 3. A prompt appears asking you to provide a username.

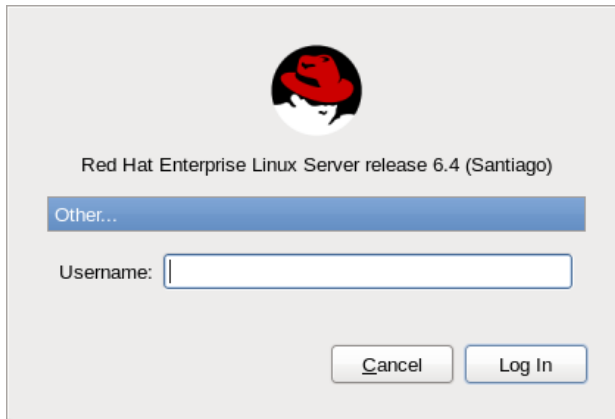


Figure 5: Username Field for VMware Login

- 4. Type this:  
`cpamadmin`  
This is your default username. Now click the **Log In** button.

The password screen appears.

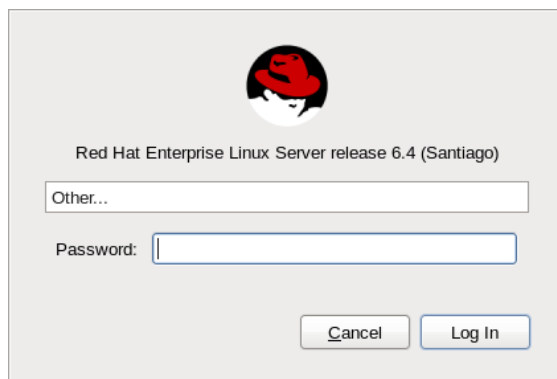


Figure 6: Password Field for VMware Login

5. Enter the default password:  
cpamadmin  
Then click the **Log In** button again.  
The console screen appears.

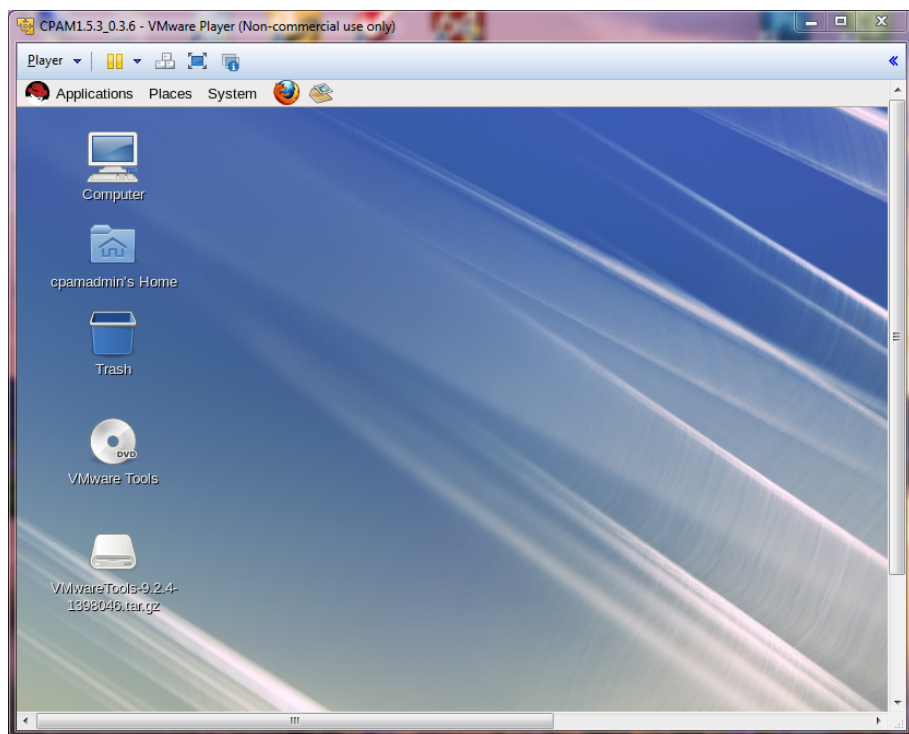


Figure 7: Red Hat Enterprise Linux (RHEL) Console Screen

You are now logged into the ICPAM Server on the virtual machine.

Next, you must obtain Super-User privilege so you can edit the IP Address and other network values for this ICPAM Server.

## Obtaining Super-user Privilege

1. On the Desktop screen, click on **Applications** (in the menu bar near the top of the screen), then select the **System Tools > Terminal** command.  
A command line dialog appears.

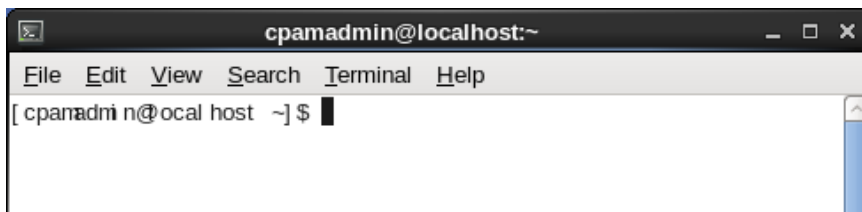


Figure 8: Terminal Command Line Dialog

2. At the command line prompt, type  
`sudo su -`  
Make sure there are spaces between `sudo` and `su` as well as between `su` and the hyphen. Press **Enter**.  
This command enables you to assume administrative privileges, after the proper password is entered. Without administrative privileges, you are not allowed to change configuration settings.  
The dialog displays a prompt for a password, as shown in Figure 9.

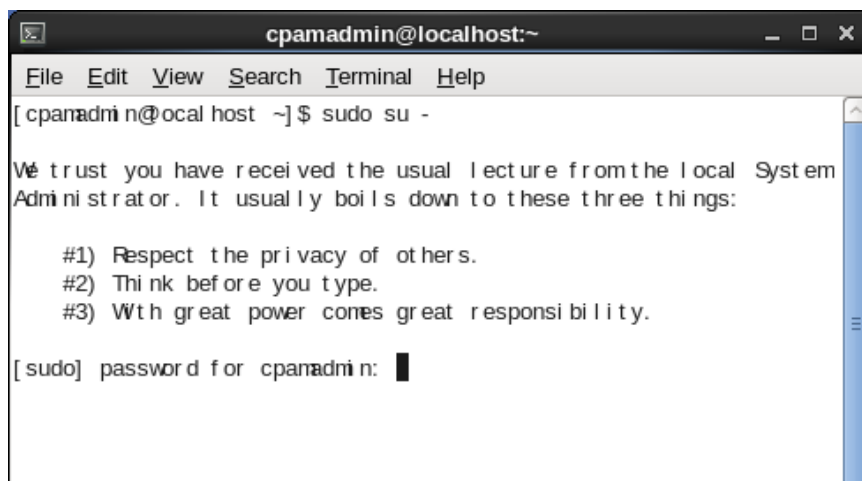
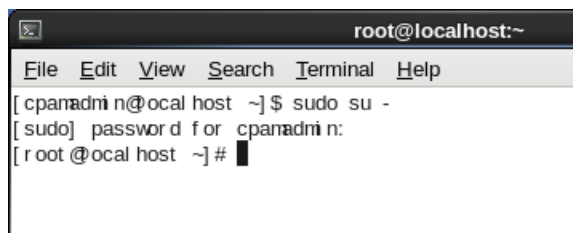


Figure 9: Super-User Permissions Command Line

3. At this command line prompt, type in the password for the super-user account, then press **Enter**.  
At least initially, this password should be the same as the default ICPAM server login password:  
`cpamadmin`

The root authority prompt appears, as shown in Figure 10:




```

root@localhost:~
File Edit View Search Terminal Help
[cpanadmin@ocal host ~]$ sudo su -
[sudo] password for cpanadmin:
[r root@ocal host ~]#

```

Figure 10: Root Authority Prompt Command Line

You now have obtained super-user authority on this system.

 **Make sure to change all default passwords as soon as possible. Select passwords that only you, the system administrator, know.**

## Configuring the ICPAM Server's Network Settings

After you have acquired super-user authority, use it to configure ICPAM in the following way:

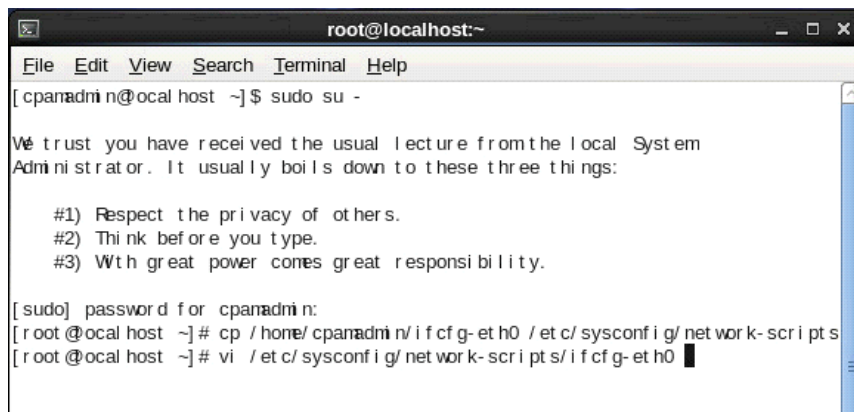
1. At the root prompt, type this command:  

```
cp /home/cpanadmin/ifcfg-eth0 /etc/sysconfig/network-scripts/
```

 where there is a space between `cp` and `/home` and also between `ifcfg-eth0` and `/etc`.
2. Press **Enter**.
3. At the shell, open the `ifcfg-eth0` file using `vi`, by typing this command:  

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

 where there is a space between `vi` and `/etc`
4. Press **Enter** again.



```

root@localhost:~
File Edit View Search Terminal Help
[cpanadmin@ocal host ~]$ sudo su -
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for cpanadmin:
[r root@ocal host ~]# cp /home/cpanadmin/ifcfg-eth0 /etc/sysconfig/network-scripts
[r root@ocal host ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0

```

Figure 11: Root Prompt Commands



This activates Insert Mode, as indicated by **-- INSERT --** at the bottom of the page (Figure 13).

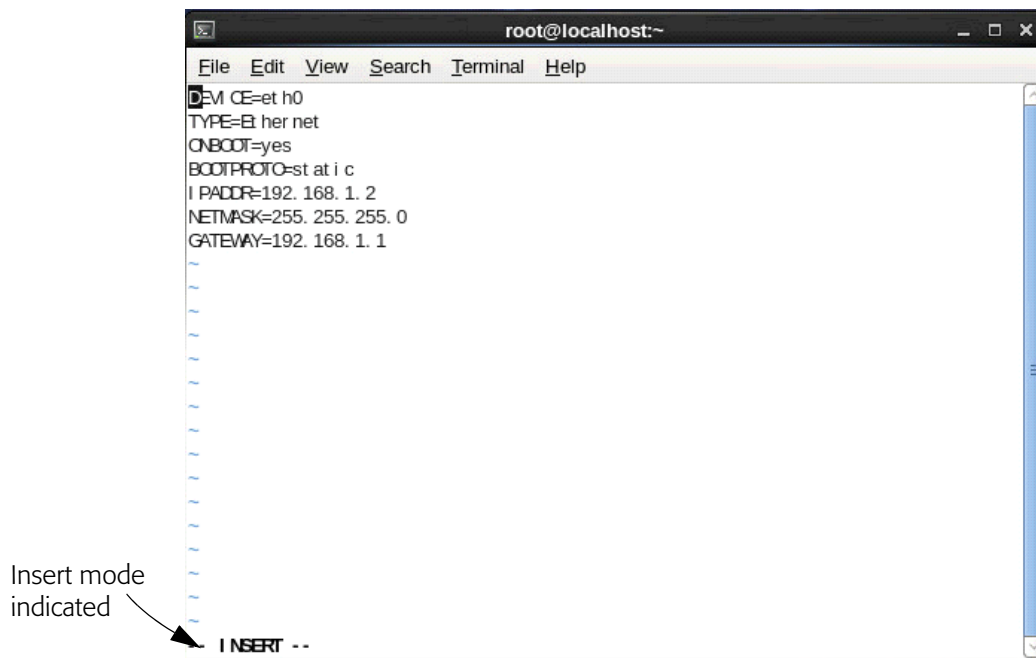



Figure 13: vi Text Editor Insert Mode Indicator

6. Change the IPADDR, NETMASK (if required), and the GATEWAY values for the eth0 configuration file in this way:
  - a. Using the arrow keys, scroll down to the IPADDR line and go to the end of the line. Delete the 192.168.1.2 IP address using the Backspace key, then type the value for your assigned IP address.
  - b. If required, move to the NETMASK field and assign a new value.
  - c. Repeat the process for the GATEWAY line, replacing the default gateway address with the assigned value.
  - d. After you are done making changes, press the **Esc** key. The **-- INSERT --** at the bottom of the window disappears.
-  ***To communicate successfully with both the ICPAM server and client, the static address, subnet mask, and gateway IP address settings must be changed to the appropriate values for your network.***
7. Type:
 

```
:wq
```

 and press **Enter**. This saves your changes to the file and exits the vi text editor. `wq` stands for write quit. Other options are just `w` to write and continue, or `q!` to quit without saving.
8. Back in the Linux shell, restart the network services by typing:
 

```
service network restart
```

 as shown in Figure 14.






10. If this server is being run on a domain, ping the DNS server to ensure the networking changes are working.  
(If there is no domain server associated with the ICPAM server, skip this step.)
  11. Close the VMware terminal window.
- The ICPAM server application is now ready to launch.

## Launching the ICPAM Server Administration Program

To launch the ICPAM Server Administration program:

1. From the VMware shell, press **Ctrl** and **Alt** together.  
The VMware cursor is frozen, and the host computer's cursor is activated.
2. From the host computer's desktop, start your Web browser.
3. At the URL field, enter the IP address chosen for the ICPAM server. For example:  
`https://192.168.1.3`  
then press **Enter**.

 *Depending on which browser you are using, you may get a warning about the SSL certificate not matching the site. In most cases, you can safely ignore this warning and continue.*

The Connected PAM Server Administration login page should appear.



**IDENTIV** [Launch Identiv PAM Client](#) [Download Identiv EDI Studio](#)

**Connected PAM Server Administration**

1.0.0

Username  
cpamadmin

Password  
\*\*\*\*\*

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

Figure 16: ICPAM Server Administration - Login Page

4. Enter the username and password as specified earlier. The default value for both fields is **cpamadmin**.

The ICPAM Server Administration main page appears.

Figure 17: ICPAM Server Administration - Server Page

5. Change the values on the CPAM Administration pages as required.  
For instructions about configuring your ICPAM system, refer to the next section, "Configuring the ICPAM Server Software".

## Configuring the ICPAM Server Software

To configure the ICPAM server software in preparation for installing the client and configuring the appliance hardware, follow these instructions:

1. At the server page of the ICPAM Server Administration screen (shown in Figure 17), enter the required server information.



**You cannot edit or modify the version or serial number.**

- a. At the 'Type' drop-down field, select the appliance server type. The available options are:

**Active Server** (Default) Select this option for a single appliance or if the appliance is the active server in a redundant configuration.

**Standby Server** Select this option if the appliance is the standby (backup) server in a redundant configuration. A standby server must have exactly the same configuration settings as the active server, except for the network addresses, host name, and High Availability (HA) license.

- b. At the 'Site Name' field, enter a description to identify the server on the network. (This field is disabled for a standby server, because the standby server assumes the primary server name if a fail-over occurs.) Enter any combination of letters and numbers up to 32 characters. Spaces are not allowed, but dashes and underscore characters are allowed. For example, Fremont.
- c. Click **Next** to continue.

The User page appears.

Figure 18: ICPAM Server Administration - User Page



*The default username is cpamadmin. This is a read-only super-user username which cannot be changed or deleted. However, you can and should change the default password as soon as possible using the User page. Identiv highly recommends that you create new user names and passwords using ICPAM's Users > Logins feature.*

2. Enter the initial user settings to define the administrator password as well as the email address.
  - a. At the 'Current Password' field, enter the current administrator password. The default password is cpamadmin.
  - b. At the 'New Password' field, enter a new administrator password. The administrator has full rights to any ICPAM-connected appliances and can grant access rights to other users. The new password is required and must be entered to continue.
  - c. At the 'Re-enter Password' field, re-enter the new administrator password to confirm its value.
  - d. At the 'Email Address' field, enter the email address that will receive system messages and 'Forgot Password' e-mails.
  - e. Click **Next** to continue.

The Network page appears.

Figure 19: ICPAM Server Administration - Network Page


3. Enter the network configuration for all ICPAM-connected appliances.
  - a. At the 'Host Name' field, enter the host name of the active server. Enter a different host name for the standby server. The host name is used to identify the appliance on the local network and does not impact other configurations.
  - b. At the 'Shared IP Address' field, enter the same IP address for the active and standby appliance.

 ***This field only applies to HA configurations.***

This address is transferred from the active server to the standby server if a fail-over occurs. The 'Shared IP address' and the Eth0 IP address should be on the same subnet. Eth0 and Eth1 can be on separate subnets.

**Hint** Enter a Shared IP Address if you are planning to install a Standby server in the future, even if you are only installing the Active server now. This allows successful HA backups when the Standby server is installed.

- c. At the 'Transport Port' field, enter the same number for the active and standby appliances. The default port number is **8020**.
- d. At the 'SSL Enable For Server' check box, check the SSL check box to enable or disable secure IP communication between the ICPAM appliance and the controller or gateway. The settings must be the same on the active and standby appliances.

 ***Identiv recommends that SSL always be enabled for all controllers or gateways and the ICPAM appliance. If SSL is disabled for a controller or gateway but enabled for ICPAM, the controller or gateway cannot connect to the appliance. If the SSL settings are changed, reset all controllers or gateways and the ICPAM appliance. For more information see the gateway's Enable SSL option on page 47, or the EM-100 controller's Encrypt Host Communication option on page 60.***

e. At the **Eth0** subpage, 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. The fields on this page include:

- |                    |   |
|--------------------|---|
| <b>IP Address</b>  | 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. |
| <b>Subnet Mask</b> | Enter the subnet mask provided by your system administrator.  |
| <b>Gateway</b>     | (Optional) Enter the Gateway provided by your system administrator.   |

f. If needed, click the **Eth1** subpage tab. This port is disabled by default. You can enable and configure the Eth1 port for remote Internet connections to the ICPAM Server Administration utility. The fields on this page include:

- |                         |  |
|-------------------------|--|
| <b>Enable Interface</b> | Check the check box to enable or disable the Ethernet interface.   |
| <b>DHCP</b>             | Check this check box to enable DHCP. When DHCP is enabled, the IP address fields in this tab are disabled, because the address information is supplied by the DHCP server. |
| <b>IP Address</b>       | Enter the IP address for the Eth0 port. If configured, this address must be different on the active and standby appliances.  |
| <b>Subnet Mask</b>      | Enter the subnet mask provided by your system administrator.   |
| <b>Gateway</b>          | (Optional) Enter the gateway or controller provided by your system administrator. If a gateway/controller is provided for Eth0, leave this field blank.                    |

g. Click **Next** to continue.

The DNS page appears, like the example in Figure 20.

The screenshot shows the 'Initial Setup' page for ICPAM Server Administration. The page title is 'IDENTIV Connected PAM Server Administration'. In the top right corner, there are links for 'Welcome', 'Log Out', 'About', and 'Help'. On the left, a 'Setup Steps' sidebar lists: 1 - Server, 2 - User, 3 - Network, 4 - DNS (highlighted), 5 - Email, 6 - Date & Time, and 7 - Event. The main content area is titled 'Initial Setup' and contains three input fields: 'Primary DNS:' with the value '192.235.84.254', 'Secondary DNS:' with the value '192.235.84.1', and 'Domain:'. Below these fields are three buttons: '< Back', 'Next >', and 'Cancel'. At the bottom of the page, there is a copyright notice: 'Copyright © 2015 Identiv, Inc. | All Rights Reserved.'

Figure 20: ICPAM Server Administration - DNS Page

4. If needed, enter the optional DNS settings for the ICPAM appliance. Enter the same settings for both the active and standby appliance.  
If you don't require DNS settings, click **Next** to skip to the next step.
  - a. At the 'Primary DNS' field, enter the domain name server (DNS) for the active ICPAM appliance.
  - b. At the 'Secondary DNS' field, enter the domain name server for the standby ICPAM appliance.
  - c. At the 'Domain' field, enter the domain name for the ICPAM appliance.
  - d. Click **Next** to continue.

The Email page appears, like the example shown in Figure 21.

The screenshot shows the 'Initial Setup' page for ICPAM Server Administration, specifically the 'Email' configuration step. The page title is 'IDENTIV Connected PAM Server Administration'. In the top right corner, there are links for 'Welcome', 'Log Out', 'About', and 'Help'. On the left, a 'Setup Steps' sidebar lists: 1 - Server, 2 - User, 3 - Network, 4 - DNS, 5 - Email (highlighted), 6 - Date & Time, 7 - Event, and 8 - License. The main content area is titled 'Initial Setup' and contains two input fields: 'SMTP Server Address:' and 'SMTP Email Address from:'. Below these fields is a 'Test' button. At the bottom of the page, there are three buttons: '< Back', 'Next >', and 'Cancel'. At the bottom of the page, there is a copyright notice: 'Copyright © 2015 Identiv, Inc. | All Rights Reserved.'

Figure 21: ICPAM Server Administration - Email6 Page

5. Enter the email settings used to send messages from the ICPAM appliance. Enter the same settings for both the active and standby appliance.
  - a. At the 'SMTP Server Address' field, enter the SMTP server address used to send outgoing messages. Outgoing messages include event and other alarm information.
  - b. At the 'SMTP Email Address from' field, 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. 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. Click **Next** to continue.

The Date & Time page appears, like the example in Figure 22.

The screenshot shows the 'Initial Setup' page for 'ENTIV Connected PAM Server Administration'. The 'Date & Time' section is active, displaying the following configuration:

- Date & Time: 06/16/15 09:21:39
- Time Zone: America/Los\_Angeles
- NTP Enable:
- NTP Server Address\*: 0.north-america.pool.ntp.org

Navigation buttons include '< Back', 'Next >', and 'Cancel'. The footer indicates 'Copyright © 2015 Identiv, Inc. | All Rights Reserved.'

Figure 22: ICPAM Server Administration - Date & Time Page

6. Enter the date and time settings. Enter an initial date and time for the server. These settings are used by the appliance and the gateways/controllers. Enter the same settings for both the active and standby appliance.
  - a. At the 'Date & Time' field, 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.
  - b. At the 'Time Zone' field, select the time zone where the appliance is installed.
  - c. At the 'NTP enable' check box, check the box to use a Network Time Protocol (NTP) server that will automatically adjust the date and time.
  - d. If NTP is enabled, at the 'NTP Server Address' field, enter the IP address of the NTP server.
  - e. Click **Next** to continue.

The Event page appears, like the example in Figure 23, with the Pruning subpage automatically displayed.

The screenshot shows the 'Initial Setup' page for ICPAM Server Administration. On the left, a 'Setup Steps' sidebar lists steps 1 through 8, with '7 - Event' highlighted. The main content area is titled 'Initial Setup' and contains two tabs: 'Pruning' (selected) and 'Archive'. Under the 'Pruning' tab, there are several configuration fields: 'Live Event Window(days):' with a text input containing '30'; 'Schedule:' with three radio buttons for 'Date:', 'Weekday:', and 'Daily:' (the 'Daily:' option is selected); 'Time:' with a text input containing '00:00:00' and a '(hh:mm:ss)' label; and 'Pruning Hours:' with a dropdown menu showing '1.0'. At the bottom of the form are three buttons: '< Back', 'Finish >', and 'Cancel'. The footer of the page reads 'Copyright © 2015 Identiv, Inc. All Rights Reserved.'

Figure 23: ICPAM Server Administration - Event Page (Pruning Subpage)

7. Enter the event pruning and archiving settings as required.
  - Pruned Events are removed from the main events database table and placed in a separate historic events database table. This enables 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 and 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.
- a. At the Pruning subpage, enter the following settings:

**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. 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 number is rounded to midnight of the last day.



**Schedule**

Define the time and frequency at which events should be pruned.

These radio buttons are available:

**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**.

For other options in **Schedule**, the **Pruning Hours** field is read-only.

**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 when you select **Daily** from the 'Schedule' field.

The default value is 1.



*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.*

b. Click the **Archive** tab, so the Archive subpage appears.

Figure 24: ICPAM Server Administration - Event Page (Archive Subpage)

**Hint** The archive settings are required during the initial setup. After a successful restore, you can disable auto-archiving if necessary. For more information, see Chapter 3, "Archiving Historical Events" in the **ICPAM User Guide**.

Supply values for the following fields as required.

|                                      |   |
|--------------------------------------|---|
| <b>Password</b>                      | Enter and re-enter the administrator Password. This password is used to restore the archive file (similar to backup files).   |
| <b>Re-enter Password</b>             |   |
|                                      | <i>Note: Do NOT use special characters for this password. Only alphanumeric (0-9, a-z, A-Z) characters are allowed.</i>   |
| <b>Historic Events Window (days)</b> | 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.<br><br>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).  |
| <b>Schedule</b>                      | 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).<br><br>Date—To schedule archiving for one day per month, select Date and then select a day of the month. For example: <b>15</b> .<br><br>Weekday—To schedule archiving once per week, select Weekday and then select a day of the week. For example: Tuesday.<br><br>Daily—To run archiving every day, select <b>Daily</b> .<br><br>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. |
| <b>Copy to remote server</b>         | Check this box to automatically copy the archived event files to a remote FTP or SFTP location.<br><br><i>Note: Only the three most recent archive files are saved. If you do not save the archive file manually or copy it to a remote server, then the oldest file will be permanently deleted when the fourth file is created.</i>   |
| <b>FTP</b>                           | Select this radio button to indicate that the remote server uses standard File Transfer Protocol.   |
| <b>SFTP</b>                          | Select this radio button to indicate that the remote server uses Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).  |
| <b>Address</b>                       | Enter the IP address or hostname of the remote server.  |
| <b>Username</b>                      | Enter the username required to log into the server.   |
| <b>Password</b>                      | Enter the login password for the remote server.   |
| <b>Path</b>                          | Enter the directory path where the compressed archive will be copied. The path must exist on the remote server, or the archive will fail.   |

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

**Hint** To avoid collisions, the Pruning and Archiving schedules should not occur during the same time period.

If this is the first time this screen was configured, the License page appears.

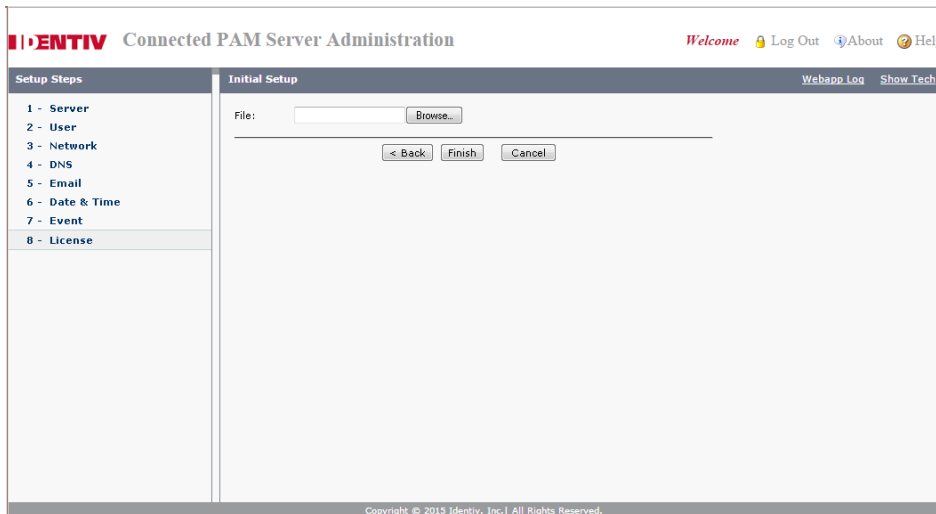




Figure 25: ICPAM Server Administration - License Page

- If you have a one-server system with the Enterprise Data Integration (EDI) option, the EDI license needs to be installed on that server.
  - If you have a two-server system with the High Availability (HA) option, the HA license only needs to be installed on the Standby Server. If your two-server system also has the Enterprise Data Integration (EDI) option, the EDI license only needs to be installed on the Active Server.
8. Enter the license settings to obtain and install the software license:
    - a. Save the file to the PC used to configure the ICPAM appliance.
    - b. In the License screen of Initial setup, click **Browse** to select the license file located on your local drive. The selected filename appears in the File field.
    - c. Click **Finish** to install the license file on the ICPAM appliance and activate the included features.
-  ***You can only add one license file in the setup. If you have other licenses, they can be added later on the license subpage of the server administration window.***
9. Wait for the installation to complete. A status screen displays each configuration item as it is applied. When all items are marked Done, the ICPAM Server Administration utility's Status page is displayed.
-  ***If any errors occur, the setup returns to Step 1. If a serious error occurs, contact your Identiv support representative for assistance.***

10. Create a system backup. You should have at least one backup file to preserve critical system data and to restore the appliance software using the recovery CD.
  - a. Select **Setup** and then **Backup**.
  - b. Select the **Manual** tab.

Manual backups are enabled only if automatic backups are disabled.
  - c. 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.
  - d. If required, check the **Exclude Events** box to exclude events from the backup. When this option is checked, events will not be backed up and cannot be restored.
  - e. If required, select the **Copy to remote server** check box to automatically copy the backup to a remote server. Select the server type and enter the server address, username, password, and directory path where the files will be copied.
  - f. Click **Backup Now** to begin the backup process and create a new .zip backup file. This takes some time, particularly if the database is large.

When the backup is complete, the new backup file is added to the top of the screen. The file name includes the date and the server software version number. For example:

    - bak-04122016-0933561.5.3\_0.3.6.cpam.noevents.zip is the name of a no-events backup file created 4/12/2016 on a CPAM 1.5.3 system
    - bak-05242016-1452592.2.0\_0.3.8.ICPAM220.zip is the name of a full backup file created 5/24/2016 on an ICPAM 2.2.0 system
  - g. To save the file to another location, right-click the filename and click the **Save** option from the browser menu.
11. Disconnect your PC from the Eth0 port and connect the Eth0 port to the IP network.

## Installing the Necessary Version of the Java Runtime Environment and the ICPAM Client

This topic describes how to install version 2.2 of the ICPAM Client software with support for the EM-100 controller, and the necessary version of the Java Runtime Environment.

1. On the workstation that you intend to use as a ICPAM client, open the Windows Control Panel, and under Add or Remove Programs check to see which versions of Java are currently installed. If versions of Java other than 1.7 (32-bit) are installed, remove them.
2. Open a Web browser.
3. At the URL field, enter the IP address chosen for the ICPAM server, in this manner:  
`https://192.168.1.3`  
then press **Enter**.

The Connected PAM Server Administration login page appears, as shown in Figure 26.



Figure 26: ICPAM Server Administration Login Page - with Link to Launch ICPAM Client

4. Login with the **cpamadmin** username and the new password, then click **Log In**. The ICPAM Server Administration page appears.
5. Click the **Downloads** tab in the ribbon bar.

The Downloads page appears.

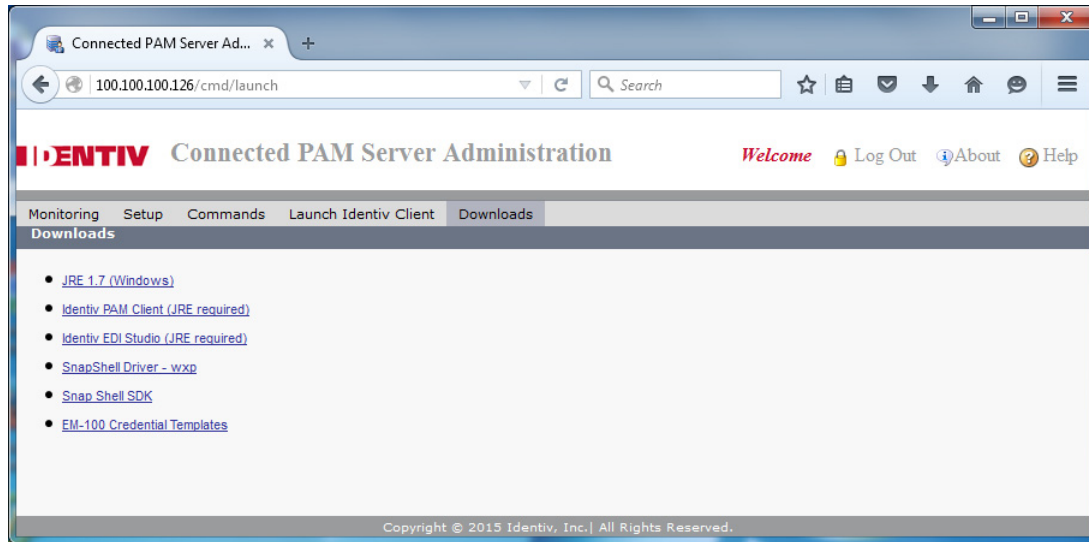


Figure 27: ICPAM Server Administration - Downloads Page

6. Click on the **JRE 1.7 (Windows)** link.  
The Java download page will appear. Do the following:
  - a. At the Java SE Runtime Environment 7u79 table, click the **Accept License Agreement** radio button.
  - b. Select the JRE 1.7 32-bit version **Windows x86 Offline** download executable.
  - c. Follow the instructions to download the executable file.
7. Click the **Run** button on the download pop-up.
8. Click the **Install** button.
9. Follow the wizard to finish the Java installation.
10. When you are finished, click **Finish**.
11. Return to the Downloads page on the browser and click on the **Identiv PAM Client (JRE required)** link.  
There are two other ways to launch the ICPAM client:
  - Click the **Launch Identiv PAM Client** from the ribbon bar, as shown in Figure 27.
  - Return to the server Login page (Figure 26) and select the **Launch Identiv PAM Client** link in the upper right. (This method does not require logging in before launching.)
12. Click the **Open** or **Run** button on the download pop-up.

The Welcome page appears.



Figure 28: ICPAM Client Installation - Welcome Page

13. Click **Next**.

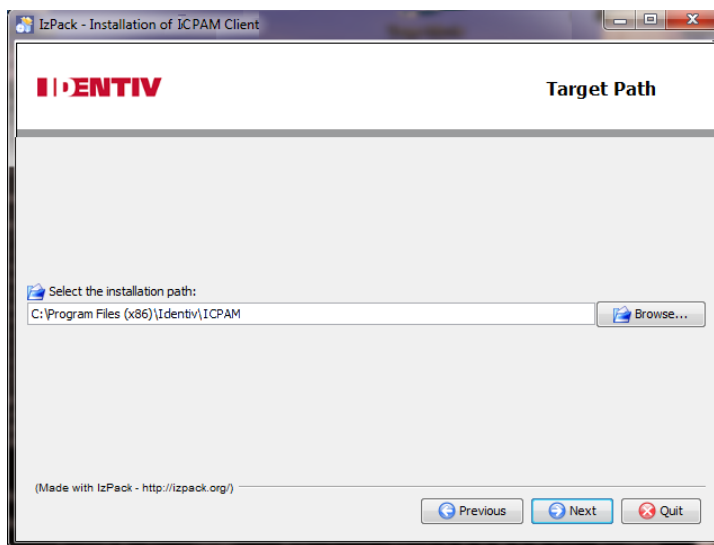


Figure 29: ICPAM Client Installation - Target Path Page


14. Either accept the default path of C:\Program Files (x86)\Identiv\ICPAM, or enter a custom path, then click **Next**.

If you chose the default path and the installer displays an error message stating that you do not have the necessary permissions to install there, then browse to the C:\Users directory and choose it as the target path for the ICPAM Client installation.

15. Click **Yes**.

16. Click **Next**.

- Click the **Create additional short cuts on the desktop** option, then click **Next** again.

 *If you get a message about the process being blocked by a firewall, allow it.*

The Installation page appears, and displays progress information.

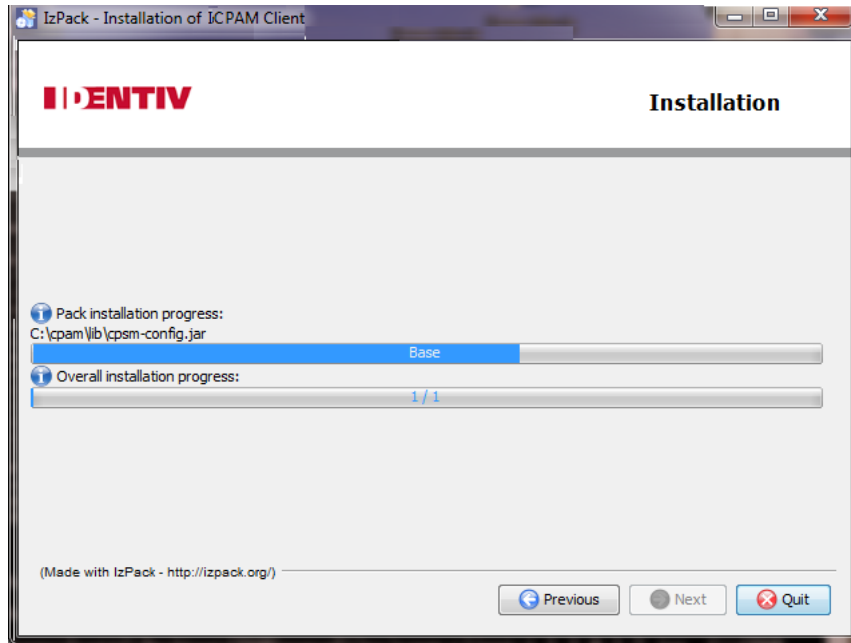


Figure 30: ICPAM Client Installation - Installation page

- Click **Next** after that button is enabled.

The Log In dialog appears:

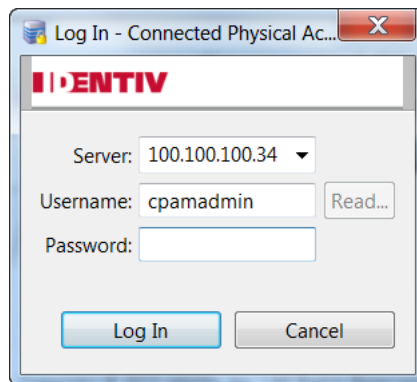


Figure 31: Log In Dialog for the ICPAM Client

- Enter the initial password of **cpamadmin**, then click **Log In**.



The Welcome page of the ICPAM client appears, as shown in Figure 32.

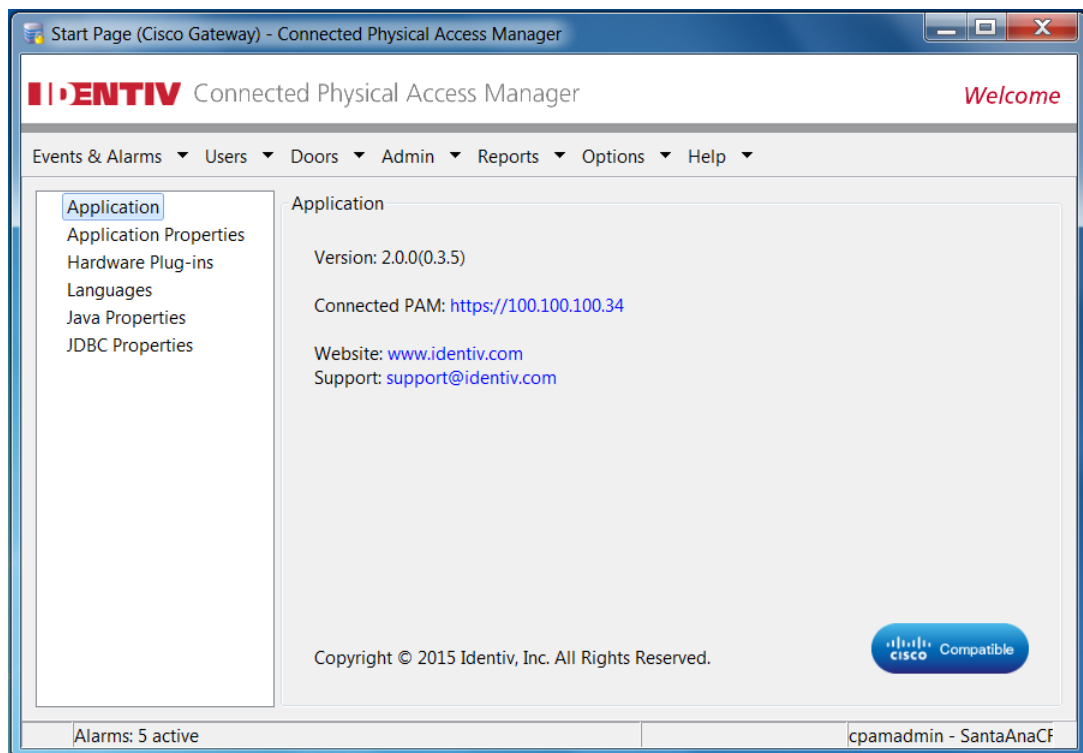


Figure 32: Welcome Page of the ICPAM Client

For instructions on configuring and running the ICPAM system through an ICPAM client, refer to the **ICPAM User Guide**.

## Upgrading a High Availability Pair of ICPAM Servers

If your ICPAM security system includes the optional High Availability feature (which provides automatic fail-over to a standby server), perform the following general procedure when upgrading the system software.

1. Check the Release Notes for any specific instructions about upgrading.
2. As a precautionary measure, use VMware to take snapshots of both the Active Server and the Standby Server.
3. Log in to the ICPAM Server Administration Utility on the Active Server, and use the **Setup > Backup** command to create a backup of the ICPAM database.
4. Store the backup file offline, in case you need to use it later to restore the ICPAM Active Server.
5. Download the .bin file for the upgraded ICPAM software, and have it available on your laptop.
6. Log in to the ICPAM Server Administration Utility on the Standby Server, and use the **Commands > Stop Server** command to stop the ICPAM Standby Server.
7. Switch to the ICPAM Server Administration Utility on the Active Server, and use the **Commands > Stop Server** command to stop the ICPAM Active Server.
8. Use the **Setup > Upgrade** command to upgrade the ICPAM server software on the ICPAM Standby Server.  
(After the upgrade has finished, leave the Standby Server in the stopped state.)
9. Switch to the ICPAM Server Administration Utility on the Active Server, and use the **Setup > Upgrade** command to upgrade the ICPAM server software on the ICPAM Active Server.
10. Use the **Commands > Start Server** command to restart the ICPAM Active Server.
11. After the Active Server has restarted, log in to it using the ICPAM Desktop Client, and verify that the door controllers (Gateways or EM-100 Controllers) are online.
12. Switch to the ICPAM Server Administration Utility on the Standby Server, and use the **Commands > Start Server** command to restart the ICPAM Standby Server.

After restarting, the ICPAM Standby Server should start synchronizing with the ICPAM database on the Active Server on the Active Server, and remain in the standby state.

If you encounter a problem while performing this procedure, you can use the backup of the ICPAM database and the VMware snapshots of the servers to restore your ICPAM security system to its previous working state.

## Installing and Configuring Door Controllers

ICPAM currently uses two types of door controllers to communicate between the ICPAM system and connected access devices:

- Cisco Physical Access Gateways (page 35)
- Identiv EM-100 Controllers (page 48)

The installation and configuration of both types of door controllers are explained in the remainder of this document.

### Cisco Physical Access Gateways

NOTE: Cisco's Physical Access Gateway is no longer being manufactured or sold.

#### Overview of a Gateway

The Cisco Physical Access Gateway (shown in Figure 33) is installed near each door to provide access control and connections for card readers, door locks, and other input and output devices. The Gateway is connected to ICPAM using an Ethernet connection to the IP network. Power is supplied either through a Power over Ethernet (PoE) connection, or using a DC power source. Each Gateway includes connections for up to two Wiegand door readers, three input devices, and three output devices.



Figure 33: Cisco Physical Access Gateway

The physical dimensions of the gateway are:

5 W x 7 H x 2.14 D in. (127 x 178 x 54.6 mm)

The most important elements of this gateway are shown in Figure 34.

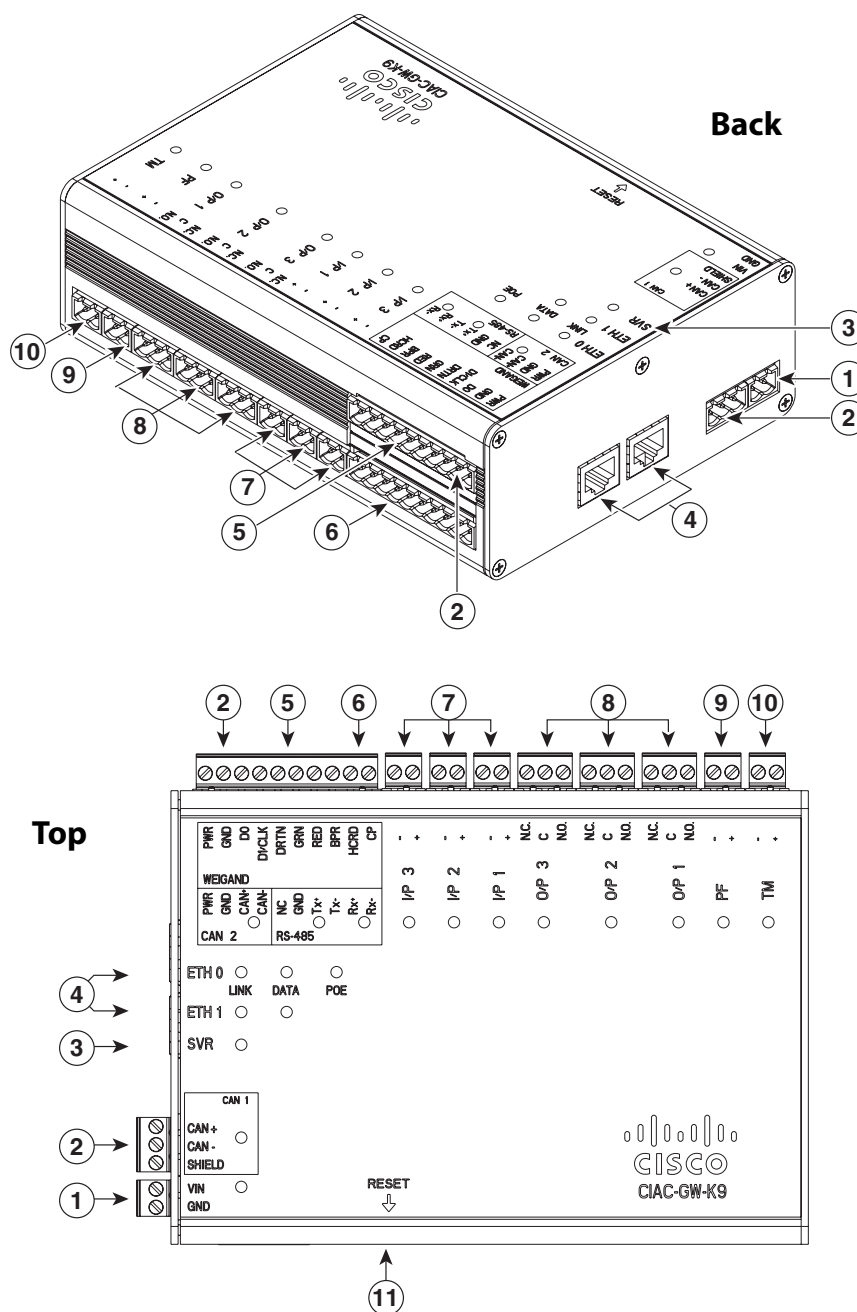


Figure 34: Cisco Physical Access Gateway - Back and Top Views (with Labels)

The numbered elements of Figure 34 are described below.

|          |   |
|----------|---|
| <b>1</b> | <p>Power – Two-pin connector for Voltage In (VIN) and Ground (GND) to connect a 12 to 24 VDC external power source.</p>   |
| <b>2</b> | <p>CAN – A three-wire CAN bus used to connect additional modules, such as the Cisco Reader Module, Cisco Input Module, and Cisco Output Module.</p> <p><i>Note: Modules for the Gateway using this CAN bus are not currently supported in ICPAM.</i></p>  |
| <b>3</b> | <p>SVR (Server) – When this LED is steady green, the Gateway is connected to an ICPAM server.</p>   |
| <b>4</b> | <p>Fast Ethernet interface – There are two 10/100 BASE-TX RJ-45 connectors:</p> <ul style="list-style-type: none"> <li>• <b>ETH 0</b>: connects the Gateway to the network. ETH 0 also supports Power over Ethernet (PoE) for the device (optional).</li> <li>• <b>ETH 1</b>: connects the Gateway to a PC to access the device configuration Web page.</li> </ul>  |
| <b>5</b> | <p>Serial interface – The Gateway's RS-485 interface is not supported in this release of ICPAM.</p>   |
| <b>6</b> | <p>Wiegand interface – This interface can be configured as the following:</p> <ul style="list-style-type: none"> <li>• One 10-pin Wiegand/clock and data reader interface to connect a single door reader.</li> <li>• Two 5-pin Wiegand/clock and data interfaces to connect two door readers (for installations where a 5-pin interface is sufficient).</li> </ul> <p><i>Note: Disconnect power from the Gateway or Reader module before connecting reader devices to the modules. Connecting a reader device when the modules are powered can cause the Gateway or Reader module to malfunction.</i></p>  |
| <b>7</b> | <p>Input interfaces – Three input interfaces used to sense the contact closure. Each input can be configured as either supervised or unsupervised, and can be configured to sense either a Normally Open (N.O.) or a Normally Closed (N.C.) contact.</p> <ul style="list-style-type: none"> <li>• An unsupervised input senses a simple contact closure state, including Normal or Alarm. When connected to open contacts, the terminal voltage range is 4V to 5V. For closed contacts, the voltage range is 0V to 0.7V.</li> <li>• A supervised input senses four contact states, including Normal, Alarm, Open, and Short. These inputs require 1K End-Of-Line (EOL) termination resistors installed at the contacts (two resistors are included in the accessory kits for each Input port).</li> </ul> |

|           |  |
|-----------|--|
| <b>8</b>  | <p>Output Interfaces – Three Form C (5A @ 30V) relay output interfaces. Each output connection can be configured as either Normally Closed (N.C.) or Normally Open (N.O.).</p> <p>Common (C) &amp; N.O. connection: The relay is normally open. The circuit is closed when triggered.</p> <p>Common (C) &amp; N.C. connection: The relay is normally closed. The circuit is opened when triggered.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>• Install surge protection between the output device and the ICPAM module. For details, see <b>Installing Surge Suppressors on Output Device Connections</b> in the <b>Cisco Physical Access Gateway User Guide</b>.</li><li>• Common (C) is always used, and either N.C. or N.O. is used to complete the connection.</li><li>• All Generic Output devices installed in CPAM systems prior to release 1.1.0 were connected to the Gateway, Reader, or Output modules with the wiring reversed. If upgrading to ICPAM from an earlier release of CPAM, disconnect all Generic Output devices and do the following:<ul style="list-style-type: none"><li>- Connect Normally Open devices to the N.O. and C connectors on the Gateway, Reader, or Output module.</li><li>- Connect Normally Closed devices to the N.C. and C connectors on the Gateway, Reader, or Output module.</li></ul></li></ul> |
| <b>9</b>  | <p>PF – Power fail input: an unsupervised input that raises a “power fail” alarm when the circuit is open. Can be configured as an additional unsupervised input which indicates only Normal or Alarm. The corresponding LED is red when the circuit is open (when no input is connected).</p>   |
| <b>10</b> | <p>TM – Tamper input: an unsupervised input that raises a “tamper” alarm when the circuit is open. Can be configured as an additional unsupervised input which indicates only Normal or Alarm. The corresponding LED is red when the circuit is open (when no input is connected).</p>   |
| <b>11</b> | <p>Reset – Resets the device.</p>  |

## Installing a Gateway

1. Unpack and mount the Cisco Physical Access Gateway, which includes:
  - Six End-Of-Line (EOL) 1K termination resistors (for supervised inputs)
  - Two mounting brackets with 4 screws for each bracket
  - Regulatory compliance and safety information
  - Quick Start guide
  - Connector plugs:

| Type   | Quantity |
|--------|----------|
| 10-Pin | 1        |
| 3-Pin  | 4        |
| 2-Pin  | 6        |

Three types of wall mounting can be used for mounting gateways or optional modules using the included brackets.

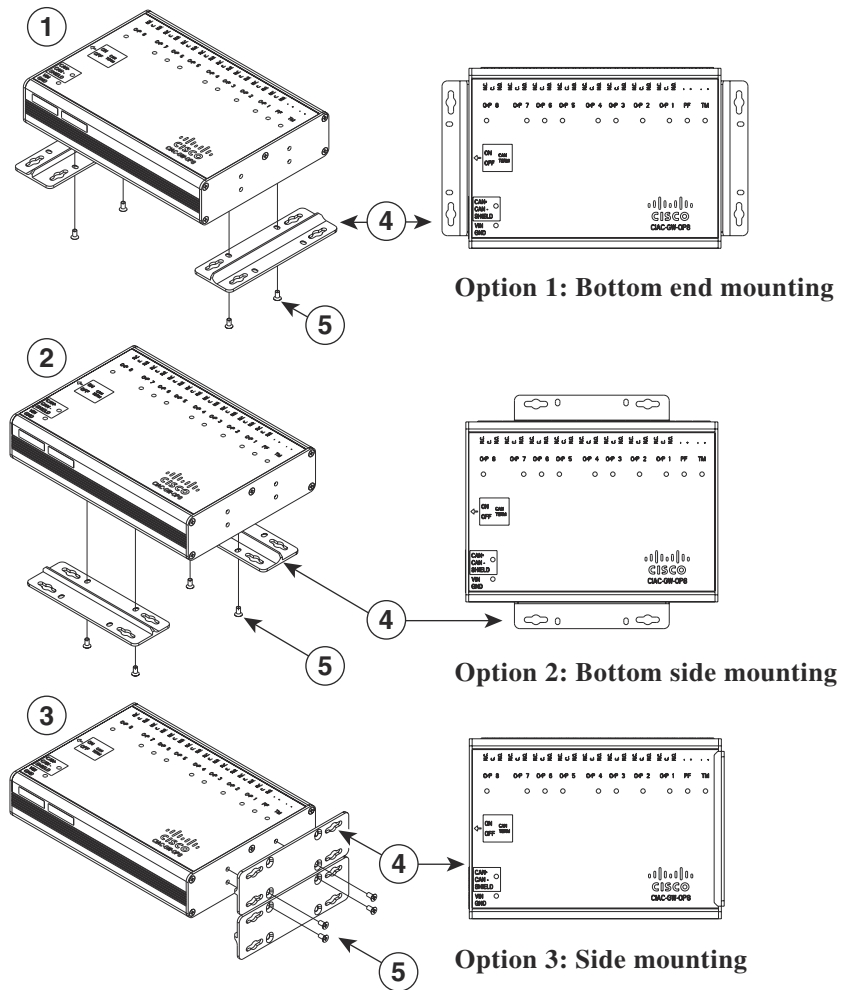


Figure 35: Three Options for Installing a Gateway's Wall Brackets

The physical dimensions of the gateway are:

5 H x 7 W x 2.14 D in. (127 x 178 x 54.6 mm)

2. Unpack and mount optional reader, input, or output modules, if necessary.
3. Connect door readers, input, and output devices to the Cisco Gateway or optional modules.
4. Connect the Cisco Gateway to a power source, using the connections shown in Figure 36.

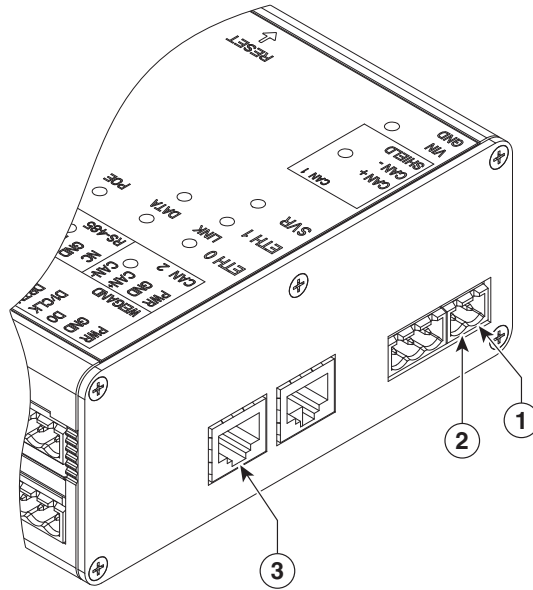


Figure 36: Gateway Power Connections

|          |  |
|----------|--|
| <b>1</b> | DC power / GND (ground) – Connects the DC ground wire to the Gateway.  |
| <b>2</b> | DC power / Voltage In (VIN) – Connects the DC Voltage In (VIN) wire to the Gateway.  |
| <b>3</b> | ETH0 for PoE – Connects the Ethernet cable from the Access Layer switch to the Gateway. To use this power option, the switch must support PoE. |

- If using a DC power source, insert a two-pin connector plug into the DC power port (Figure 36), and connect the Voltage In (VIN) and ground (GND) wires.
- If using PoE, connect an Ethernet cable from the IP network to the ETH0 port.



The power requirements for the various modules are shown in the following table.

| Module                        | Current Draw Requirement | Notes   |
|-------------------------------|--------------------------|---|
| Cisco Physical Access Gateway | 1.5A                     | 1.5A is required for the Gateway module only. Add an additional 1A if a reader or lock is attached to the module. |
| Cisco Reader Module           | 1A                       | 1A is required for the Reader module only. Add an additional 1A if a reader or lock is attached to the module.    |
| Cisco Input Module            | 1A                       | N/A   |
| Cisco Output Module           | 1A                       | N/A   |

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



***To enter the Gateway's initial configuration, be sure to connect your PC to the ETH1 port. The ETH0 port is used for network communication.***

6. Connect one or two door reader devices to the Wiegand interface, using one of the following configurations:
  - Connect a single door reader using all 10 Wiegand interface pins.
  - Connect one or two door readers using 5-pin Wiegand interface connections (for installations where a 5-pin interface is sufficient).

Figure 37 shows the location of the Wiegand interface connections.

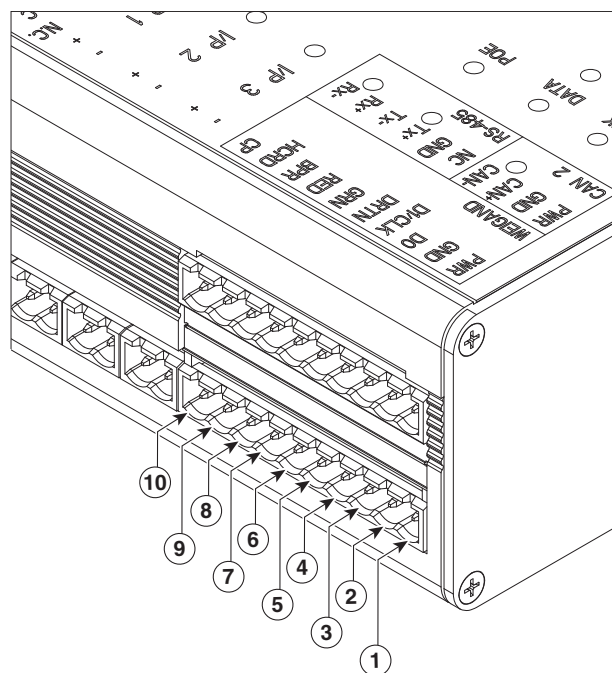


Figure 37: Wiegand Interface Connections on Gateway and Reader Modules

The following table describes the wiring connections for 10-pin and 5-pin Wiegand reader interface connections. The wire connectors from the reader device are shown in parentheses. When attaching a second reader, use the alternative connections shown in the column on the far right.

|    | <b>Chassis Label</b> | <b>Description</b> | <b>1 Reader 10-wire Connection</b> | <b>First Reader 5-wire Connection</b> | <b>Second Reader 5-wire Connection</b> |
|----|----------------------|--------------------|------------------------------------|---------------------------------------|--|
| 1  | PWR                  | +12V               | PWR (red)                          | PWR (red)                             | PWR (red)                              |
| 2  | GND                  | Ground             | GND (black)                        | GND (black)                           | GND (black)                            |
| 3  | D0                   | Data 0             | D0 (green)                         | D0 (green)                            |  |
| 4  | D1/CLK               | Data 1             | D1/CLK (white)                     | D1/CLK (white)                        |  |
| 5  | DRTN                 | Shield             | DRTN (shield)                      | DRTN (shield)                         | DRTN (shield)                          |
| 6  | GRN                  | Output             | GRN (orange)                       | GRN (orange)                          |  |
| 7  | RED                  | Output             | RED (brown)                        | ---                                   | GRN (orange)                           |
| 8  | BPR                  | Output (Beeper)    | BPR (yellow)                       | ---                                   | ---                                    |
| 9  | HRCDD                | Hold Control       | HCRD (blue)                        | ---                                   | D1/CLK (white)                         |
| 10 | CP                   | Card Present       | CP (purple)                        | ---                                   | D0 (green)                             |

7. Connect input devices to the gateway.
  - a. Insert two-pin connector plugs into the input ports (see Figure 39).
  - b. (Optional, for supervised input connections only). Install two End-Of-Line (EOL) 1K termination resistors in each supervised input interface (one terminator in each connector). Figure 38 shows the terminator installation for a Normally Closed (N.C.) and Normally Open (N.O.) input connection.

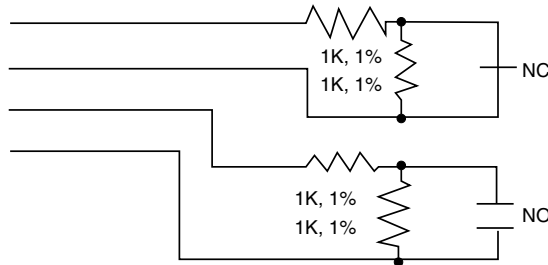


Figure 38: Wiring of Termination Resistors for Supervised Input Connections

- c. Connect the wires from the input devices (see Figure 39).

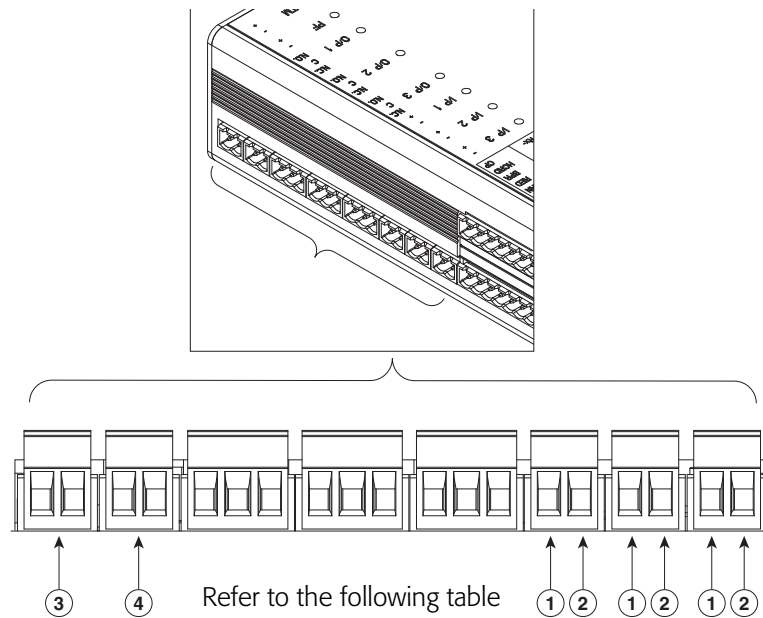



Figure 39: Input Connections on the Cisco Physical Access Gateway

- 1 Positive Input Connections—Positive connection to an Input device.
- 2 Ground Input Connections—Ground connection to an Input device.
- 3 TM—Tamper input: an unsupervised input that raises a “tamper” alarm when the circuit is open. Can be configured as a general unsupervised input which indicates only Normal or Alarm. The corresponding LED is red when the circuit is open (when no input is connected).
- 4 PF—Power fail input: an unsupervised input that raises a “power fail” alarm when the circuit is open. Can be configured as an additional unsupervised input which indicates only Normal or Alarm. The corresponding LED is red when the circuit is open (when no input is connected).

 ***Each of the dedicated input connections can be configured as either supervised or unsupervised. The tamper and power fail inputs can be configured as additional unsupervised ports. A supervised input supports four states: Normal, Alarm, Open, and Short. An unsupervised input indicates only Normal or Alarm.***

8. Connect output devices to the gateway (see Figure 40 on page 45). Each of the three Form C (5A @ 30V) relay output connections can be configured as either Normally Closed (N.C.) or Normally Open (N.O.).
  - a. Insert three-pin connector plugs into the output ports.
  - b. Connect the wires from the output devices in accordance with these three rules:
    - Common (C) is always used, and either N.C. or N.O. is used to complete the connection.
    - If the relay is normally open, use the C & N.O. connections. The circuit is closed when triggered.
    - If the relay is normally closed, use the C & N.C. connections. The circuit is opened when triggered.

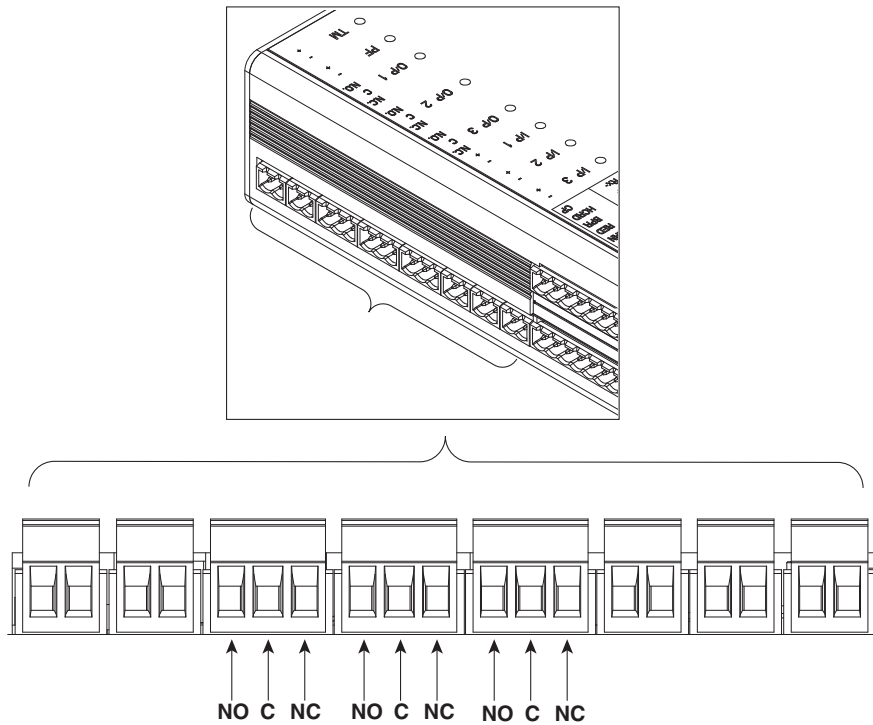


Figure 40: Output Connections on the Cisco Physical Access Gateway

9. Connect the Gateway to the IP network by connecting an Ethernet cable to the ETH0 port, as shown in Figure 41.

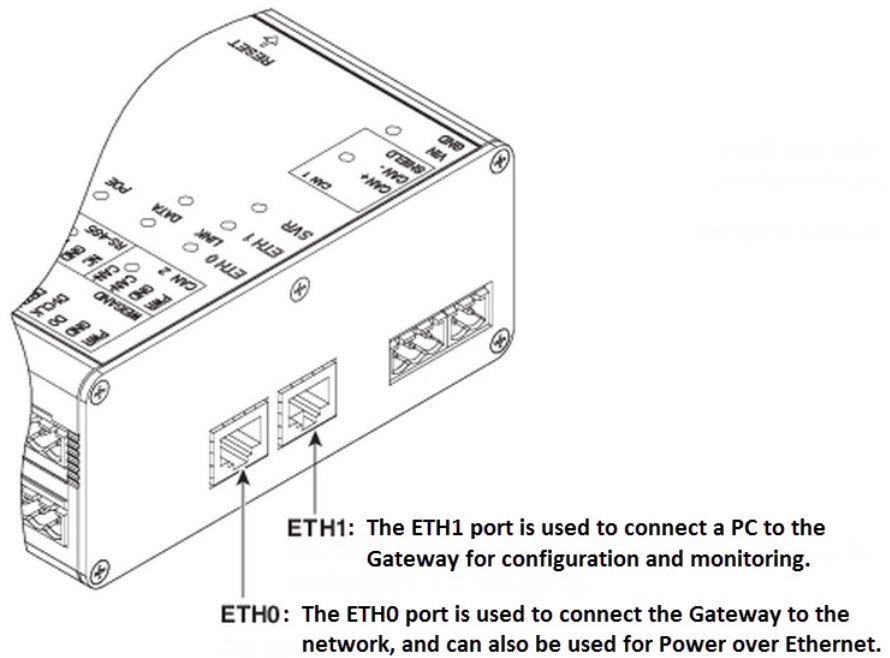


Figure 41: ETH 0 (and ETH1) Ethernet Connections on the Cisco Physical Access Gateway

The ETH1 connector is used to perform configuration by connecting a PC to the Gateway. ETH0 is commonly used for connecting the gateway to the network after it has been configured or when employing PoE.

10. Continue to the next topic about “Configuring a Gateway”.

## Configuring a Gateway

After the Gateway has been wired to its attached devices and mounted in an appropriate location, you must configure the Gateway so that ICPAM can discover and use it.

1. Connect an Ethernet cable from a PC to the ETH1 interface on the Gateway module, as shown in Figure 41.
2. Open a Web browser on the attached PC and enter **https://192.168.1.42**. This URL opens the Web-based configuration page.
3. On the Login page, enter the default username and password, then click the Log In button.  
default username: gwadmin  
default password: gwadmin
4. The Network Setup page appears, as shown in Figure 42.

The screenshot displays the Cisco Access Control Gateway Network Setup page. The page title is "Cisco Access Control Gateway" with a "Welcome" message and links for "Log Out", "About", and "Help". The main navigation bar includes "Network Setup", "Image Management", "User Management", and "Show Inventory". The "Network Setup" section is active, showing three configuration panels: "Eth0 Configuration" with a checked "DHCP" box and input fields for "IP Address", "Subnet Mask", and "Default Gateway"; "DNS Configuration" with a "DNS Server" input field; and "Cisco PAM Configuration" with input fields for "Address" and "Port" (set to 8020) and a checked "Enable SSL" box. At the bottom, there are buttons for "Save", "Cancel", "Reset Application", "Reboot", "Reset Factory Defaults", "Delete Events", "Delete Configuration", and "Delete Credentials". A copyright notice "© 2008-2012 Cisco Systems, Inc. All Rights Reserved." is visible at the very bottom.

Figure 42: Configuring the Cisco Access Control Gateway - Network Setup Page

5. Enter the ETH0 Configuration settings. The ETH0 port is used for network communications with the ICPAM appliance.
  - a. If a 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. The DHCP check box is selected by default.

- b. (Optional) If a DHCP server is not used to assign IP address settings, enter the following information in the ETH0 fields:

|                        |  |
|------------------------|--|
| <b>IP Address</b>      | Enter the IP address of the Cisco Gateway. |
| <b>Subnet Mask</b>     | Enter the subnet mask.                     |
| <b>Default Gateway</b> | Enter the IP gateway address.              |

6. (Optional) Enter the DNS Server address if names (not IP addresses) are used for the ICPAM address.
7. Enter the ICPAM Configuration in this manner:
  - a. Enter the ICPAM IP address (IP address or name) to enable gateway communication with the appliance.
  - b. Enter the port number for the ICPAM appliance. The port number must be greater than 1024 and less 65535. The default is 8020.


---

|      |   |
|------|---|
| Hint | DHCP can also be configured to supply the Gateway with the IP address of the ICPAM appliance by configuring option 150 in the DHCP response. The ICPAM appliance TCP port number can be provided by DHCP option 151 of the DHCP response. |
|------|---|

---

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

The SSL and port values should match the SSL and port values configured on the server during setup.

 ***SSL must be consistently either enabled or disabled for all gateways, controllers, and the ICPAM appliance. Identiv recommends that SSL always be enabled to ensure secure communications. If the SSL settings are changed, you must reset all gateways and the ICPAM appliance.***

8. Click **Save** to save the settings. Wait until the Gateway resets and the Web browser displays the 'Network Settings Applied' page. Changes do not take effect until they have been saved.
9. Repeat these steps for each Gateway in the system.
10. Perform additional configuration, verification, and monitoring tasks as described in the **ICPAM User Guide**.

## Identiv EM-100 Controllers

The instructions for installing and configuring the Identiv EM-100 controller are provided in the following sections.

### Overview of an EM-100 Controller

The Identiv EM-100 controller is a single-door controller which supports an entry reader. You can connect an optional Exit Reader Expansion Module, which adds a second (exit) reader to the door. Having an exit reader makes it possible to better track a person's location or movements, and provides more flexibility when defining and enforcing anti-passback areas.



The following tables provide various specifications for the EM-100 controller.

**Table 4: EM-100 Controller: General Specifications**

| Aspect of EM-100 controller | Specification   |
|-----------------------------|---|
| Dimensions                  | 6.1 W x 4.8 H x 1.5 D in.<br>(154.9 x 122.5 x 37.1 mm)            |
| Weight                      | 11.3oz (320g)   |
| Mounting Holes              | US double-gang, US single-gang, and EU/APAC<br>60mm               |
| Housing Material            | UL94 polycarbonate  |
| Audio / Visual Indicators   | Two LEDs on RJ-45 port for network; beeper for<br>boot and tamper |
| Operating Temperature       | 32° to 122° F (0° to 50° C)                                       |
| Operating Humidity          | 5% to 95% relative, non-condensing                                |



|   |   |
|---|---|
| Communication Ports                             | Ethernet (10/100), Hi-O CANbus, Wiegand, or Clock-and-Data<br>Certifications: UL294 (US) Listed Component, CSA 205 (Canada), FCC Class A (US), ICES-003 Class A (Canada), CE Mark EN 301 489-3 EN 55022 EN 50130-4 (EU), C-Tick AS/NZS CISPR 22 (Australia, New Zealand), & Korea (KCC) |
| Ethernet Cabling Length                         | 328 feet (100 meters) using Category 5 cable  |
| HiO CAN Bus Wiring Length using 22 AWG (0.65mm) | 30 feet (10 meters) max between drops;<br>100 feet (30 meters) total length   |

**Table 5: EM-100 Controller: Power Specifications**

|  |  |
|--|--|
| <b>Input Power</b>   |  |
| DC Input (max) @ PoE   | 14.4W (300mA @ 48VDC)                        |
| DC Input (max) @ AUX   | +12VDC 18W (1500mA @ 12VDC)                  |
| DC Input (max) @ AUX   | +24VDC 36W (1500mA @ 24VDC)                  |
| Supervised Inputs Power (max)  | 0.025W (5mA sink, 5V nominal) 0 to +5VCD Ref |
| <b>Output Power (MAX) for total system (all field devices)</b>           |  |
| DC Input @ PoE   | 9.6W   |
| DC Input @ AUX   | +12VDC 14.4W                                 |
| DC Input @ AUX   | +24VDC 28.8W                                 |
| <b>Hi-O CANbus Output</b>  |  |
| Voltage, DC Input = PoE  | 24VDC  |
| Voltage, DC Input = AUX  | AUX +VDC                                     |
| <b>Output Power (max) for individual field devices, DC Input = PoE</b>   |  |
| Hi-O Device on CANbus  | 9.6W (400mA @ 24VDC)                         |
| Wiegand / C&D Reader   | 7.1W (580mA @ 12.25VDC)                      |
| Wet Output (@12VDC)  | 6.9W (580mA @ 12VDC)                         |
| Wet Output (@24VDC)  | 8.6W (360mA @ 24VDC)                         |
| <b>Output Power (MAX) for individual field devices, DC Input = 12VDC</b> |  |
| Hi-O Device on CANbus  | 14.4W (1200mA @ 12VDC)                       |
| Wiegand / C&D Reader   | 3.9W (320mA @ 12.25VDC)                      |
| Wet Output (@12VDC)  | 8.4W (700mA @ 12VDC)                         |

| <b>Output Power (MAX) for individual field devices, DC Input = 24VDC</b> |                         |
|--|-------------------------|
| Hi-O Device on CANbus  | 28.8W (1200mA @ 24VDC)  |
| Wiegand / C&D Reader   | 7.3W (600mA @ 12.25VDC) |
| Wet Output (@12VDC)  | 8.4W (700mA @ 12VDC)    |
| Wet Output (@24VDC)  | 16.8W (700mA @ 24VDC)   |
| <b>Relay Rating</b>  |                         |
| Relay Contact Rating (Dry Output)  | 2A @ 30VDC              |

### *Door Peripherals Operational Current*

The following table provides typical operational current draw for doors associated with the EM-100.

| <b>Device</b>   | <b>Conditions</b>       | <b>Typical Operational Current</b> |
|---|-------------------------|------------------------------------|
| Door Position Switch<br>(For example, Securitron MSS) | V <sub>in</sub> = 12VDC | 15mA                               |
|   | V <sub>in</sub> = 24VDC | 15mA                               |
| Mag Lock<br>(For example, Securitron M32)             | V <sub>in</sub> = 12VDC | 300mA                              |
|   | V <sub>in</sub> = 24VDC | 150mA                              |
| REX Switch<br>(For example, Securitron EEB)           | V <sub>in</sub> = 12VDC | 28mA                               |
|   | V <sub>in</sub> = 24VDC | 38mA                               |
| iCLASS Wiegand Reader                                 | V <sub>in</sub> = 12VDC | 150mA                              |

### *Compute and Compare Overall Current Draw*

Calculate the total current draw for all door peripherals and the attached Wiegand readers with the following equation, adding terms as required.

$$I_{\text{total}} = I_{\text{dps}} + I_{\text{mag}} + I_{\text{rex}} + \dots + I_{\text{iCLASS reader}}$$

The following calculations provide load current computations.

$$I_{\text{total}} @ 12\text{VDC} = 15\text{mA} + 300\text{mA} + 28\text{mA} + 150\text{mA} = 493\text{mA}$$

$$I_{\text{total}} @ 24\text{VDC} = 15\text{mA} + 150\text{mA} + 38\text{mA} + 150\text{mA} = 353\text{mA}$$

Compare the required current draw ( $I_{\text{total}}$ ) to the output current capacity of the EM-100 to select the EM-100 power scheme.

| <b>Device</b>                          | <b>Port</b>             | <b>Conditions</b>  | <b>V<sub>out</sub></b> | <b>I<sub>out</sub></b> |
|--|-------------------------|--------------------|------------------------|------------------------|
| Standard Networked Controller (EM-100) | CAN DC PWR Output (MAX) | AUX 12-24VDC Input | +10.8 to +24VDC        | 1.2Amp                 |
|  |                         | PoE input          | +24VDC (NOM)           | 0.4Amp                 |

In this example, the EM-100 provides sufficient power when operated with a PoE injector, or with +12/24VDC auxiliary power supplies.

Ensure all door peripherals connected to the Strike/AUX relays and the Reader DC PWR Output or both do not exceed 1.2Amps (AUX Input) or 0.4Amps (PoE Input), combined. Alternatively, the door peripherals may be connected to the Strike/AUX relays configured for Dry contact up to 2Amps per relay.

### Installing an EM-100 Controller

The EM-100 controller can be installed and configured using the following procedure:

1. Install a junction box and connect the EM-100 controller's mounting plate to it at the required wall location, as shown in Figure 43.

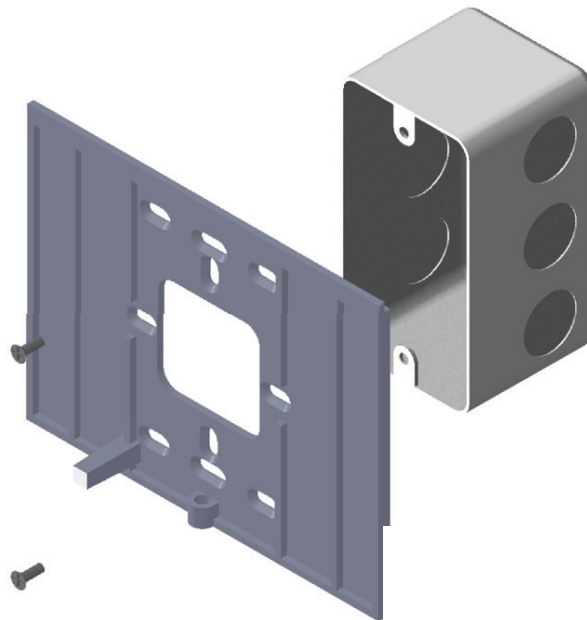


Figure 43: Installing the Mounting Plate for an EM-100 Controller

The physical dimensions of the EM-100 controller's mounting plate are:

6.1 W x 4.8 H in. (154.9 x 122.5 mm)

2. Wire the EM-100 controller as required for the connected devices.

Figure 44 and Figure 45 show the most commonly used connections.

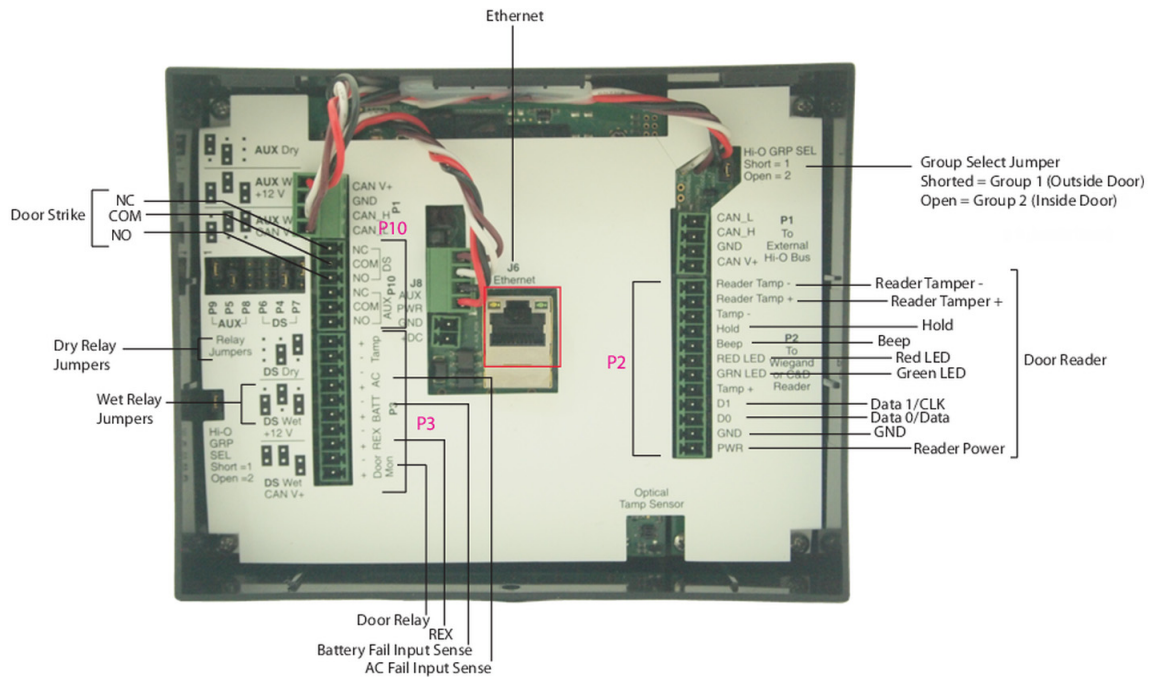


Figure 44: Commonly Used Connections on the EM-100 Controller

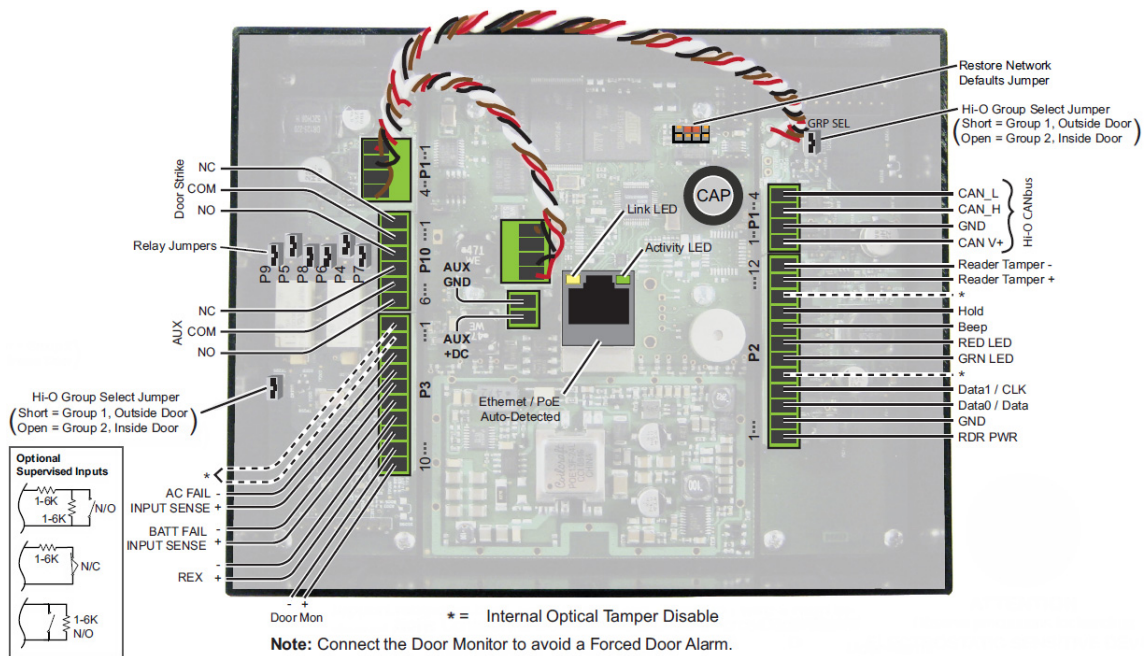


Figure 45: Wiring Connections on the EM-100 Controller

The following table lists the function of each pin on the connectors of an EM-100 controller.

**Table 6: Function of the Pins on an EM-100 Controller**

| <b>Pin</b>                                      | <b>Function</b>                  |
|---|----------------------------------|
| <b>P1 Connector (4 pins) for the HiO CANbus</b> |                                  |
| Pin 1   | CAN V+                           |
| Pin 2   | Ground                           |
| Pin 3   | CAN_H                            |
| Pin 4   | CAN_L                            |
| <b>P2 Connector (12 pins)</b>                   |                                  |
| Pin 1   | Reader Power                     |
| Pin 2   | Ground                           |
| Pin 3   | Data0 (Data)                     |
| Pin 4   | Data1 (Clock)                    |
| Pin 5   | Internal Optical Tamper Disable  |
| Pin 6   | Green LED                        |
| Pin 7   | Red LED                          |
| Pin 8   | Beep                             |
| Pin 9   | Hold                             |
| Pin 10  | Internal Optical Tamper Disable  |
| Pin 11  | Reader Tamper +                  |
| Pin 12  | Reader Tamper -                  |
| <b>P3 Connector (10 pins)</b>                   |                                  |
| Pin 1   | Internal Optical Tamper Disable  |
| Pin 2   | Internal Optical Tamper Disable  |
| Pin 3   | AC Power Failure -               |
| Pin 4   | Input Sense +                    |
| Pin 5   | Battery Failure -                |
| Pin 6   | Input Sense +                    |
| Pin 7   | Request to Exit (REX) -          |
| Pin 8   | Request to Exit (REX) +          |
| Pin 9   | Door Monitor -                   |
| Pin 10  | Door Monitor +                   |
| <b>P10 Connector (6 pins)</b>                   |                                  |
| Pin 1   | Door Strike Normally Closed (NC) |
| Pin 2   | Door Strike Common               |
| Pin 3   | Door Strike Normally Open (NO)   |
| Pin 4   | AUX Normally Closed (NC)         |
| Pin 5   | AUX Common                       |
| Pin 6   | AUX Normally Open (NO)           |

The most important wiring and setup instructions include:

- a. Set relay jumpers for either wet or dry, as required for your devices.
    - Wet can be set to either 12V or 24V.
    - Dry can be set to either open or closed.
  - b. Specify whether this door is Outside for entry (Group 1) or Inside for exit (Group 2) by setting the Group Select jumper.

The Exit Reader Expansion Module (introduced with the ICPAM 2.2 release) is enabled by this jumper. When you add a second reader to the EM-100, use the Group Select jumper to identify it as the exit (Inside) reader of the door.
  - c. Unpack and mount any input or output devices as required. Connections include door relays (P3 pins 9-10), REX button (P3 pins 7-8), and door strike (P10 pins 1-3).
    - Output 1 is provided for the Door Strike.
    - Output 2 is available to program however you like.
    - Tamper – this cannot be changed for other uses; it is connected to the optical sensor on the controller and therefore has a specific use. It can be wired to an alternate tamper device and either the optical sensor or tamper device will put the EM-100 into tamper mode (Loud beeping).
    - Door Monitor – the default behavior of this input is managing the status of the door (Open or Closed).
    - REX – the default behavior of this input is masking the alarm and momentarily triggering output 1 (door strike).
    - AC Power Failure – the default behavior is monitoring the AC power connection; if the AC power is lost, the controller will quietly beep (like a smoke detector without a battery).
    - Battery Failure – the default behavior is monitoring the battery power; if battery power is lost, the controller will quietly beep (like a smoke detector without a battery).
  - d. Connect one or more door readers (P2 pins 1-12), as well as any other input and output devices to the EM-100 controller.
3. Connect power to the EM-100 controller.
- When using PoE, install a UL294-compliant PoE injector between the Ethernet switch or router and the controller.

Figure 46 on page 55 shows an example wiring diagram incorporating several elements, including an optional power supply and an optional strike (assuming that PoE is used).

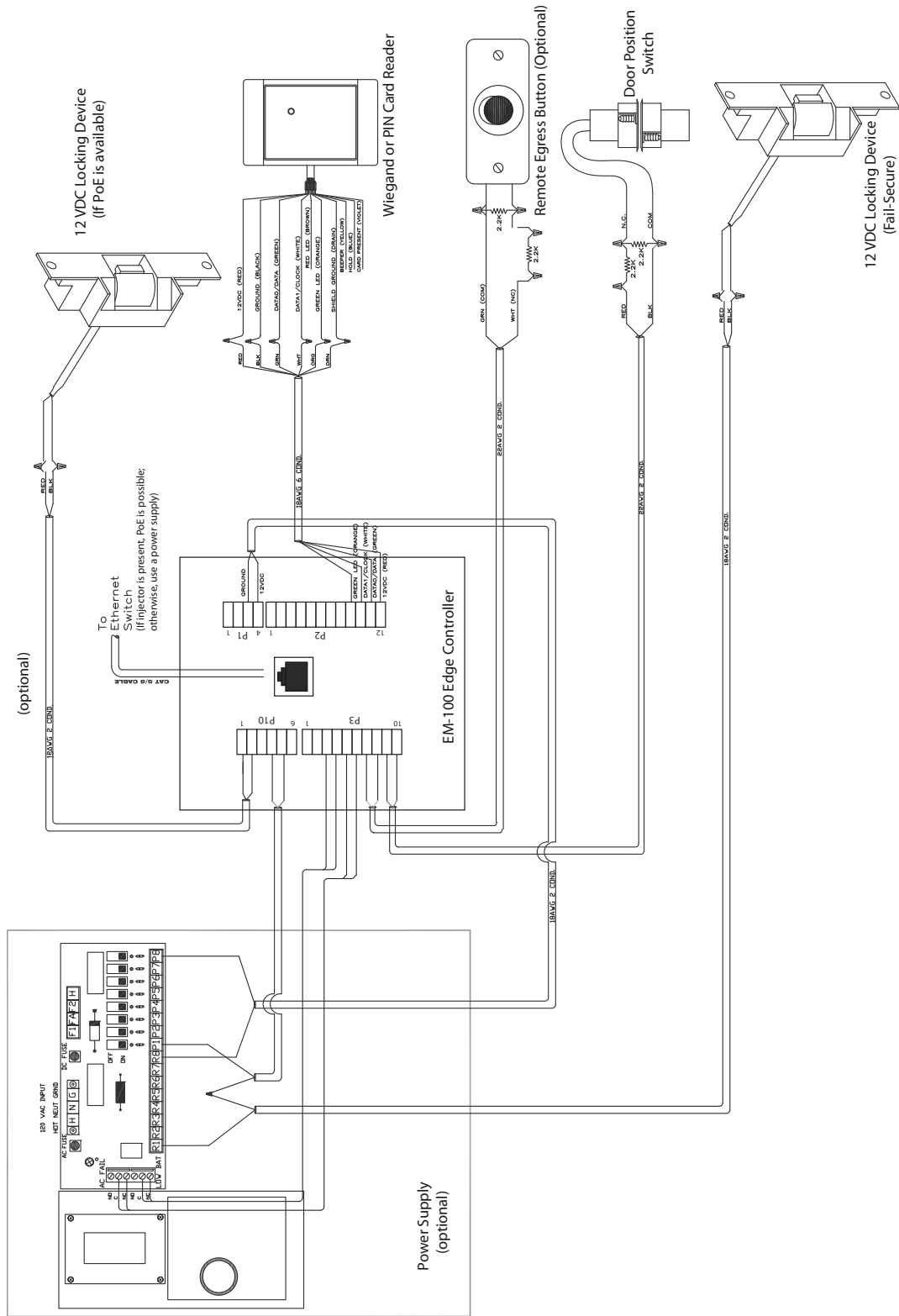


Figure 46: Example Wiring Diagram for an EM-100 Controller

Hint In most installations, a conventional power supply is used because it can reliably supply more power to more components, including more types of readers, than can be supported by a PoE injector.

---

4. Install the EM-100 controller on the mounting plate, securing it with a screw at the bottom.

### Configuring an EM-100 Controller

1. Use an Ethernet cable to connect the RJ-45 socket on the EM-100 controller directly to the RJ-45 socket on a computer running either the Windows XP, Windows 2000, or Windows 7 operating system.
2. Ensure that power is supplied to the controller, as explained in the previous topic.
3. Set the computer's Ethernet port to use DHCP.
4. Open a Command Prompt window, type the following command:  
`ipconfig /renew`  
and then press **Enter**.
5. Open a Web browser on the connected computer and enter **https://169.254.242.121** in the URL field.  
The Web browser warns that this is not a private connection.

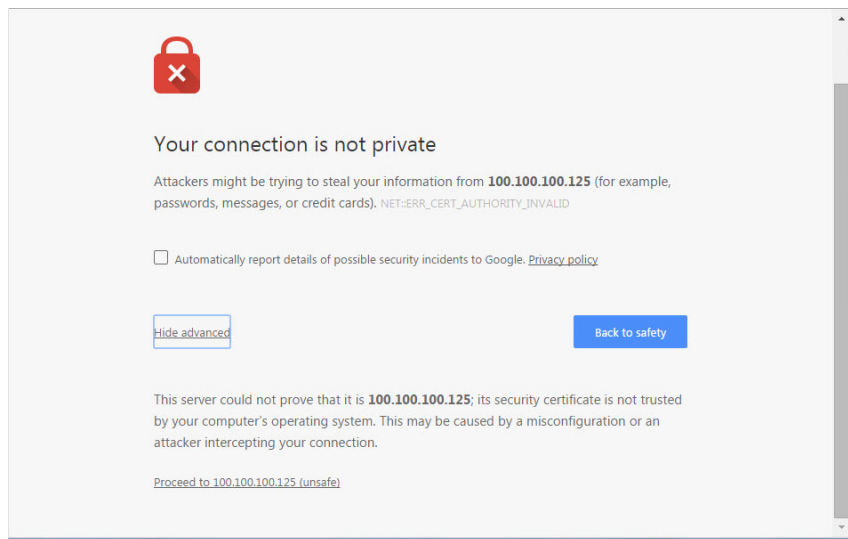
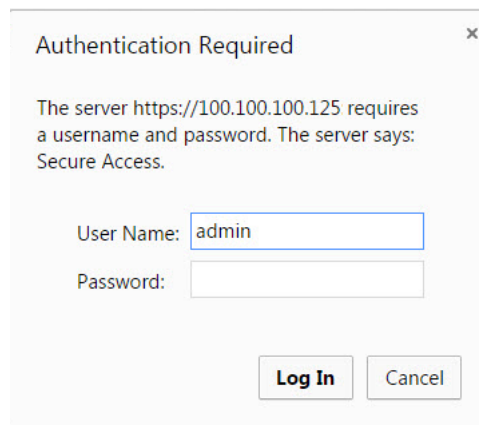


Figure 47: EM-100 Configuration - Warning that Connection Is Not Private

6. Click the '**Proceed to 169.254.242.121 (unsafe)**' link at the bottom of the page.



An 'Authentication Required' dialog appears.

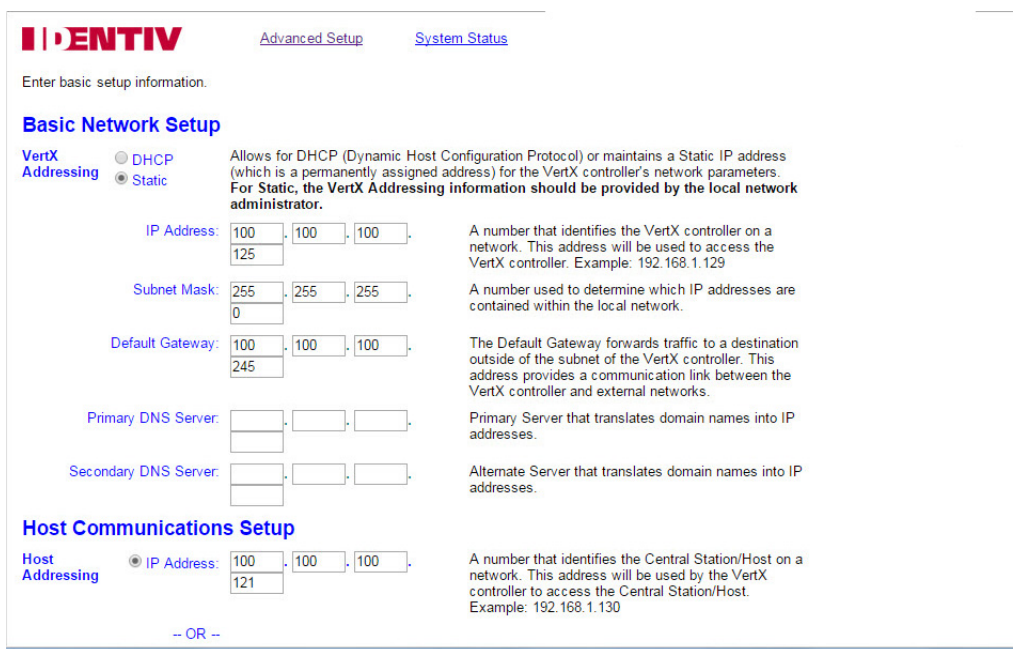


The dialog box is titled "Authentication Required" and contains the following text: "The server https://100.100.100.125 requires a username and password. The server says: Secure Access." Below this text are two input fields: "User Name:" with the value "admin" and "Password:" which is empty. At the bottom right are two buttons: "Log In" and "Cancel".

Figure 48: EM-100 Configuration - Authentication Required Dialog

7. In the User Name field, type **admin**.
8. In the Password field, type **identiv123**.
9. Click **Log In**.

The Basic Network Setup page appears.



The screenshot shows the "Basic Network Setup" page in the IDENTIV configuration interface. The page has a header with the IDENTIV logo and links for "Advanced Setup" and "System Status". Below the header, it says "Enter basic setup information." The main section is titled "Basic Network Setup" and includes radio buttons for "DHCP" and "Static" (selected). To the right of these buttons is a note: "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." Below this are several input fields for network parameters, each with a brief description to its right:
 

- IP Address:** 100.100.100.125. Description: "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. Description: "A number used to determine which IP addresses are contained within the local network."
- Default Gateway:** 100.100.100.245. Description: "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:** [Empty]. Description: "Primary Server that translates domain names into IP addresses."
- Secondary DNS Server:** [Empty]. Description: "Alternate Server that translates domain names into IP addresses."

 Below the network setup section is the "Host Communications Setup" section, which includes radio buttons for "IP Address" (selected) and "DHCP". The "IP Address" field is set to 100.100.100.121. Description: "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". At the bottom of the page, it says "-- OR --".

Figure 49: EM-100 Configuration - Basic Network Setup Page

Each field is defined briefly in the right column.

10. Click the **Advanced Setup** link at the top of this page.

The Advanced Network Setup page appears.

**IDENTIV** [Basic Setup](#) [System Status](#) [Supplemental Configuration](#)

Enter advanced setup information.

### Advanced 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.

**Network Broadcast:** 10 . 19 . 255 . 255  
 The IP address used to broadcast messages to multiple local network devices.

**Domain Name:** identiv.com  
 A name that identifies a network. The domain name will be used to access a VertX controller. Example: HIDVertX.com

Figure 50: EM-100 Configuration - Advanced Network Setup Page (Part 1)

11. Change or enter values for these fields:

- Click the **Static** radio button. The EM-100 controller must be provided with a fixed address. DHCP does not function properly with the EM-100, unless an address has been reserved.
- In the 'IP Address' field, enter the fixed IP address for this controller.
- In the 'Subnet Mask' field, enter the subnet mask for this controller.
- In the 'Default Gateway' field, enter the default gateway address for this controller.
- If required, in the 'Primary DNS Server' and 'Secondary DNS Server' fields, enter appropriate values for the DNS servers to which this controller will be connected.
- In the 'Network Broadcast' field, enter the IP address used to broadcast messages to multiple local network devices.
- In the 'Domain Name' field, enter the designated name that identifies this network.

|  |   |
|--|---|
| <p>Host Name: <input type="text" value="uTrustVerge"/></p> <p>FTP Enabled: <input type="radio"/> Yes<br/><input checked="" type="radio"/> No</p> <p>Telnet Enabled: <input type="radio"/> Yes<br/><input checked="" type="radio"/> No</p> <p>SSH Enabled: <input type="radio"/> Yes<br/><input checked="" type="radio"/> No</p> <p>SSL Enabled: <input type="radio"/> Yes<br/><input checked="" type="radio"/> No</p> <p>Virtual Port Enabled (169.254.242.121): <input type="radio"/> Yes<br/><input checked="" type="radio"/> No</p> | <p>An identifier used to access a VertX controller on a network by name.</p> <p>Enables or disables the VertX controller FTP need this enabled.</p> <p>Enables or disables the VertX controller Telnet capability. Note that the Central Station/Host may need this enabled.</p> <p>Enables or disables the VertX controller SSH capability. Note that the Central Station/Host may need this enabled.</p> <p>Enables or disables the VertX controller SSL capability. Note that the Central Station/Host may need this enabled.</p> <p>Alternate IP address for the VertX controller. When the Virtual Port is enabled it provides a pathway to always contact the controller.</p> |
|--|---|

### Advanced Host Communications Setup

|  |   |
|--|---|
| <p><b>Host Addressing</b></p> <p><input checked="" type="radio"/> IP Address: <input type="text" value="100"/><input type="text" value="100"/><input type="text" value="100"/><br/><input type="text" value="121"/></p> <p>-- OR --</p> <p><input type="radio"/> Host Name: <input type="text"/></p> | <p>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</p> <p>An identifier used by the VertX controller to access a Central Station/Host on a network. Example: CSHost.HIDVertX.com</p> |
|--|---|

|   |  |
|---|--|
| <p>Here I Am Interval (sec): <input type="text" value="20"/></p> <p>TCP/IP Connection Port: <input type="text" value="4070"/></p> <p>TCP/IP Listen Port: <input type="text" value="4050"/></p> <p>Encrypt Host Communication: <input type="radio"/> Yes<br/><input checked="" type="radio"/> No</p> <p>Encryption Key Seed Value: <input type="text" value="2244668800"/></p> | <p>The time interval in which a controller sends a Here I Am message to a Central Station/Host. Valid entry is 20 to 86400 seconds.</p> <p>The port in which the Central Station/Host listens for an incoming VertX controller connection. Valid entry is 1025 to 65535.</p> <p>The port in which the VertX controller listens for an incoming Central Station/Host connection. Valid entry is 1025 to 65535.</p> <p>Enable encrypted communication between the Vertx and Host controllers.</p> <p>Seed from which the shared VertX/Host encryption key is derived. Valid entry is between 0 and 200 numeric values.</p> |
|---|--|

### Login Password

The login password for the admin user has been set.

[Change Login Password](#)

Select Save to confirm the network settings and the VertX controller will be configured as listed above, or select Cancel to reconfigure.

Figure 51: EM-100 Configuration - Advanced Network Setup Page (Part 2)

- In the 'Host Name' field, enter the identifier used to access the controller.
- For the next five items, select either its Yes button or its No button. Unless otherwise required, the recommended settings are:

|                      |            |
|----------------------|------------|
| FTP Enabled          | <b>No</b>  |
| Telnet Enabled       | <b>No</b>  |
| SSH Enabled          | <b>No</b>  |
| SSL Enabled          | <b>Yes</b> |
| Virtual Port Enabled | <b>Yes</b> |
- In the 'Host Addressing' field, enter the IP address that identifies the ICPAM Server on the network. Alternatively, click the 'Host Name' radio button, and supply the identifier used by the controller to access the ICPAM Server on the network.

- If you want to encrypt the communication between the ICPAM Server and its door controllers (whether they are Gateways or EM-100 controllers), you must do it for all of them. To enable encryption on this EM-100 controller, select the **Yes** radio button for the **Encrypt Host Communication** option, and make sure a random seed number is entered in the **Encryption Key Seed Value** field.

If you are encrypting the communication, be sure that later when you are using the ICPAM Desktop Client to add this EM-100 controller to the Hardware Tree, you check the **Use encryption** option on the Configuration page, and you enter the same seed number in the **Encryption seed** field.

- Leave the other advanced host communication settings at their default values.
- Click the **Change Login Password** link to change the login password for this EM-100 configuration.
- At the bottom of the screen, click **Save**.

The current controller status is displayed graphically.

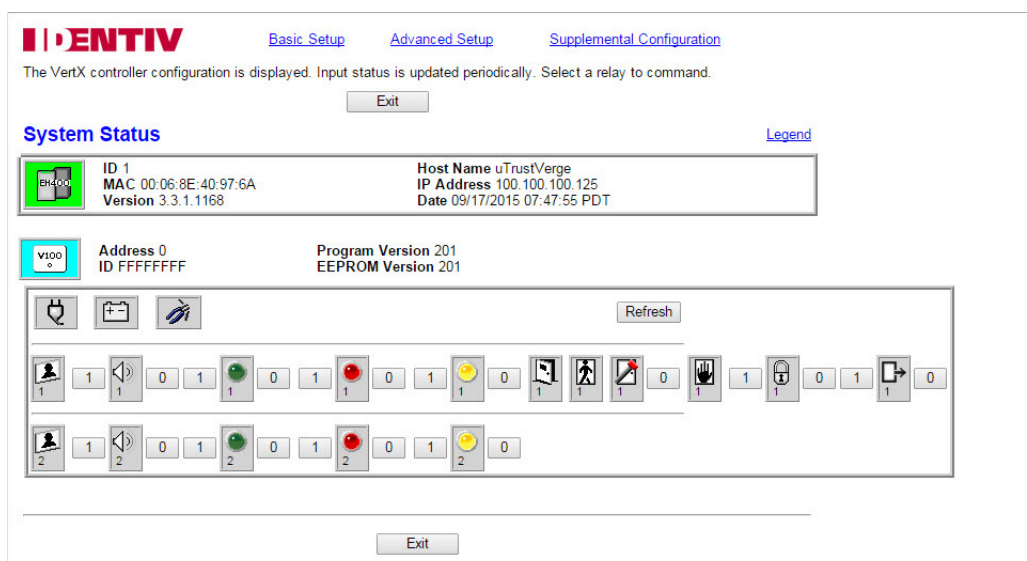


Figure 52: EM-100 Configuration - System Status Page

Click the **Legend** link (in the upper right) for definitions of the symbols and colors that can appear on this page.

You can use this utility to update relays and alarms attached to the controller; however, using ICPAM is easier and more productive.


12. Click **Exit** to leave this EM-100 configuration program.
13. After configuration is completed, disconnect the Ethernet cable between the configuring computer and the EM-100 controller, then reconnect the network cable routed through the EM-100 controller's mounting plate to the EM-100's RJ-45 socket.

## Optical Tamper Feature of an EM-100 Controller

To disable the internal optical tamper sensor for the right side PCB (reader interface board), attach a jumper wire from P2 pin 10 to P2 pin 5.

To disable the internal optical tamper sensor for the left side PCB (door interface board), attach a jumper wire from P3 pin 1 to P3 pin 2.

**CAUTION** *The EM-100 controller ships with these jumpers pre-installed on the connectors. Removing these jumpers causes false tampers to trigger.*

 *If desiring an external tamper, wire an unsupervised Normally Closed contact, replacing one of the pre-installed jumpers.*

## Beep Patterns of an EM-100 Controller

The following table explains the beep patterns generated by an EM-100 controller to indicate different alarm conditions.

**Table 7: Beep Patterns of an EM-100 Controller**

| Beep Pattern                              | Explanation  |
|---|--|
| Short (80 ms) beeps, every 10 seconds     | AC power failure alarm.  |
| Two short (80 ms beeps), every 40 seconds | Battery failure alarm.   |
| Short (100ms) beeps, 2 seconds apart      | After a normal access grant, the door was held open or did not close fully. (The door held timer was exceeded prior to seeing the door contact sensor close.)<br>Look for someone propping the door open. If this is a recurring issue, check the door for friction or air pressure which prevents the door position sensor from detecting the door closed condition.  |
| Long (500ms) beeps, 1 second apart        | The door was forced open. (The door contact sensor was seen to open even though the door mode was secured and no access grant was seen within the unlock timer time.) This can result from: <ul style="list-style-type: none"> <li>the door actually being forced open.</li> <li>the door rubbing on the door frame (or other resistance to it fully closing), so that it closed enough for the door contact sensor to indicate it was closed, but the back lock or door strike did not engage and properly secure the door. So when someone later comes to the door and opens it without presenting a badge or entering a PIN code (because the door was ajar), the Door Forced Open alarm and event are triggered.</li> <li>the door being unlocked with a physical key, even though the door is secured with a reader.</li> <li>the door has a motion sensor that is not picking up traffic approaching the door from the secure side. When the approaching person opens the door, if the motion sensor acting as a REX has not seen them, the door is seen by the controller to open without a badge or REX triggering a door forced open</li> </ul> |

|                     |  |
|---------------------|--|
| One continuous beep | <p>The controller and/or reader tamper has been triggered.</p> <p>Check that the controller's enclosure is fully shut and secured with its screw.</p> <p>A distortion of the plastic housing due to poor wiring which prevents the optical tamper post from completely covering the optical tamper sensor will trigger a tamper alarm and event. Tamper alarms typically subside no more than 15 seconds after resolving the tamper condition, although occasionally you may have to manually clear the alarm via the web console.</p> |
|---------------------|--|

## Resetting an EM-100 Controller's Password and IP Address

You can use the Debug Port to correct persistent problems in an EM-100 controller's network configuration. This is particularly useful if the admin password is forgotten.

Resetting the controller's password and IP address to their default values requires access to the controller's back plate. After this is done, you must place a jumper over two pins of the debug port before rebooting the controller. With this jumper in place, the controller resets the settings to the factory defaults during the ensuing reboot.

1. Remove the EM-100's back plate.
2. Loosen the Mylar cover.

The debug port jumper pins are located underneath the Mylar, to the left of the group select jumper, as shown in Figure 53.

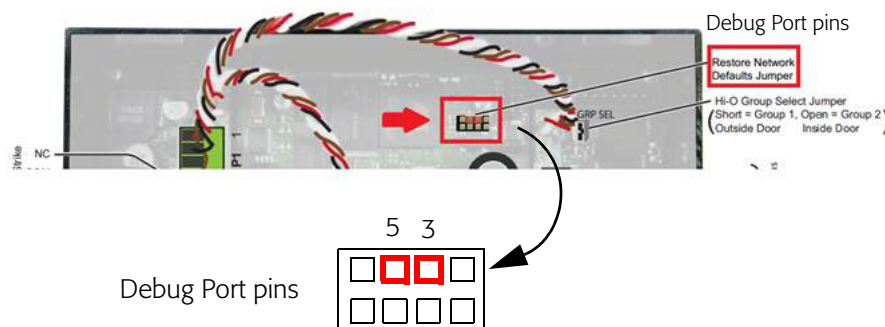


Figure 53: Debug Port Jumper Pins on an EM-100 Controller

3. Remove the jumper from the Hi-O Group Select (GRP SEL) jumper pins.
4. Reboot the controller.
5. After the first beep, place the jumper over pins 3 and 5 of the eight-pin debug port header.



**Network reset mode is available for 30 seconds after the first beep, while the EM-100 is rebooting; a second beep signals the end of the 30-second interval, indicating that network reset mode is no longer active.**

6. After 30 seconds, the beeper issues a sustained tone indicating success. If an error occurs, you receive a single beep.

- 
7. Remove the jumper and replace it on the Hi-O termination header, then recycle power.

The controller resets in approximately 60 seconds. After the reset is complete, you hear the single beep. After the 30-second window, you will hear the second beep. The controller is fully functional during this time.

**CAUTION** *During the controller rebooting process, the controller's password and IP address is overwritten and returned to these default values:*

- User name = admin
  - Password = identiv123
  - Static IP Address = 10.4.19.129
  - Direct-connect IP Address (for configuration) = 169.254.242.121
8. Configure the controller for your installation parameters.
  9. Reinstall the EM-100 controller's mylar and back plate.

For a demonstration of this process, see the YouTube video:  
<https://www.youtube.com/watch?v=vNhs1ZMOfNY>



## Connecting an Exit Reader Expansion Module

Starting with the ICPAM 2.2 release, the EM-100 controller supports an Exit Reader Expansion Module which adds a second (exit) reader to the door. Having an exit reader makes it possible to better track a person's location or movements, and provides more flexibility when defining and enforcing anti-passback areas.

The following diagram shows the connections on the back of the module, which are used for running wires to the corresponding pins on the back of an EM-100 controller. Be sure that you set the position of the HiO Group Select jumper to Open, to designate that this second reader is for exiting an inside door.

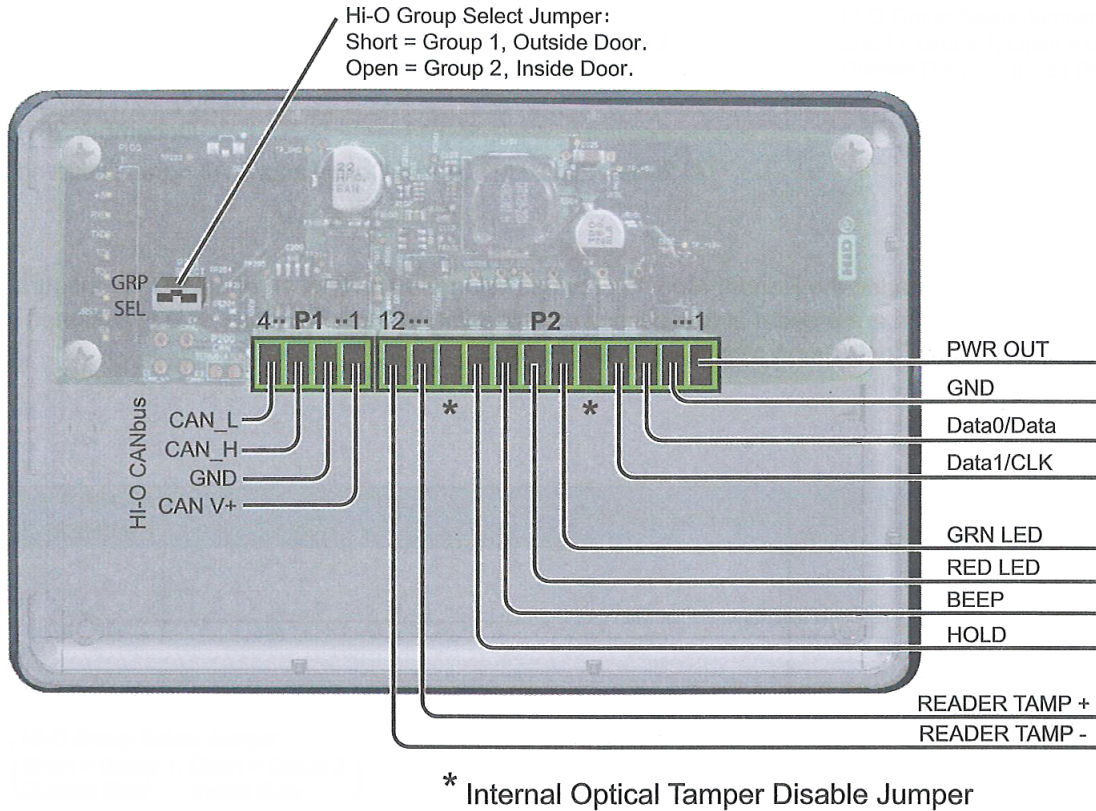


Figure 54: Wiring Connections on the Exit Reader Expansion Module (for an EM-100 Controller)

The following table lists the function of each pin of the connectors on an Exit Reader Expansion Module, which is the same as on an EM-100 controller.

**Table 8: Function of the Pins on an Exit Reader Expansion Module**

| Pin   | Function |
|---|----------|
| <b>P1 Connector (4 pins) for the HiO CANbus</b> |          |
| Pin 1   | CAN V+   |
| Pin 2   | Ground   |
| Pin 3   | CAN_H    |
| Pin 4   | CAN_L    |



| <b>P2 Connector (12 pins)</b> |                                 |
|-------------------------------|---------------------------------|
| Pin 1                         | Reader Power                    |
| Pin 2                         | Ground                          |
| Pin 3                         | Data0 (Data)                    |
| Pin 4                         | Data1 (Clock)                   |
| Pin 5                         | Internal Optical Tamper Disable |
| Pin 6                         | Green LED                       |
| Pin 7                         | Red LED                         |
| Pin 8                         | Beep                            |
| Pin 9                         | Hold                            |
| Pin 10                        | Internal Optical Tamper Disable |
| Pin 11                        | Reader Tamper +                 |
| Pin 12                        | Reader Tamper -                 |

- If you are connecting this module to a new EM-100 controller, then when you add that controller to your ICPAM security system, choose the **EM-100 - Single Door, Two Readers** template.
- If you are connecting this module to an EM-100 controller which is already part of your ICPAM security system, then after connecting the module, right-click on that controller in the Hardware Tree, and choose the **New Slave Door...** command to open a dialog for configuring the second reader.

