Identiv Connected Physical Access Manager 2.1 Installation Guide

January 7, 2016

Identiv, Inc.
www.identiv.com

Text Part Number: IC02-01

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

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

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.

Contents

List of Figures

ICPAM Server Installation Instructions

The following sections provide detailed instructions on setting up the ICPAM server platform.

Preparations for Server Installation

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

- Ensure that your ICPAM server includes at least 16GB of RAM memory, four virtual processors, and sufficient hard drive memory to accommodate the database that will be created (at least 100GB).
- Make sure 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 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 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 or Mac OS environment. This means that in order to run ICPAM server on a PC or Mac, you need to install VMware. (Other virtualization products, such as Virtual Box or HyperV, are not supported.) The recommended versions of VMware is version 5.1 or 6.0.

There are a wide range of products in the VMware family.

- The free version is called VMware Player. This is sufficient for testing environments and small installations. The link for VMware Player is listed here:

  ```
  https://my.vmware.com/web/vmware/free#desktop_end_user_computing/
  vmware_player/5_0|PLAYER-504|product_downloads
  ```

- A company environment normally requires a more robust version of VMware, such as ESXi vSphere or VMware Workstation. These versions require licenses and must be paid for after a brief evaluation period.
  - VMware ESXi 6.0 is the recommended version of VMware for enterprise systems and can be downloaded from this location:

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

    This version provides vSphere Hypervisor as virtualization manager and user interface, one of the easier approaches to installing and configuring a computer for use with VMware.
  - VMware Workstation is another reliable version for ICPAM servers. Like ESXi, it provides a user-friendly interface and many useful features. It can be downloaded from:

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

Depending on your application and requirements, the free version might not prove sufficient. Obtain an appropriate version of VMware and install it according to the manufacturer's specifications and your system's requirements.

Once downloaded, install your selected VMware version. Follow the installation instructions provided by the VMware installation wizard.

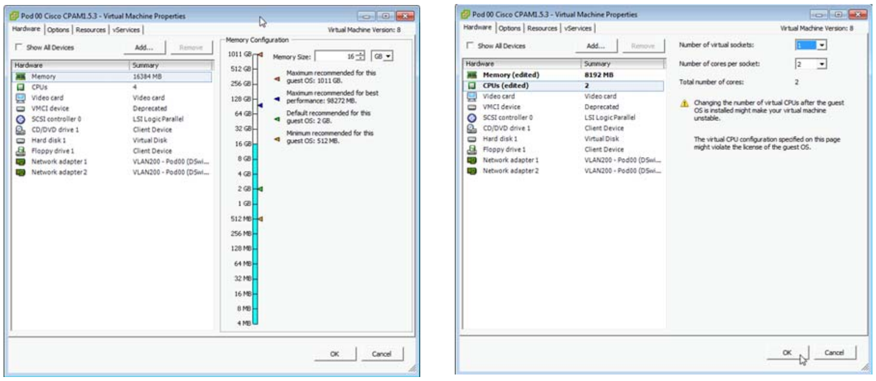
Deploying the OVA file

An OVA file is a pre-configured virtual appliance that can be deployed to your VMWare environment to allow 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.

1. To download the current OVA, go to:
   www.identiv.com/icpam-support

   Follow the instructions for registering and downloading the latest ICPAM OVA.
2. In the VMware software, perform one of the following tasks.
   - For VMware player, click the **Open a Virtual Machine** option.
   - For vSphere client, select **Deploy OVF Template...** from the **File** menu.
   - For VMware Workstation, select **File > Open**.
3. Browse to the location where you downloaded the ICPAM OVA file and select it.
4. Click **Import** or **Open**.
5. Once the OVA file becomes available, click the **Edit virtual machine settings** option or right click the file and select **Edit Settings** from the pop-up option list.

   A configuration window appears.


Pod 00 Cisco CPAM1.5.3 - Virtual Machine Properties
Hardware
Options
Resources
vServices
Virtual Machine Version: 8
Show All Devices
Add...
Remove
OK
Cancel

Hardware	Summary
Memory	16384 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	Client Device
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VLAN200 - Pod00 (DSwi...
Network adapter 2	VLAN200 - Pod00 (DSwi...

Memory Configuration

Memory Size: 16 GB

Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 98272 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 512 MB.

Hardware	Summary
Memory (edited)	**8192 MB**
CPUs (edited)	**2**
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	Client Device
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VLAN200 - Pod00 (DSwi...
Network adapter 2	VLAN200 - Pod00 (DSwi...

Number of virtual sockets: 1

Number of cores per socket: 2

Total number of cores: 2

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Figure 1: VMware Settings for OVA File

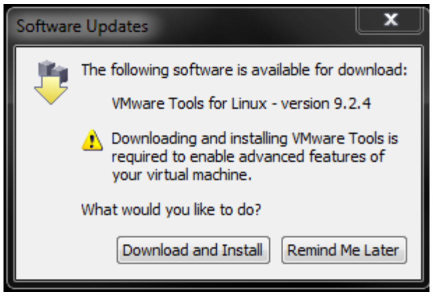
6. Edit the virtual machine settings as required. Minimally, the settings should include these values:
   - 16GB of RAM
   - 4 processor cores

   Change other values required for your system.

Launching the CPAM Server Virtual Machine for the First Time

1. Do one of these:

- For VMware player, click on the **Play Virtual Machine** button then click **Download and Install**.



Software Updates

The following software is available for download:

VMware Tools for Linux - version 9.2.4

Downloading and installing VMware Tools is required to enable advanced features of your virtual machine.

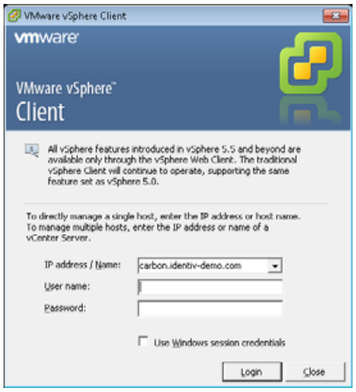
What would you like to do?

Figure 2: Software Updates Message

Hint Customers often cause themselves problems by closing a virtual machine when it is loading. While the virtual machine is booting, 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.

- From VMware ESXi, launch the VMware vSphere Client using this procedure:
  - Enter the default user name and password then click **Login**.



VMware vSphere Client

All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: carbon.identiv-demo.com

User name:

Password:

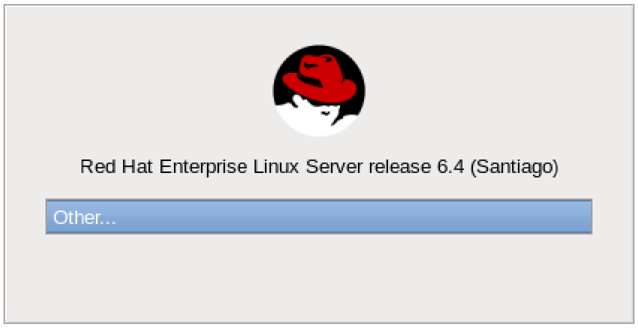
□ Use Windows session credentials

Figure 3: VMware vSphere Client

  - Click on **VMs and Templates**.
  - Locate your virtual appliance in the left window tree and right-click on it.
  - Select the **Open Console** option.
- From VMware Workstation, use this procedure:

- Select **File** > **Open** > **Virtual Machine**.
- Navigate to the ICPAM virtual machine and select **Open**.

The RHEL console window appears.

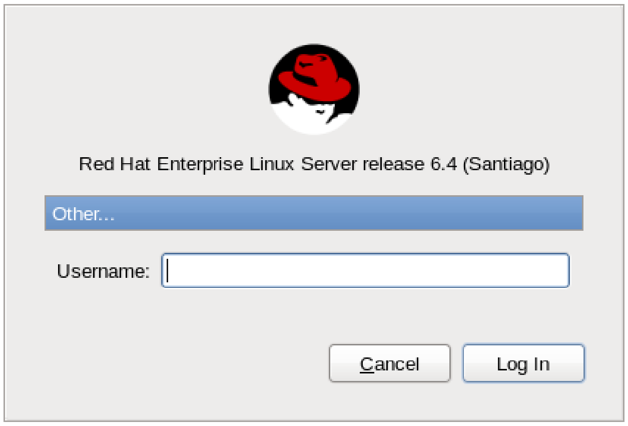


Red Hat Enterprise Linux Server release 6.4 (Santiago)

Figure 4: VMware Console Window

☞ *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 like Figure 5.



Red Hat Enterprise Linux Server release 6.4 (Santiago)

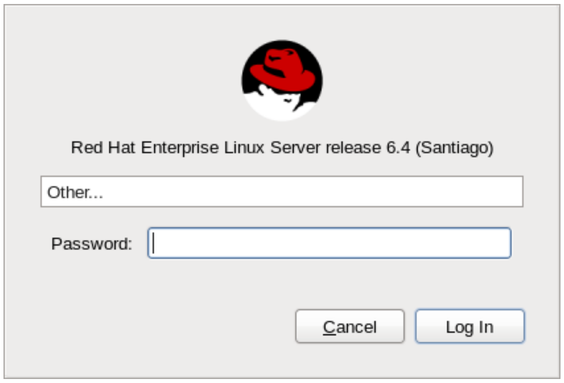
Figure 5: Username Field Sign-In

4. Type this:

```
cpamadmin
```

This is your default username. Now click the **Log In** button.

The password screen appears.



Red Hat Enterprise Linux Server release 6.4 (Santiago)

Other...

Password:

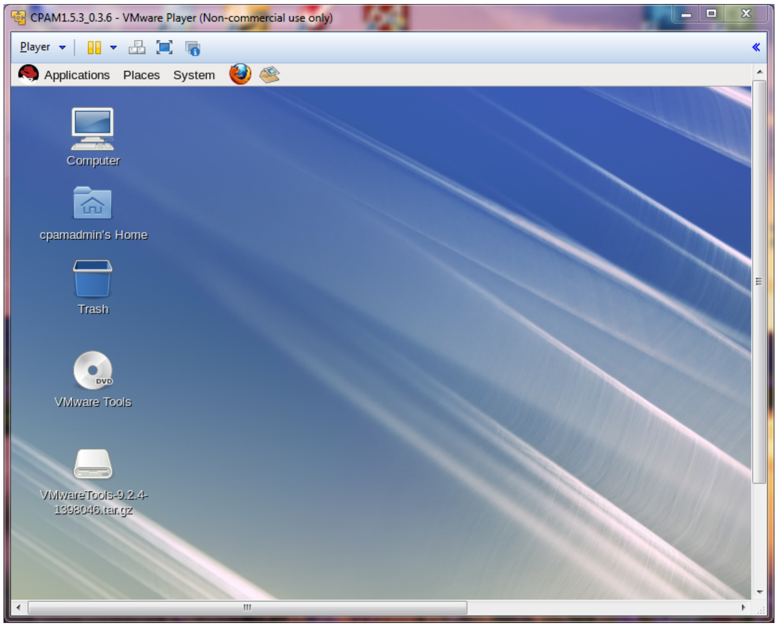
Figure 6: Password Field

5. Enter the default password:

   ```
   cpamadmin
   ```

   Then click the **Log In** button again.

   The console screen appears.



CPAM1.5.3_0.3.6 - VMware Player (Non-commercial use only)
Player
Applications
Places
System
Computer
cpamadmin's Home
Trash
VMware Tools
VMwareTools-9.2.4-1398046.tar.gz

Figure 7: RHEL Console Screen

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

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

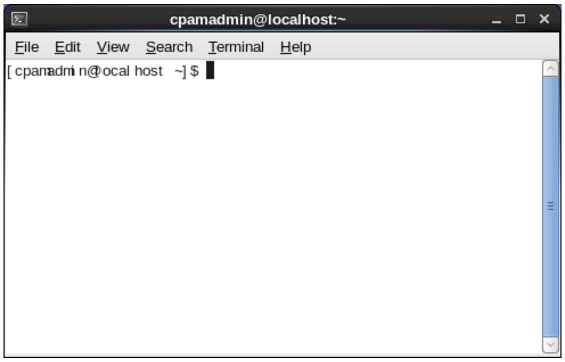
Obtaining Super-user Privilege

1. From the Desktop screen, select the **Applications** menu at the top of the screen then click the **System Tools** menu option.

You are presented with two options.

2. Select **Terminal**.

   A command line dialog box appears.



```
[cpamadmin@localhost ~]$ 
```

Figure 8: Terminal Command Line Window

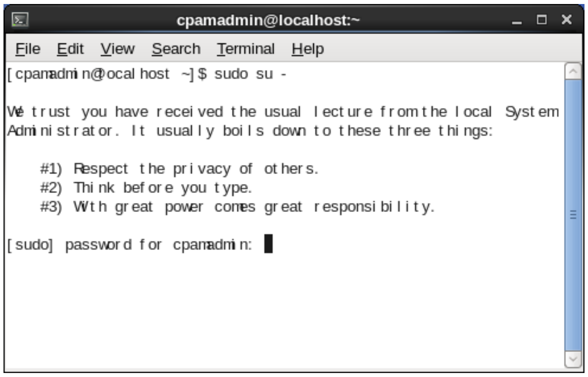
3. At the command line prompt, type

   ```
   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, once the proper password is entered. Without administrative privileges, you are not allowed to change configuration settings.

   The dialog box returns a prompt for a password as shown in Figure 9.



```
[cpamadmin@localhost ~]$ 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 cpamadmin: 
```

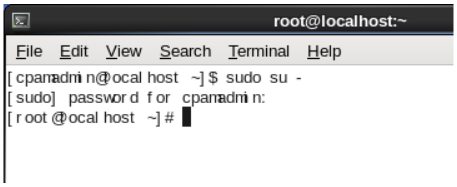
Figure 9: Super-User Permissions Command Line

4. At the new 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:



```
[cpamadmin@localhost ~]$ sudo su -
[sudo] password for cpamadmin:
[root@localhost ~]#
```

Figure 10: Root 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.*

Setting the ICPAM Server Address

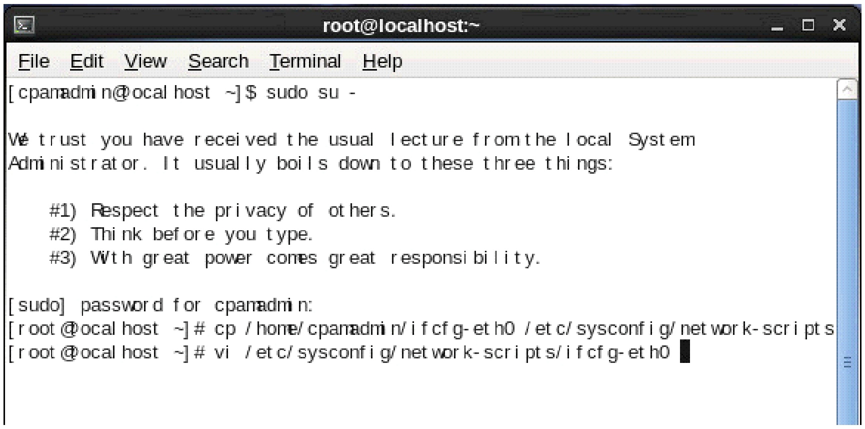
Once you have acquired root authority, use it to configure ICPAM in the following way:

1. At the root prompt, type this command:

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

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

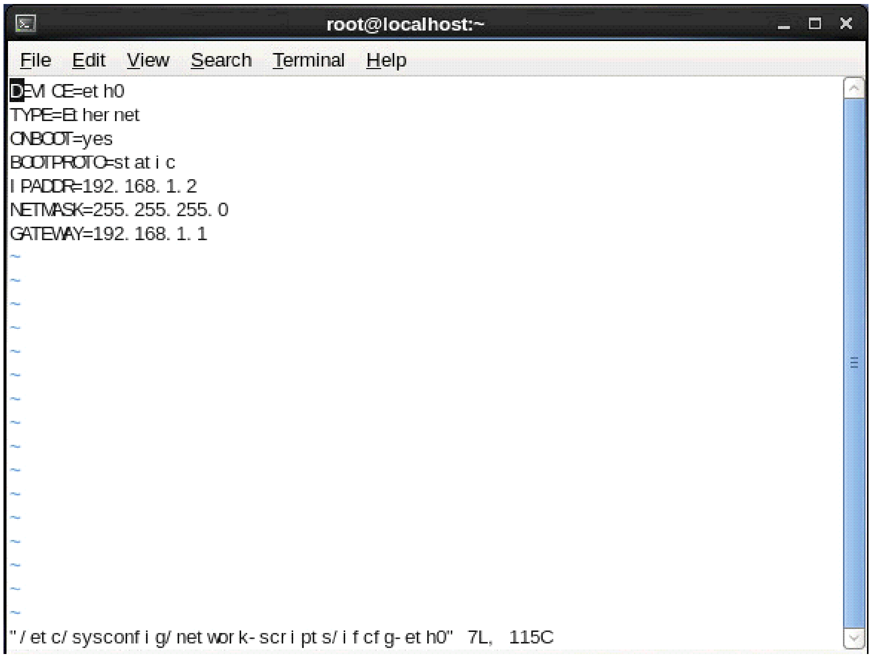
   where there is a space between `vi` and `/etc`
4. Press **Enter** again.



```
[cpamadmin@localhost ~]$ 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 cpamadmin:
[root@localhost ~]# cp /home/cpamadmin/ifcfg-eth0 /etc/sysconfig/network-scripts
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Figure 11: Root Prompt Commands

The vi text editor displays a list of ifcfg-eth0 file parameters including the IP address, netmask, and gateway (Figure 12).

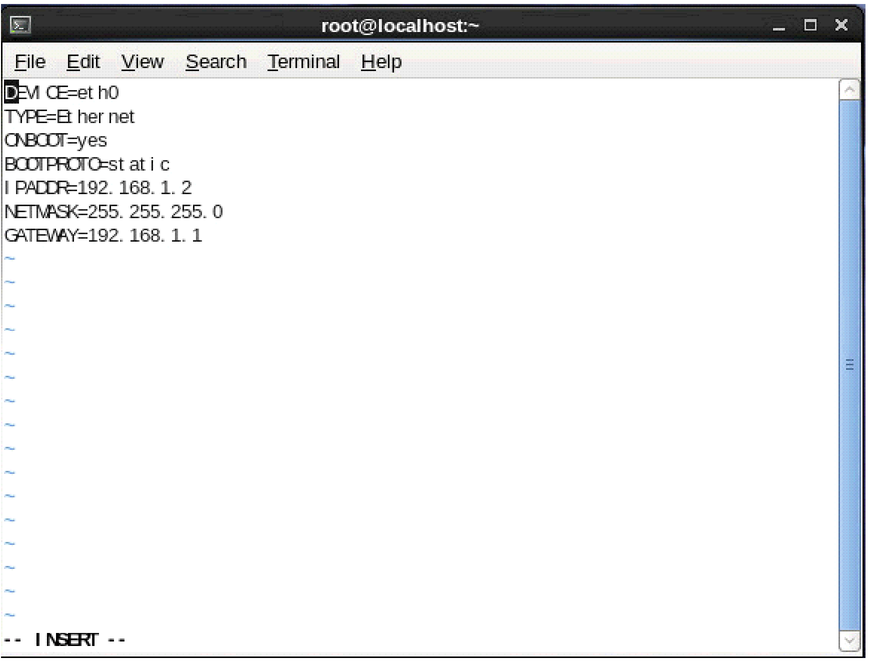


```
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.2
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/network-scripts/ifcfg-eth0"  7L,  115C
```

Figure 12: vi Text Editor ifcfg-eth0 File Example

5. Once in vi, press **i**.

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



```
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.2
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

Insert mode indicated

Figure 13: Enter Insert Mode

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 IPPADDR line and go to the end of the line. Delete the 192.168.1.2 IP address using the Backspace button (the Delete key on a Mac) and replace the value with 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. Once you are done with the changes, hit the **Esc** key. The -- INSERT -- at the bottom of the window disappears.

☞ ***The static address, subnet mask, and gateway IP address settings must be changed to the appropriate values for your network to communicate successfully with both the ICPAM server and client.***

7. Type:

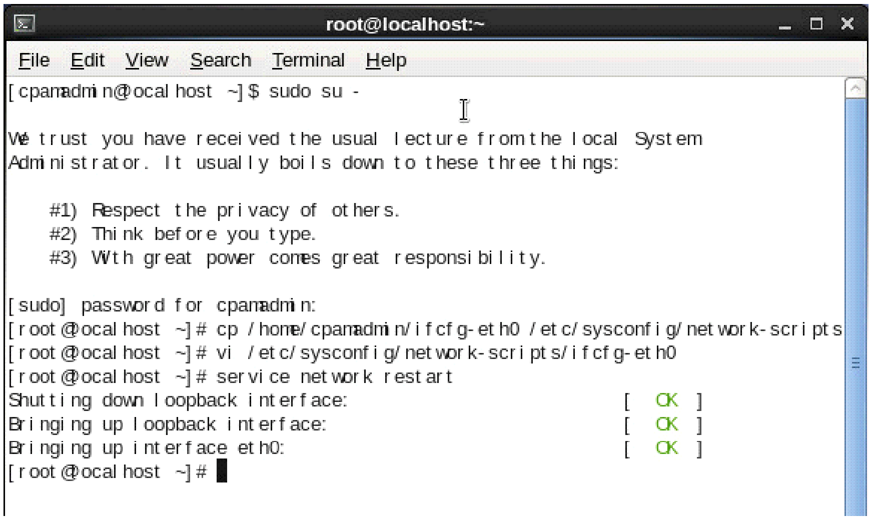
   ```
   :wq
   ```

   and press **Enter**. This saves changes to the file and exits vi.

   `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.



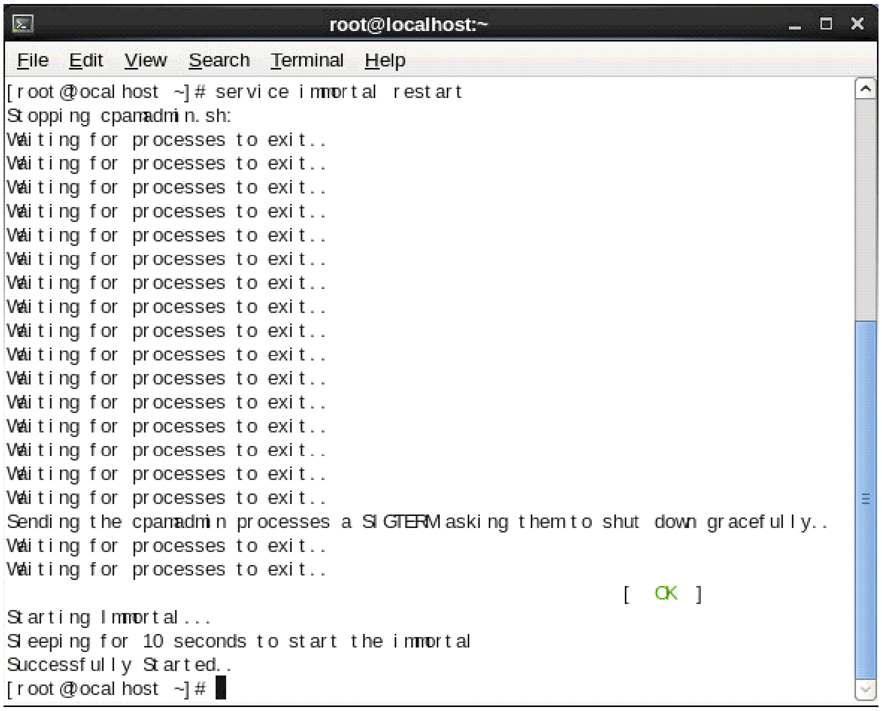
```
[cpamadmin@localhost ~]$ sudo su -

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 cpamadmin:
[root@localhost ~]# cp /home/cpamadmin/ifcfg-eth0 /etc/sysconfig/network-scripts
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
[root@localhost ~]# service network restart
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
[root@localhost ~]#
```

Figure 14: Running service network restart

9. Restart the cpamadmin service by typing:

   `service immortal restart`

   As shown in Figure 15.



```
[root@localhost ~]# service immortal restart
Stopping cpamadmin.sh:
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Waiting for processes to exit..
Sending the cpamadmin processes a SIGTERM asking them to shut down gracefully..
Waiting for processes to exit..
Waiting for processes to exit..
                                                           [  OK  ]
Starting Immortal...
Sleeping for 10 seconds to start the immortal
Successfully Started..
[root@localhost ~]#
```

Figure 15: Running service immortal restart

If during step 8 or 9 you receive a ‘permission denied’ message, you must reacquire super-user authority by entering `sudo su -` at the prompt.

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 for launch.

Launching ICPAM Server

To launch ICPAM server:

1. From the VMware shell, press **Ctrl** and **Alt** together.

   The VMware cursor is frozen and the host computer's cursor is activated.

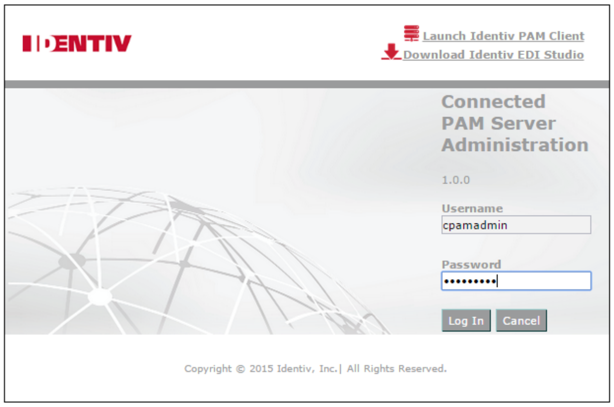
2. From the host computer's desktop, start your web browser.
3. At the URL field, enter the IP address chosen for the ICPAM server. For example:

   ```
   https://192.168.1.3
   ```

   then press **Enter**.

☞ *Depending on the browser you use, 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 screen should appear.


IDENTIV
Launch Identiv PAM Client
Download Identiv EDI Studio
Connected PAM Server Administration
1.0.0
Log In
Cancel

Username: cpamadmin

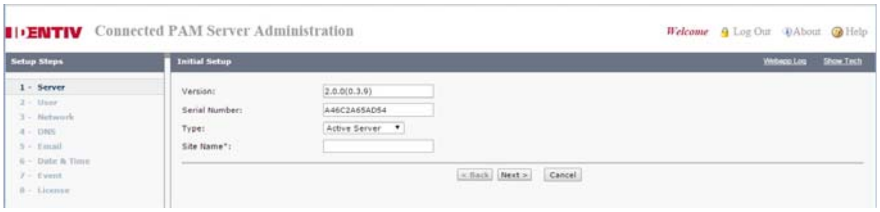
Password: •••••••••

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

Figure 16: ICPAM Server Login Window

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

   The ICPAM Server Administration main page appears.



Version: 2.0.0(0.3.9)

Serial Number: A46C2A65AD54

Type: Active Server

Site Name*:

Figure 17: ICPAM Server Administrator Starting Page

5. Change the values on the CPAM Administration pages as required.

   For instructions on configuring your ICPAM system, refer to the next section, “Configuring ICPAM Server Administration”, starting on page 13.

Configuring ICPAM Server Administration

To configure the ICPAM server administration program in preparation for installing the client and configuring the appliance hardware, follow this instruction:

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:

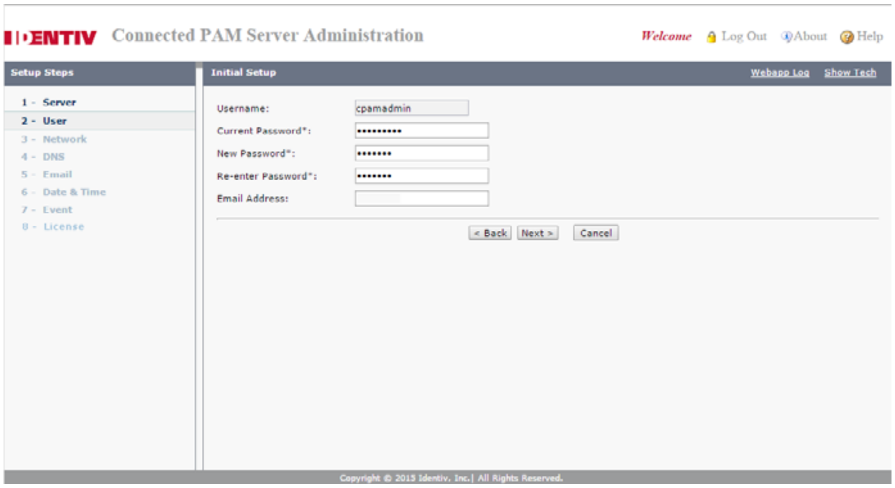
Active Server (Default) Select this option for a single appliance or if the appliance is the active server in a redundant configuration.

Standby Server Select this option if the appliance is the standby (backup) server in a redundant configuration. A standby server must exactly have the same configuration settings as the active except 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 since 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. Dashes and underscore characters are allowed. For example, `Fremont`.

c. Click **Next** to continue.

The User page appears.



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

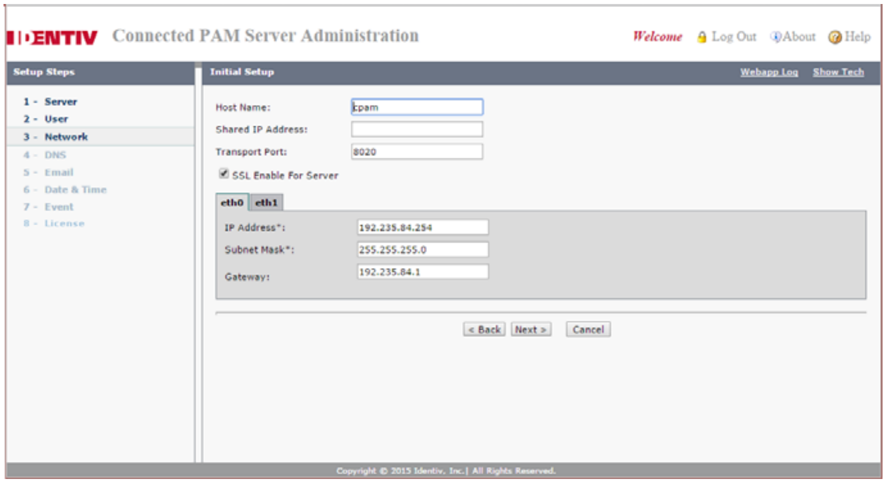
Copyright © 2013 Identiv, Inc.| All Rights Reserved.

Figure 18: ICPAM Server Administration User Page

☞ *The default username is cpamadmin. This is a read-only super-user username and cannot be changed or deleted. However, you can and should change the default password as soon as possible using the User page (Figure 18). 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 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 the setting.
   d. At the ‘Email Address’ field, enter the email address that will receive system messages. This e-mail address also receives ‘Forgot Password’ e-mails.
   e. Click **Next** to continue.

   The Network page appears.



Host Name: cpam
Shared IP Address:
Transport Port: 8020
☑ SSL Enable For Server

IP Address*: 192.235.84.254
Subnet Mask*: 255.255.255.0
Gateway: 192.235.84.1

Figure 19: ICPAM Administrator Network Page

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

☞ *This field only applies to HA configurations.*

This address is transferred from the active 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 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 on 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. See the relevant gateway or controller user guide for more information.***

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:

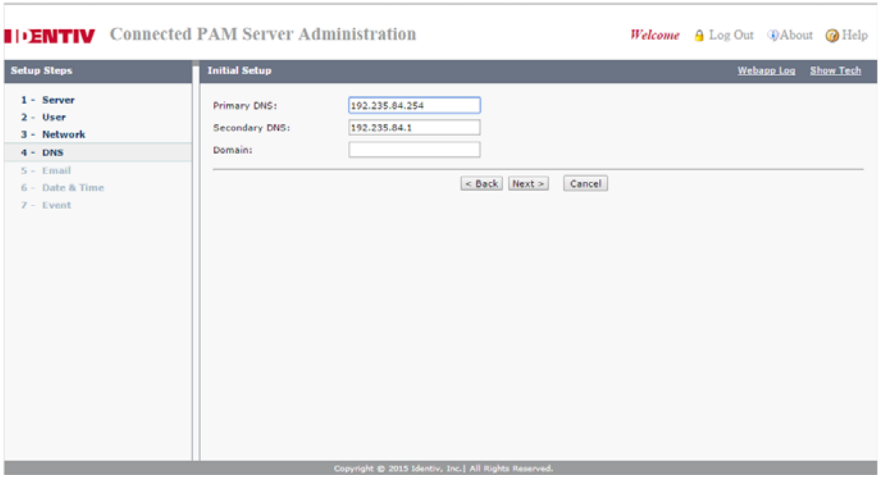
IP Address	Enter the IP address for the Eth0 port. This address should be on the same subnet as the Shared IP address, and must be different on the active and standby appliances.
Subnet Mask	Enter the subnet mask provided by your system administrator.
Gateway	(Optional) Enter the Gateway provided by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

f. 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:

Enable Interface	Check the check box to enable or disable the Ethernet interface.
DHCP	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.
IP Address	Enter the IP address for the Eth0 port. If configured, this address must be different on the active and standby appliances.
Subnet Mask	Enter the subnet mask provided by your system administrator.
Gateway	(Optional) Enter the gateway 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.



Primary DNS: 192.235.84.254

Secondary DNS: 192.235.84.1

Domain:

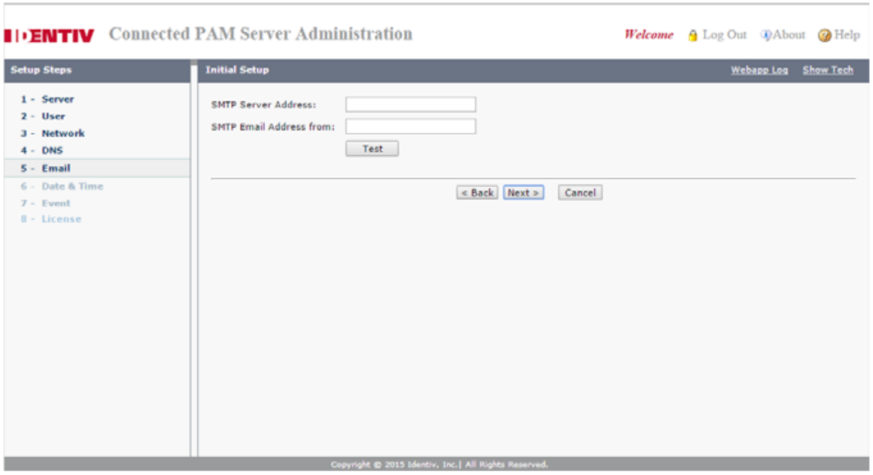
Figure 20: ICPAM Administrator DNS Page

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 screen appears like the example shown in Figure 21.



SMTP Server Address:

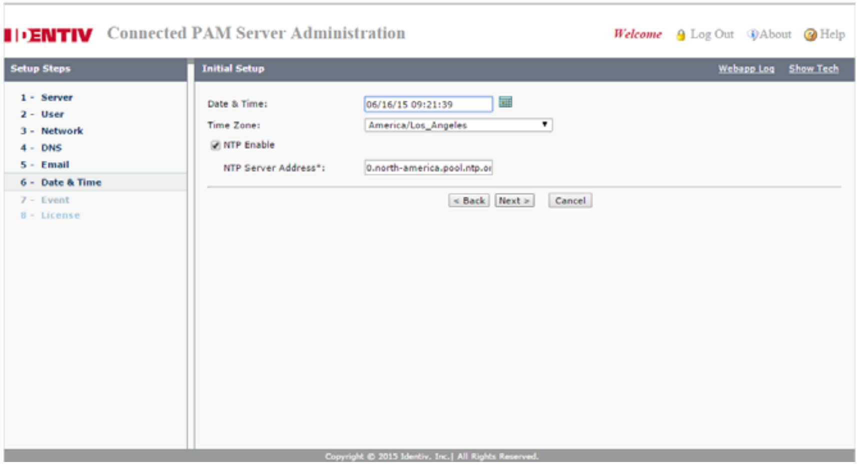
SMTP Email Address from:

Figure 21: ICPAM Administrator Email 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.



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

Time Zone: America/Los_Angeles

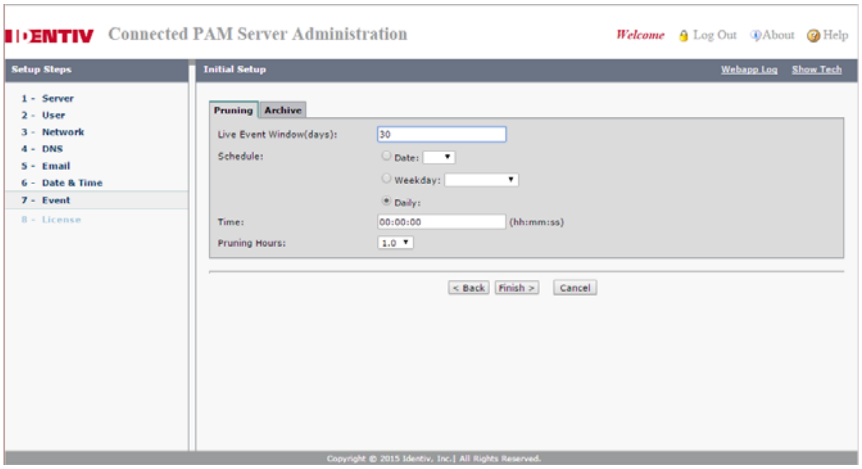
☑ NTP Enable

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

Figure 22: ICPAM Administrator 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. At the ‘NTP Server Address’ field, if NTP is enabled, enter the IP address of the NTP server.
   e. Click **Next** to continue.

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



Live Event Window(days): 30

Schedule: ○ Date: ○ Weekday: ● Daily:

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

Pruning Hours: 1.0

Figure 23: ICPAM Administrator 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 allows you to reduce the size of the main database while keeping them accessible on the ICPAM system. Pruned events are not visible in Events & Alarms, but are included in reports. Pruned events are also included in system backups.
   - Archived events are removed from all ICPAM database tables and copied to a compressed file. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archived events are not visible in the Events & Alarms listings or Reports, and are not included in system backups.

   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).

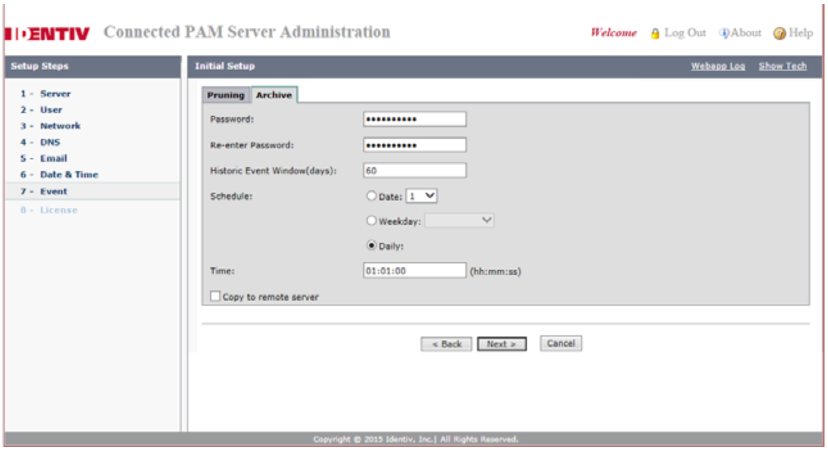
For example, to run pruning at 2 p.m., enter 14:00:00. To run pruning at 1 a.m., enter 01:00:00.

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 and the Archive subpage appears.



Password: ••••••••••

Re-enter Password: ••••••••••

Historic Event Window(days): 60

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

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

□ Copy to remote server

Figure 24: Server Administrator Event Archive Page

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

Supply values for the following fields as required.

Password

Re-enter Password

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

Note: Do NOT use special characters for this password.Only alphanumeric (0-9, a-z, A-Z) characters are allowed.

Historic Events Window (days)

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

Schedule

Enter a schedule when the historic events will be removed from the pruned database and placed into a compressed archive file (archived files are listed above the entry fields).

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

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

Daily—To run archiving every day, select **Daily**.

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

Copy to remote server

Check this box to automatically copy the archived event files to a remote FTP or SFTP location.

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

FTP

Select this radio button to indicate that the remote servers use standard File Transfer Protocol.

SFTP

Select this radio button for indicate that the remote server uses Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).

Address

Enter the IP address or hostname of the remote server.

Username

Enter the username required to log into the server.

Password

Enter the login password for the remote server.

Path

Enter the directory path where the compressed archive will be copied. The path must exist on the remote server. If the directory is not available, the archive will fail.

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

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

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

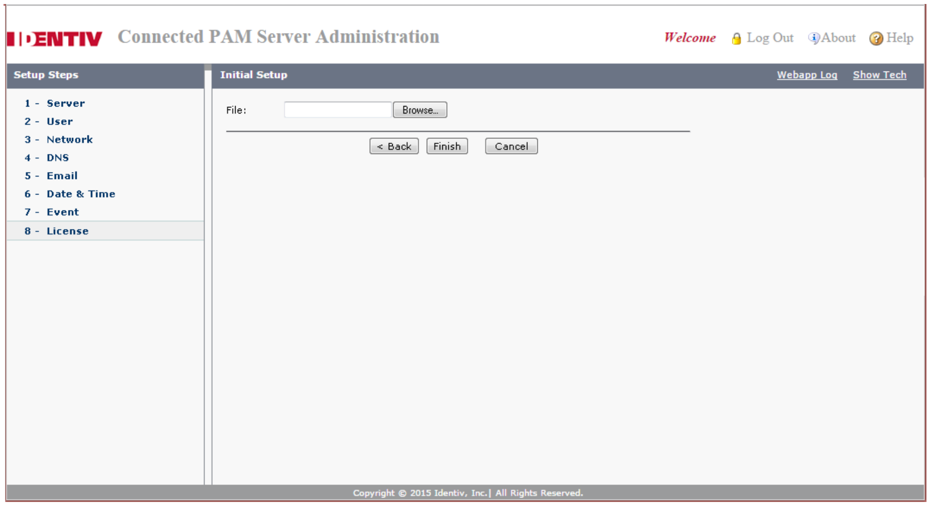


Figure 25: ICPAM Administrator License Page

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

8. Enter the license settings to obtain and install the software license:

☞ *Enter all licenses except high availability (HA) on the active appliance. Enter only the HA license on the standby appliance.*

a. Locate the Product Authorization Key (PAK) included with the ICPAM appliance.
b. In a Web browser, open the Identiv Product License Registration web page:

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

c. Follow the on-screen instructions to complete the form and enter the PAK. A license file with the extension .lic is sent to your email address.
d. Save the file to the PC used to configure the ICPAM appliance.
e. 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.
f. 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 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. 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: December 16, 2009 11:53:15 AM PST.
    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 ICPAM Client

This section describes how to install version 2.1 of the ICPAM Client software with support for the EM-100 controller.

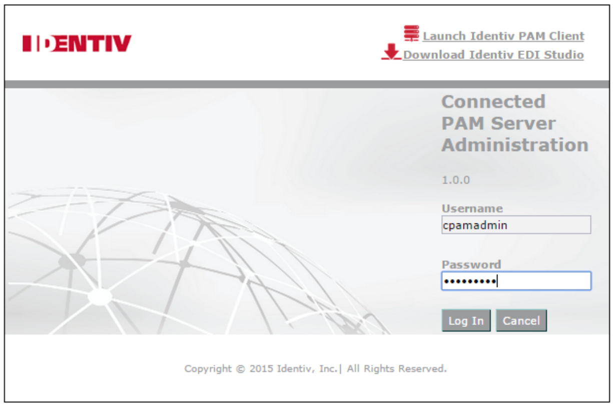
Before continuing, install the Java 1.7 32-bit client from the server and remove all other Java versions from your workstation. To do this, go to the workstation's Control Panel and under Add or Remove Programs check to see which version of Java is currently installed. If other versions of Java are installed, remove them. If Java 1.7 is not currently installed, go to `https://java.com/en/download/manual.jsp` and download version 1.7 then install it before proceeding.

1. From a host computer you intend to use as a ICPAM client, open a browser.
2. 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 screen appears as shown in Figure 26.


IDENTIV
Launch Identiv PAM Client
Download Identiv EDI Studio
Connected PAM Server Administration
1.0.0
Log In
Cancel

Username: cpamadmin

Password: •••••••••

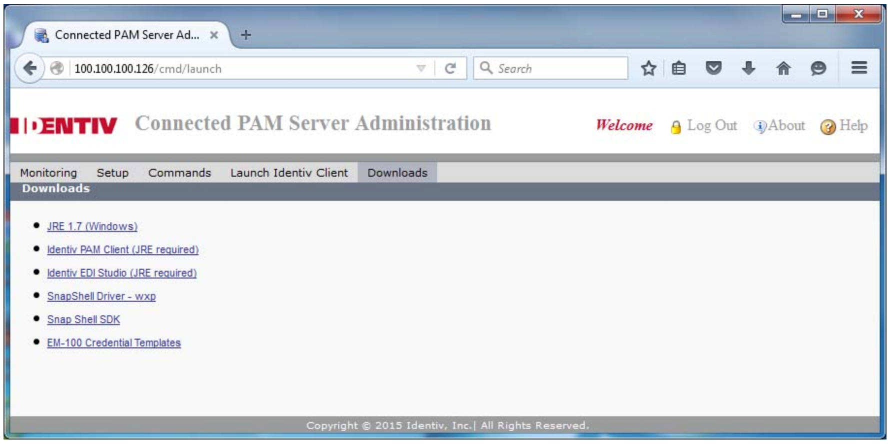
Copyright © 2015 Identiv, Inc.| All Rights Reserved.

Figure 26: ICPAM Server Login Dialog Box with ICPAM Client Link

3. Login with the cpamadmin user and the new password, then click **Log In**.

   The ICPAM Server Administration window appears.
4. Once logged in, click the **Download** tab in the ribbon bar.

The Downloads page appears.



Downloads

- JRE 1.7 (Windows)
- Identiv PAM Client (JRE required)
- Identiv EDI Studio (JRE required)
- SnapShell Driver - wxp
- Snap Shell SDK
- EM-100 Credential Templates

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

Figure 27: ICPAM Downloads Page

5. Click on the **JRE 1.7 (Windows)** link.

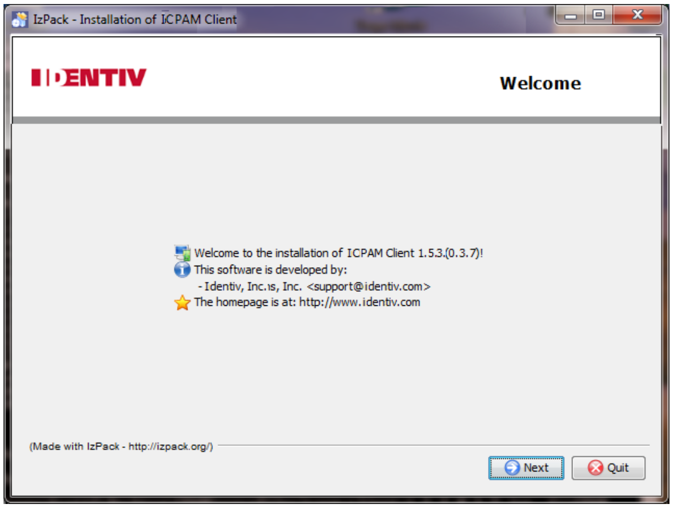
   The Java download page will appear. Do the following:

   a. At the Java SE Runtime Environment 7u80 table, click the Accept License Agreement radio button.
   b. Since JRE 1.7 must be a 32-bit version, click the **Windows x86 Online** download executable.
   If you are currently offline and cannot access the internet, you may select the Windows x86 Offline version of this executable.
   c. Follow the instructions to download the executable.
6. Click the **Run** button on the download pop-up.
7. Click the **Install** button.
8. Follow the wizard to finish the Java installation.
9. When you are finished, click **Finish**.
10. 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 window (Figure 26) and select the **Launch Identiv PAM Client** link from the upper left. (This method does not require logging in before launching.)
11. Click the **Open** or **Run** button on the download pop-up.

A welcome screen appears.

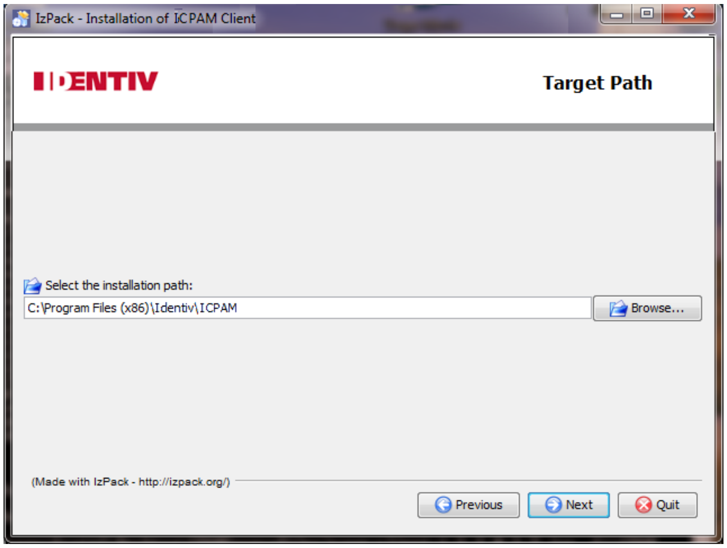

IzPack - Installation of ICPAM Client
IDENTIV
Welcome

Welcome to the installation of ICPAM Client 1.5.3.(0.3.7)!
This software is developed by:
- Identiv, Inc.ıs, Inc. <support@identiv.com>
The homepage is at: http://www.identiv.com

(Made with IzPack - http://izpack.org/)
Next
Quit

Figure 28: Client Installation Welcome Page

12. Click **Next**.


IzPack - Installation of ICPAM Client
IDENTIV
Target Path

Select the installation path:
C:\Program Files (x86)\Identiv\ICPAM

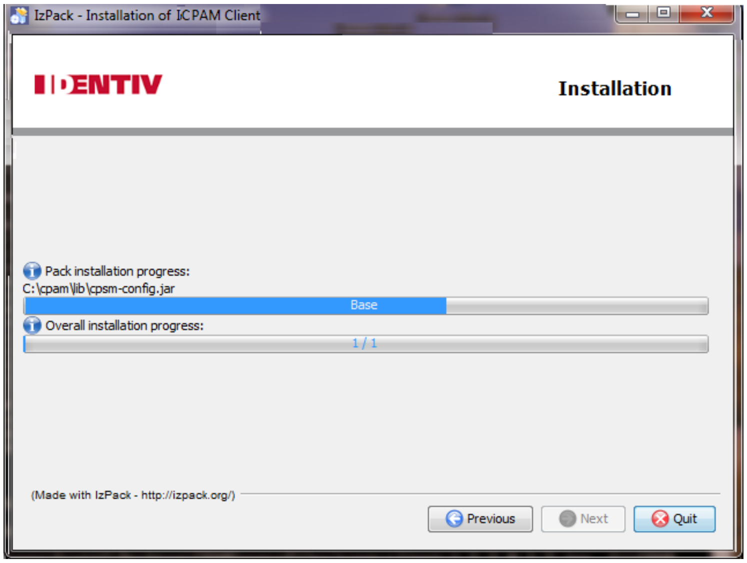
Browse...
(Made with IzPack - http://izpack.org/)
Previous
Next
Quit

Figure 29: Target Path Page

13. Either accept the default path, C:\Program Files (x86)\Identiv\ICPAM, or enter a custom path, then click **Next**.
14. Click **Yes**.
15. Click **Next**.
16. 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.*

A dialog box appears as shown in Figure 30.



IzPack - Installation of ICPAM Client

Installation

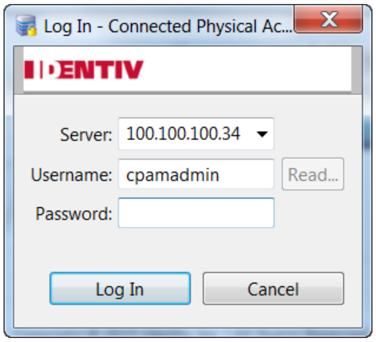
Pack installation progress:
C:\cpam\lib\cpsm-config.jar

Overall installation progress:

Figure 30: ICPAM Client Installation

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

    The Log In dialog box appears:



Log In - Connected Physical Ac...

Server: 100.100.100.34

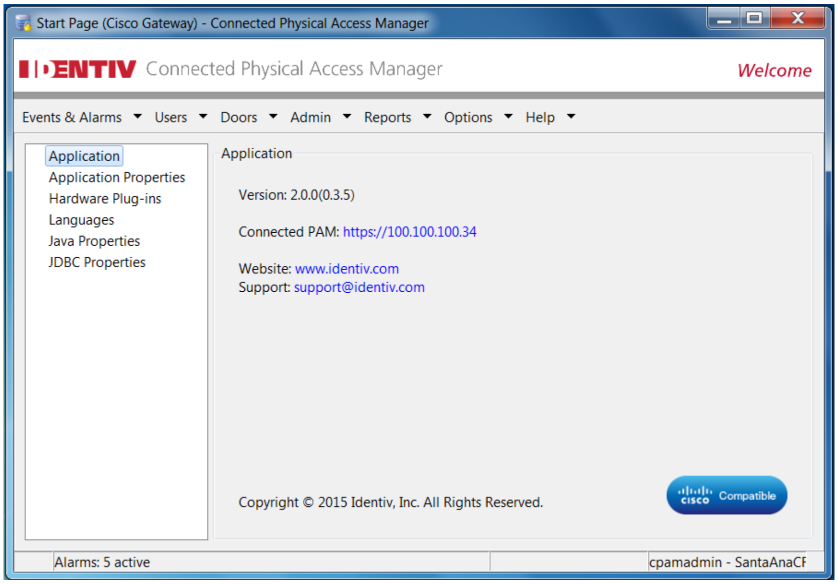
Username: cpamadmin

Password:

Figure 31: Client Log In Dialog Box

18. Enter the initial password: **cpamadmin** then click **Log In**.

The first screen of the ICPAM client appears as shown in Figure 32.



Version: 2.0.0(0.3.5)

Connected PAM: https://100.100.100.34

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

Copyright © 2015 Identiv, Inc. All Rights Reserved.

Alarms: 5 active

cpamadmin - SantaAnaCF

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*.

Controller and Gateway Installation Instructions

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

- Cisco Physical Access Gateways (page 28)
- Identiv EM-100 Controllers (page 40)

The installation and configuration of both types are explained on the following pages.

Cisco Physical Access Gateway Configuration Instructions

The Cisco Physical Access Gateway (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 the ICPAM using an Ethernet connection to the IP network. Power is supplied 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.

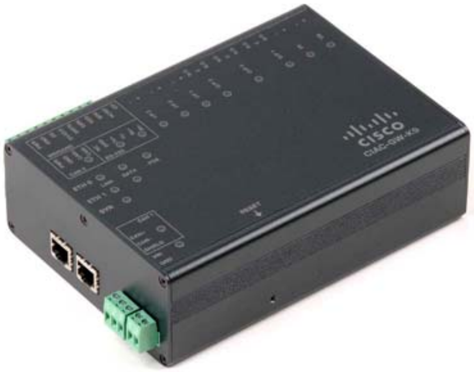


Figure 33: Cisco Physical Access Gateway

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.

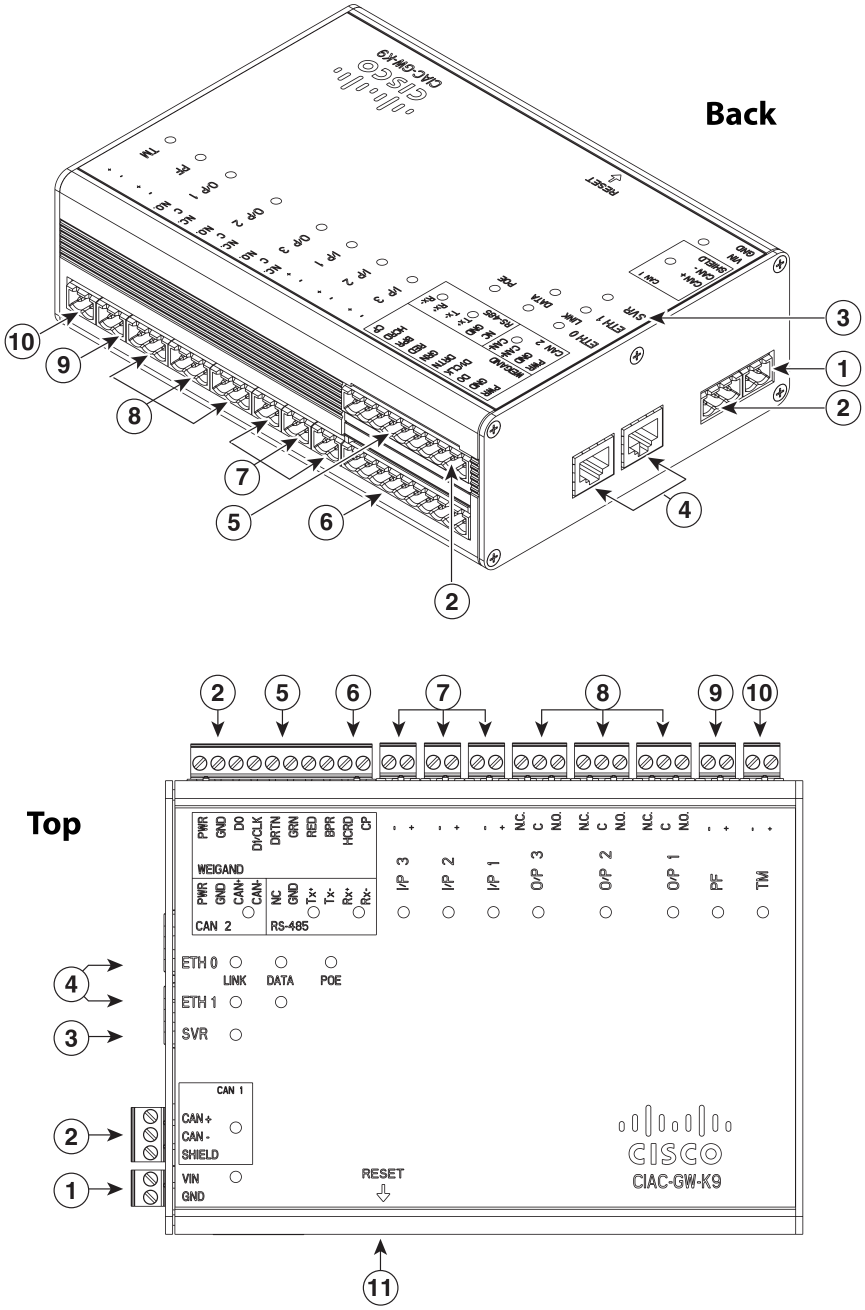


Figure 34: Cisco Gateway Back and Top Views with Labels

The elements of this diagram are described below.

1	Power – Two-pin connector for Voltage In (VIN) and Ground (GND) to connect a 12 to 24 VDC external power source.
2	CAN – A three-wire CAN bus used to connect additional modules, including the Cisco Reader Module, Cisco Input Module, and Cisco Output Module. *Note: Modules using this bus are not currently supported in ICPAM.*
3	SVR (Server) – When the LED is steady green, the Gateway is connected to a ICPAM server.
4	Fast Ethernet interface – There are two 10/100 BASE-TX RJ-45 connectors: • **ETH 0**: connects the Gateway to the network. ETH 0 also supports Power over Ethernet (PoE) for the device (optional). • **ETH 1**: connects the device to a PC to access the device configuration web page.
5	Serial interface – The RS-485 interface is not supported in this release.
6	Wiegand interface – This interface can be configured as the following: • One 10-pin Wiegand/clock and data reader interface to connect a single door reader. • Two 5-pin Wiegand/clock and data interfaces to connect two door readers (for installations where a 5-pin interface is sufficient). *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*
7	Input interfaces – Three input interfaces used to sense the contact closure. Each input can be configured as supervised or unsupervised and can be configured to sense a Normally Open (NO) or Normally Closed (NC) contact. • 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. • 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).

8	Output Interfaces – Three Form C (5A @ 30V) relay output interfaces. Each output connection can be configured as either Normally Closed (NC) or Normally Open (NO). C & NO connection: The relay is normally open. The circuit is closed when triggered. C & NC connection: The relay is normally closed. The circuit is opened when triggered. **Notes:** • Install surge protection between the output device and the ICPAM module, as described in Installing Surge Suppressors on Output Device Connections. • Common (C) is always used, and either NC or NO is used to complete the connection. • 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, disconnect all Generic Output devices and do the following: - Connect Normally Open devices to the N.O. and C connectors on the Gateway, Reader, or Output module. - Connect Normally Closed devices to the N.C. and Connectors on the Gateway, Reader, or Output module
9	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 port. An unsupervised input indicates only normal or alarm. The corresponding LED is red when circuit is open (when no input is connected)
10	TM – Tamper input: an unsupervised input that raises a "tamper" alarm when the circuit is open. Can be configured as an additional unsupervised port. An unsupervised input indicates only normal or alarm. The corresponding LED is red when circuit is open (when no input is connected).
11	Reset – Resets the device.

Installing the Gateway

To install a Cisco Gateway for use with ICPAM, follow these instructions.

1. Unpack and mount the Cisco Gateway.

   Each Cisco Physical Access Gateway includes the following:

   - Six End-Of-Line (EOL) 1K termination resistors (used for supervised input interfaces)
   - Two mounting brackets with 4 screws for each bracket
   - Regulatory compliance and safety information
   - Quick Start guide

- Connector plugs including the following:

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.

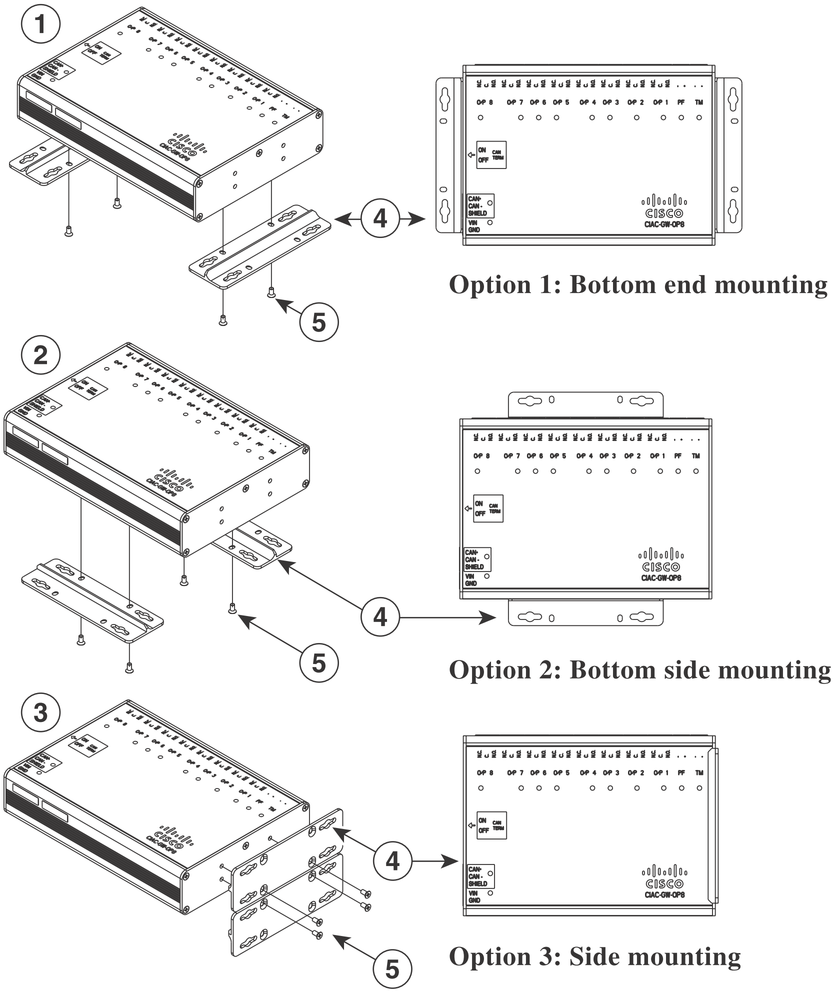


Figure 35: Three Options for Installing Module Wall Brackets

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 as shown in Figure 36.

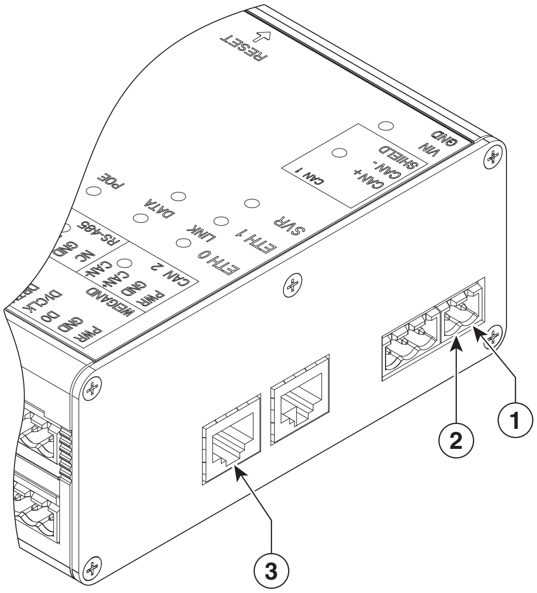


Figure 36: Gateway Power Connections

1	DC power / GND (ground) – Connects the DC ground wire to the Gateway.
2	DC power / Voltage In (VIN) – Connects the DC Voltage In (VIN) wire to the Gateway.
3	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 available power requirements 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 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.

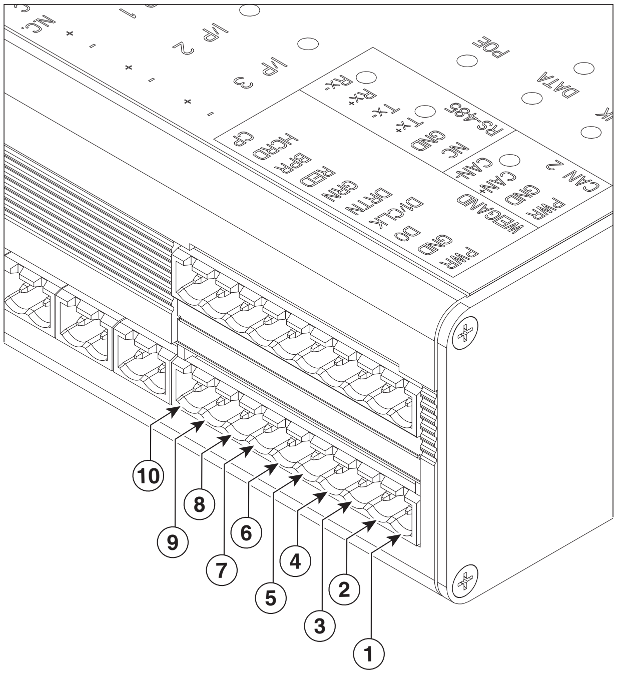


Figure 37: Wiegand Interface on Gateway and Reader Modules

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

	Chassis Label	Description	1 Reader 10-wire Connection	First Reader 5-wire Connection	Second Reader 5-wire Connection
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	HRCD	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 (NC) and Normally Open (NO) input connection.

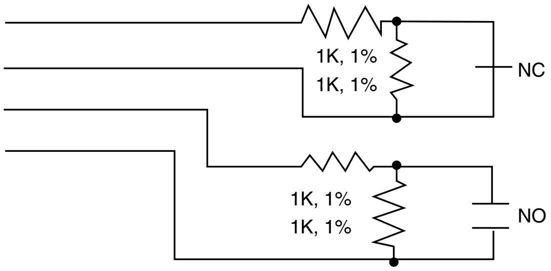


Figure 38: Input Connections: Cisco Physical Access Gateway Input and Reader Modules

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

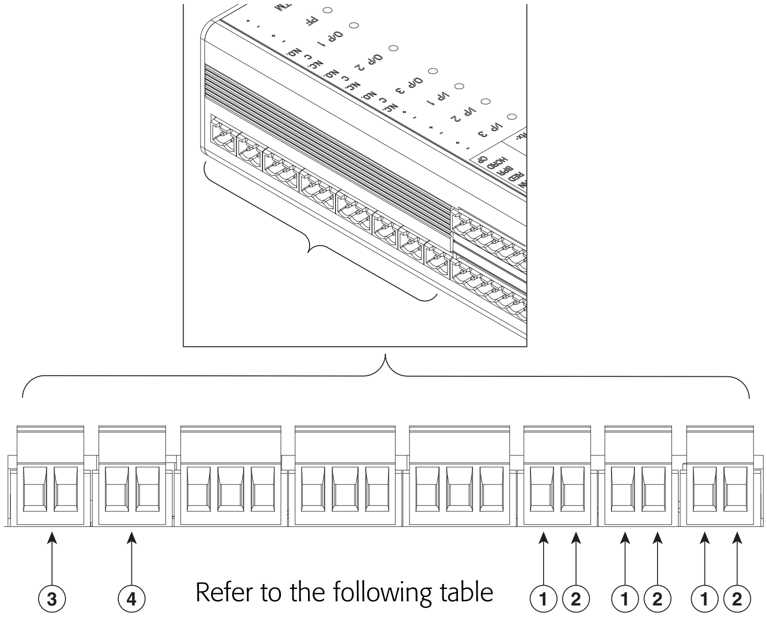


Figure 39: Input Connections: Cisco Physical Access Gateway and Reader Module

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 input device using the Cisco Physical Access Manager. An unsupervised input indicates only normal or alarm. The corresponding LED is red when 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 port. An unsupervised input indicates only normal or alarm. The corresponding LED is red when circuit is open (when no input is connected).

☞ ***Each of the input connections can be configured as 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 (Figure 40 on page 38). Each of the three Form C (5A @ 30V) relay output connections can be configured as either Normally Closed (NC) or Normally Open (NO).
   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 NC or NO is used to complete the connection.
      – If the relay is normally open, use the C & NO connections. The circuit is closed when triggered.
      – If the relay is normally closed, use the C & NC connections. The circuit is opened when triggered.

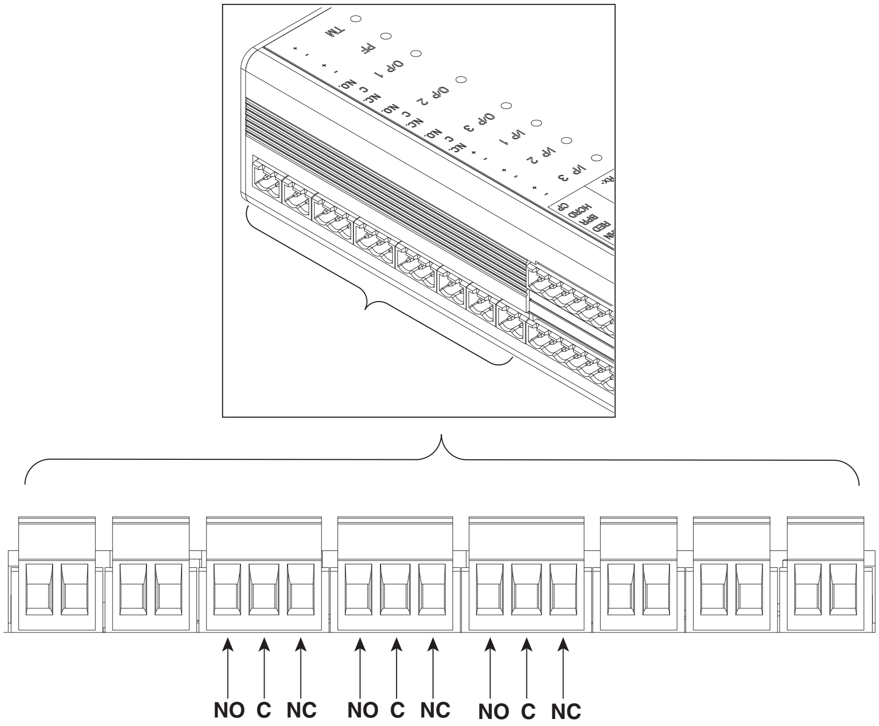
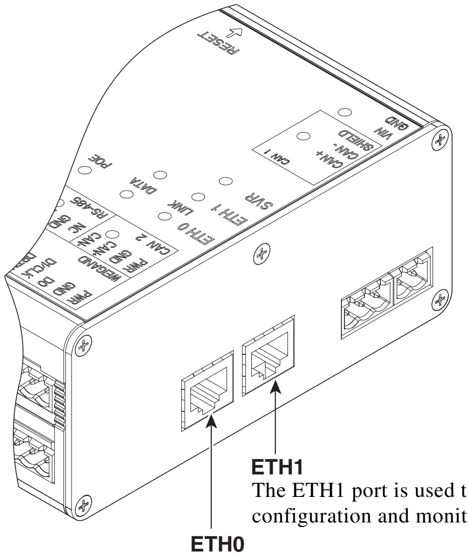


Figure 40: Output Connections: Cisco Physical Access Gateway and Reader Module

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



ETH1
The ETH1 port is used to connect a PC to the Gateway for configuration and monitoring.

ETH0
The ETH0 connection can also be used for Power over Ethernet.

Figure 41: ETH 0 Ethernet Connection for the Cisco Physical Access Gateway

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

10. Continue to "Configuring the Gateway" on page 39.

Configuring the Gateway

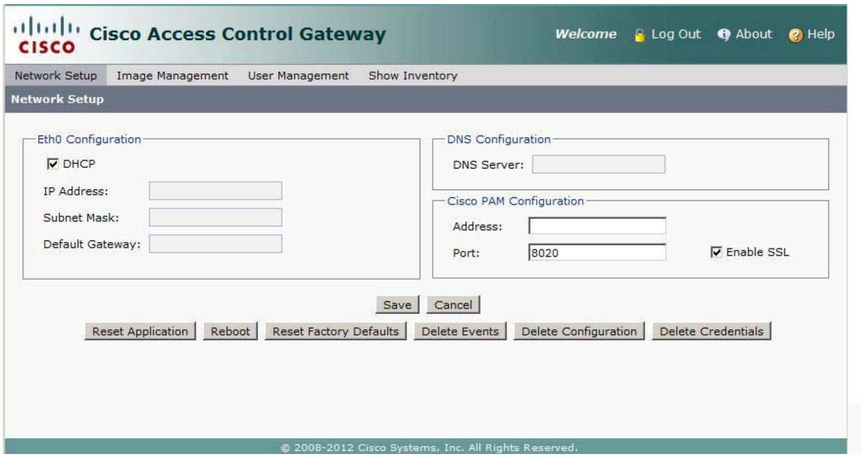
Once the gateway has been wired to its attached devices and mounted in an appropriate location, it is time to configure the gateway so that ICPAM can discover and use it.

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. Enter the default username and password:

   default username: `gwadmin`

   default password: `gwadmin`
4. Enter the Network settings, as shown in Figure 42.



Network Setup

Eth0 Configuration

☑ DHCP

IP Address:

Subnet Mask:

Default Gateway:

DNS Configuration

DNS Server:

Cisco PAM Configuration

Address:

Port: 8020

☑ Enable SSL

Figure 42: Network Settings for the Cisco Access Control Gateway

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:

IP address	Enter the IP address of the Cisco Gateway.
Subnet Mask	Enter the subnet mask.
Gateway	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 is 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 screen 'Network Settings Applied'. Changes do not take effect until 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*.

EM-100 Controller Configuration Instructions

The instructions for installing and configuring the EM-100 are shown in the following sections.

Controller Specifications

The following table provides relevant specifications for the EM-100 controller.

Dimensions	6.1″ W x 4.8″ H x 1.5″ D (154.9 mm x 122.5 mm x 37.1 mm)
Weight	11.3oz (320g)
Mounting Holes	US double-gang, US single-gang, and EU/APAC 60mm
Housing Material	UL94 polycarbonate
Audio / Visual Indicators	Two LEDs on RJ-45 port for network; beeper for 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 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)
Input Power	
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
Output Power (MAX) for total system (all field devices)	
DC Input @ PoE	9.6W
DC Input @ AUX	+12VDC 14.4W
DC Input @ AUX	+24VDC 28.8W
Hi-O CANbus Output	
Voltage, DC Input = PoE	24VDC
Hi-O CANbus Output	
Voltage, DC Input = AUX	AUX +VDC
Output Power (max) for individual field devices, DC Input = PoE	
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)
Output Power (MAX) for individual field devices, DC Input = 12VDC	
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)
Output Power (MAX) for individual field devices, DC Input = 24VDC	
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)
Relay Rating	
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.

Device	Conditions	Typical Operational Current

Door Position Switch
(For example, Securitron MSS)
	Vin = 12VDC
	Vin = 24VDC
		15mA
		15mA

Mag Lock
(For example, Securitron M32)
	Vin = 12VDC
	Vin = 24VDC
		300mA
		150mA

REX Switch
(For example, Securitron EEB)
	Vin = 12VDC
	Vin = 24VDC
		28mA
		38mA

iCLASS Wiegand Reader	Vin = 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.

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

The following calculations provide load current computations.

$$I_{total}\ @\ 12VDC = 15mA + 300mA + 28mA + 150mA = 493mA$$
$$I_{total}\ @\ 24VDC = 15mA + 150mA + 38mA + 150mA = 353mA$$

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

Device	Port	Conditions	V_{out}	I_{out}
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.

Impact on a Network

The EM-100 controller uses standard TCP and UDP packets to send and receive data from the host server and other EM-100 controllers. An EM-100 controller utilizes 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. This Alias IP address is only accessible through a direct connection since this address is in a non-routable range of IP addresses.

DHCP

A DHCP network can be used only if the addresses designated for the one or more 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.

Static IP Address

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

Firewall Configuration

When installing the EM-100 Host controller to communicate through a firewall, a requirement may be to configure the firewall to allow TCP data transfer on the specified port(s). If all communications are originated from the EM-100 (default configuration), modify the firewall if strict outbound rules are implemented.

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

- connection port (4050 default)
- listen 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, manager or consult your firewall user/installation manual.

For a table of default port values available for the EM-100, refer to the following table.

CAUTION ***Without configuring the firewall properly, the controller may not communicate with the server/host.***

Default Services and Ports

Out of the box, a controller has the following ports open. Modify or shut-off these ports to make the controller more secure.

Network Port	Description
TCP 20/21	FTP
TCP 22	Secure Shell (SSH/SCP) only on R2.3.1 units
TCP 23	Telnet
TCP 80/443	Web Server/SSL Web Server (R2.2.7.145+ and R2.3.1 units)
TCP 4050	Controller Listening Port
TCP 4070	Controller Connection Port
UDP 4070	Discovery GUI Communication Port
UDP 9000	Peer to Peer Communication Port
IP 169.254.242.121	Alias IP Address used for Direct Connect Configuration
Linux root Login	For web (R227 only), telnet, ftp, and ssh (R231 only)

Installation Instructions

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

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

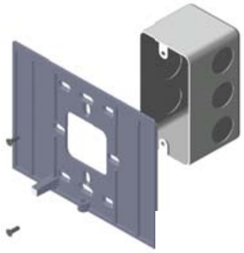


Figure 43: Installing Faceplate for EM-100 Controller

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

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

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

Figure 44 illustrates the most commonly used connections.

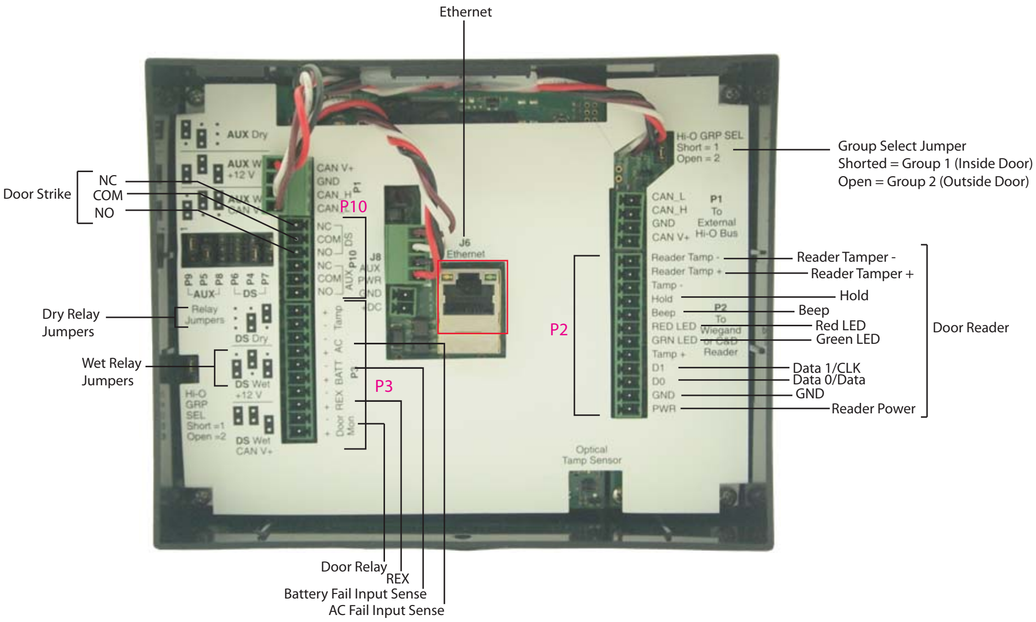


Figure 44: Wiring EM-100 Controller

The most important wiring and setup instructions include:

a. Set relay jumpers for either wet or dry as required.
   - Wet can be set to either12V or 24V
   - Dry can be set to either open or closed

b. Specify whether this door is inside (Group 1) or outside (Group 2) by setting the Group Select jumper.
   When Identiv introduces an extra I/O module, it will be enabled by this jumper. You can also add a second reader to the EM-100 with an I/O module and use the jumper to identify it as the exit reader or second door.

c. Unpack and mount any input or output modules as required. This includes 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 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 Mon – the default behavior of this input is managing the status of the door (open or closed)
   - REX – Default behavior of this input is masking the alarm and momentarily triggering output 1 (door strike)
   - AC – Default behavior is monitoring the AC power connection; if the AC power is lost, the controller will beep like a smoke detector (quiet beeps) without a battery
   - Battery – Default behavior is monitoring the battery power; if battery power is lost, the controller will beep like a smoke detector (quiet beeps) 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.

3. Connect power to the EM-100.

   When using PoE, install a UL294-compliant PoE injector between the Ethernet switch or router and the controller.

   Figure 45 on page 47 shows a sample wiring diagram incorporating several elements including an optional power supply and an optional strike (assuming that PoE is used).

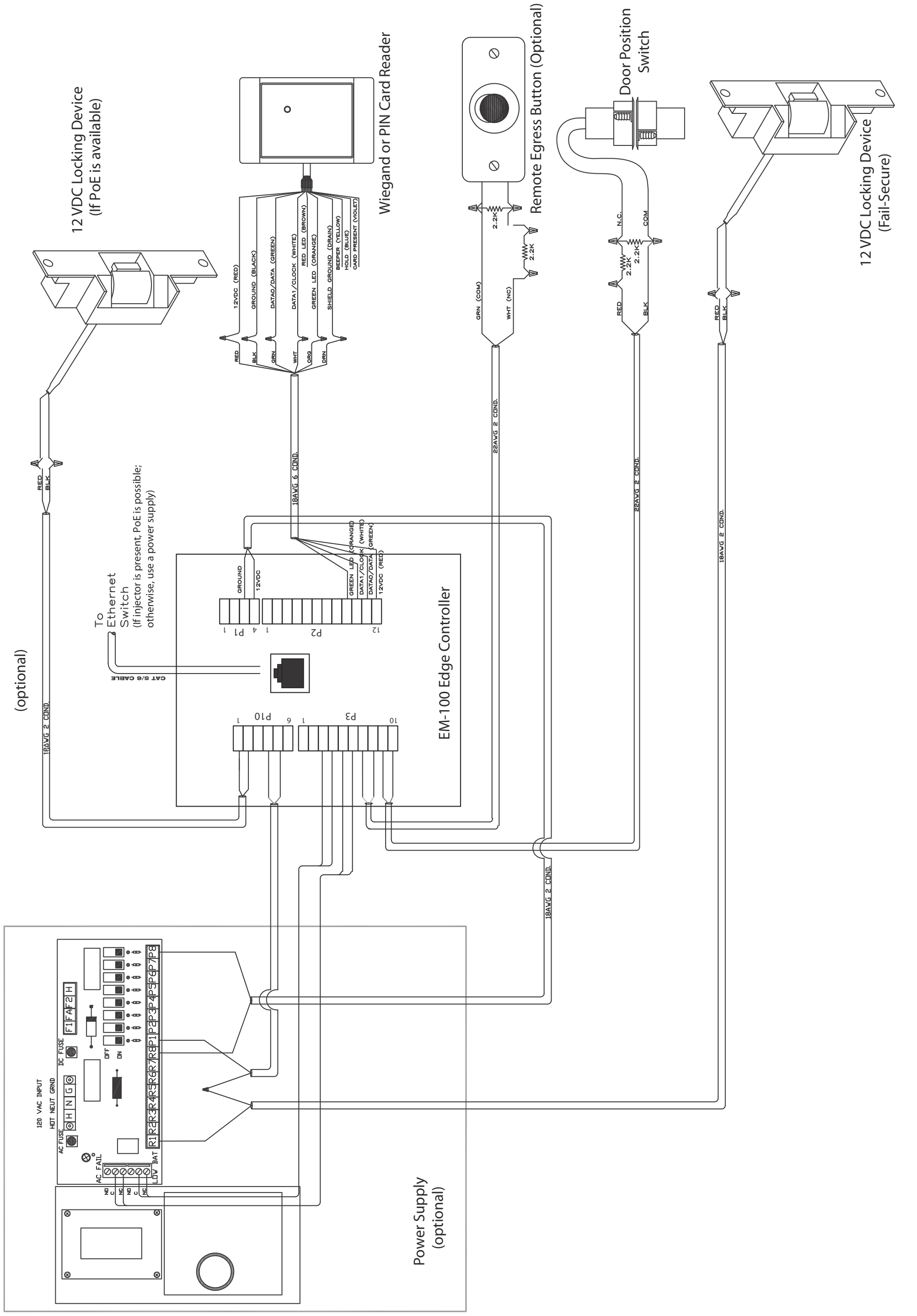


Figure 45: EM-100 Wiring Sample

Hint In most installations, a conventional power supply is used since 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 on the mounting plate, securing it with a screw at the bottom.
5. Connect a computer directly to the RJ-45 socket on the EM-100 using an Ethernet cable.
6. At the configuring computer’s desktop, click **Start** > **Run**.

☞ ***The computer being used to configure the EM-100 must be using Windows XP, Windows 2000, or Windows 7 in order to complete the configuration. Also, the computer must be connected to a network using a fixed address. DHCP will not function properly unless a reserved address is used.***

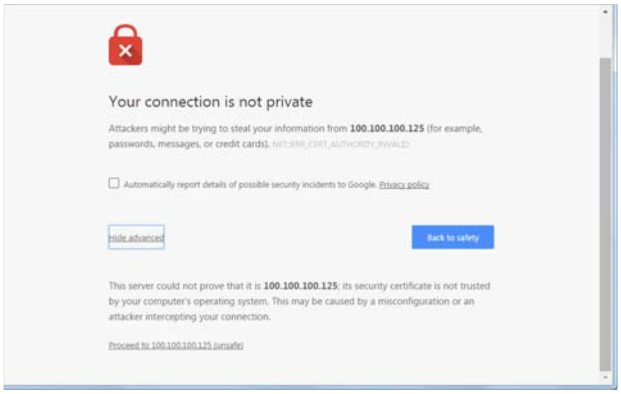
7. At the prompt, enter:

```
ipconfig /renew
```

then click **Enter**.

8. Access a web browser on the connected computer and enter **https://169.254.242.121** in the URL field.

The web browser prompts that this is not a private connection.



Your connection is not private

Attackers might be trying to steal your information from **100.100.100.125** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically report details of possible security incidents to Google. Privacy policy

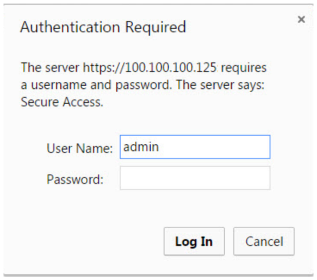
This server could not prove that it is **100.100.100.125**; its security certificate is not trusted by your computer’s operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 100.100.100.125 (unsafe)

Figure 46: EM-100 Configuration Warning

9. Click the ‘Proceed to 169.254.242.121 (unsafe)’ link at the bottom of the window.

An ‘Authentication Required’ window appears.



Authentication Required

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

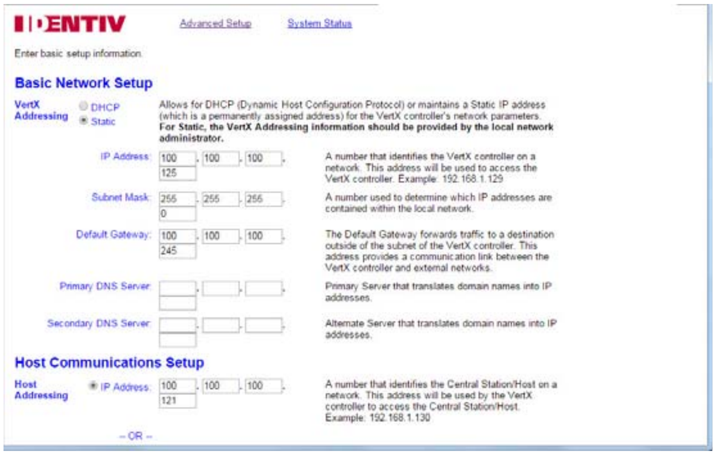
User Name: admin

Password:

Figure 47: EM-100 Configuration Authentication Required

10. From the Login window User Name field, enter **admin**.
11. At the Password field, enter **identiv123** and click **Log In**.

    The Basic Network Setup screen appears.



Enter basic setup information.

Basic Network Setup

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

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

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

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

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

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

Host Communications Setup

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

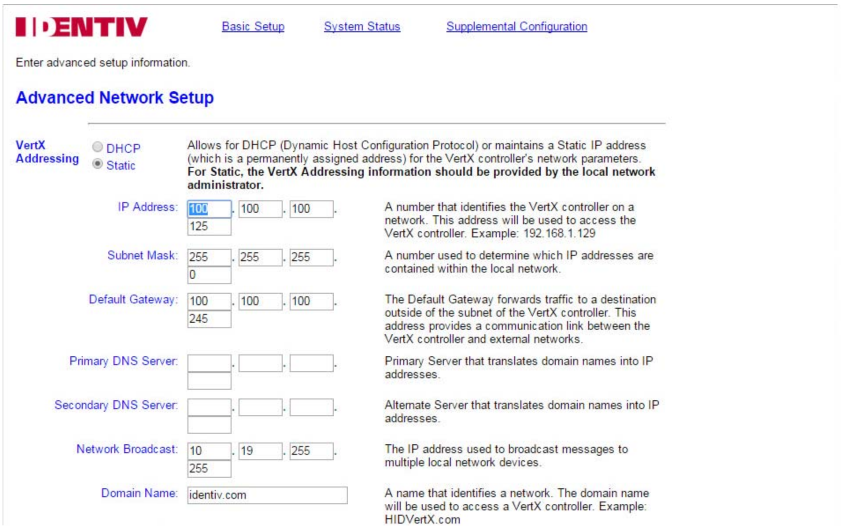
-- OR --

Figure 48: EM-100 Basic Network Setup

Each field is defined briefly on the left column of the setup screen.

12. Click the **Advanced Setup** link up at the top of this window.

    The Advanced Setup window appears.



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.

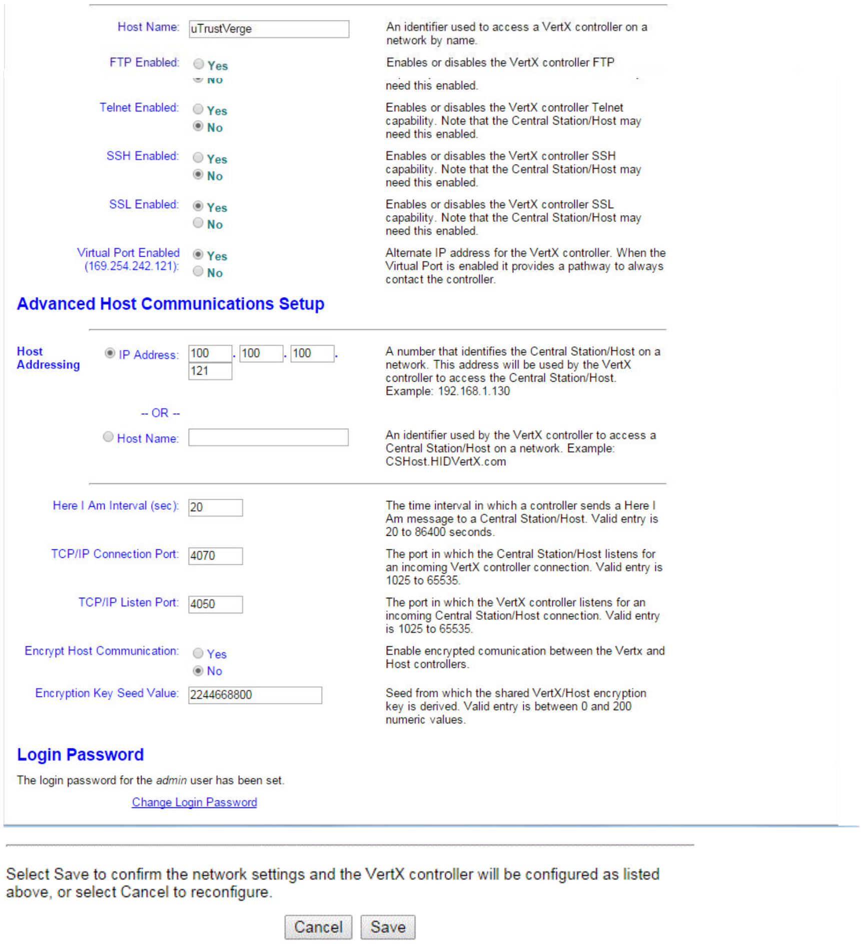
Network Broadcast: 10 . 19 . 255 . 255 — The IP address used to broadcast messages to multiple local network devices.

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 49: EM-100 Advanced Network Setup 1

13. Change or enter values for these fields:
    - Click the **Static** radio button. The EM-100 must be provided with a fixed address. DHCP does not function properly with the EM-100.
    - 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



Host Name:	uTrustVerge	An identifier used to access a VertX controller on a network by name.
FTP Enabled:	○ Yes No	Enables or disables the VertX controller FTP need this enabled.
Telnet Enabled:	○ Yes ● No	Enables or disables the VertX controller Telnet capability. Note that the Central Station/Host may need this enabled.
SSH Enabled:	○ Yes ● No	Enables or disables the VertX controller SSH capability. Note that the Central Station/Host may need this enabled.
SSL Enabled:	● Yes ○ No	Enables or disables the VertX controller SSL capability. Note that the Central Station/Host may need this enabled.
Virtual Port Enabled (169.254.242.121):	● Yes ○ No	Alternate IP address for the VertX controller. When the Virtual Port is enabled it provides a pathway to always contact the controller.

Advanced Host Communications Setup

Host Addressing	● IP Address:	100 . 100 . 100 . 121	A number that identifies the Central Station/Host on a network. This address will be used by the VertX controller to access the Central Station/Host. Example: 192.168.1.130
	-- OR --		
	○ Host Name:		An identifier used by the VertX controller to access a Central Station/Host on a network. Example: CSHost.HIDVertX.com

Here I Am Interval (sec):	20	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.
TCP/IP Connection Port:	4070	The port in which the Central Station/Host listens for an incoming VertX controller connection. Valid entry is 1025 to 65535.
TCP/IP Listen Port:	4050	The port in which the VertX controller listens for an incoming Central Station/Host connection. Valid entry is 1025 to 65535.
Encrypt Host Communication:	○ Yes ● No	Enable encrypted comunication between the Vertx and Host controllers.
Encryption Key Seed Value:	2244668800	Seed from which the shared VertX/Host encryption key is derived. Valid entry is between 0 and 200 numeric values.

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.

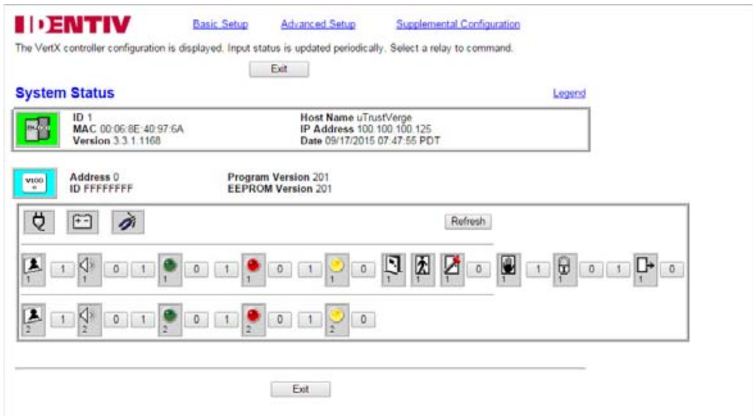
Figure 50: EM-100 Advanced Network Setup 2

- At the ‘Host Name’ field, enter the identifier used to access the controller
- Enable or disable radio buttons for the next five items as required. Unless otherwise required, the recommended settings are:

FTP Enabled	**No**
Telnet Enabled	**No**
SSH Enabled	**No**
SSL Enabled	**Yes**
Virtual Port Enabled	**Yes**

- At the ‘Host Addressing’ field, enter the IP address that identifies the central station or host on the network. Alternatively, click the ‘Host Name’ radio button and supply the identifier used by the controller to access the central station or host on the network.
- Leave the other advanced host communication settings as 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.



The VertX controller configuration is displayed. Input status is updated periodically. Select a relay to command.

System Status

ID 1
MAC 00:06:8E:40:97:6A
Version 3.3.1.1168

Host Name uTrustVerge
IP Address 100.100.100.125
Date 09/17/2015 07:47:55 PDT

Address 0
ID FFFFFFFF

Program Version 201
EEPROM Version 201

Figure 51: EM-100 Controller Status

Click the **Legend** link at 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.

14. Click **Exit** to leave the EM-100 setup program.
15. Once configuration is completed, disconnect the Ethernet cable between the configuring computer and the EM-100, then reconnect the network cable routed through the EM-100 faceplate to the EM-100’s RJ-45 socket.

Resetting the EM-100 Network Configuration to Factory Defaults

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

Resetting the network defaults requires access to the EM-100 controller back plate. Once 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 52.

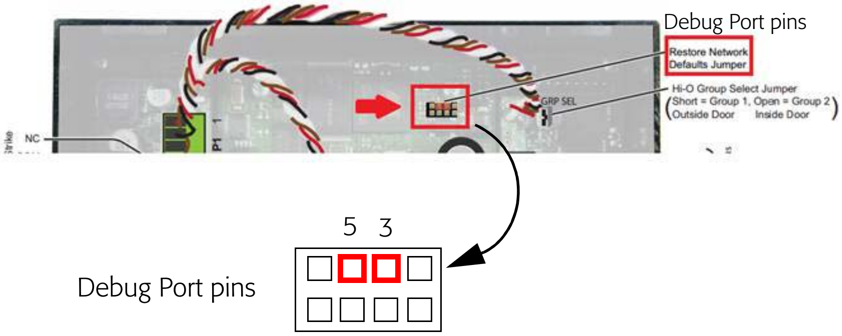


Figure 52: Debug Port Jumper Pins

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. Once 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, all network configuration information is overwritten and returned to the original defaults.***

8. Configure the controller for your installation parameters.
9. Reinstall the EM-100 mylar and back plate.

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