



Identiv Connected Physical Access Manager 3.0 Installation Guide

February, 2017

Identiv, Inc.
www.identiv.com

Copyright © 2017 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

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: 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 CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression 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. CISCO 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 CISCO 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 CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright © 2015 Cisco Systems, Inc. All rights reserved.

Contents

Contents	iii
ICPAM Server Installation Instructions	1
Preparations for Server Installation.....	1
Installing VMware	1
Deploying the OVA file	2
Launching the CPAM Server Virtual Machine for the First Time	2
Obtaining Super-user Privilege	5
Configuring the ICPAM Server	7
Configuring ICPAM Server	11
Configuring the ICPAM Server	13
Installing the ICPAM Client	24
Controller and Gateway Installation Instructions.....	29
Cisco Physical Access Gateway Configuration Instructions	29
Installing the Gateway.....	32
Configuring the Gateway	39
EM-100 Edge Controller Configuration Instructions.....	42
Door Peripherals Operational Currents	42
Compute and Compare Overall Current Draw	42
Installation Instructions	43
Mx Controller Configuration Instructions.....	50
Components of the Mx Controller	50
Mx Controller Main Board	51
Internal Power Supply	53
Standby Battery	54
Tamper Switch	54
Expansion Boards	54
Data Capacity of an Mx Controller.....	55
Replaceable Parts of the Mx Controller	56
M64 Controller Design	57
M64 Controller Battery Standby Capacity.....	58
Design Considerations for the Mx Controller.....	59
Electrical Ratings	59
Mx Controller Design	59
Separation of Circuits.....	60
Controller Battery Standby Capacity	62
Power Provided at the Terminal Blocks.....	63
ScramblePad/MATCH2 Power Requirements.....	63
Typical Connections	65
Wiring for a Door.....	66
Typical Line Module Inputs	67
Typical Door Relay Outputs	68
ScramblePad/MATCH Inputs	70
Power Requirements for Various Devices	72
Wiring Diagram for the TS-8010 Reader.....	76
Wiring Diagram for the TS-8110 Reader.....	78
Setup and Installation of an Mx Controller.....	79
Mounting the Controller.....	79

Wiring to the Controller	80
Connecting Line Module Inputs	81
Connecting Outputs	83
Connecting ScramblePad and MATCH Interfaces.....	84
Wiring Distance Limits	86
Configuring the Integrated SNIB3	86
SNIB3 Network Configuration Options.....	90
Deploying the SNIB3	91
Preparing an Mx Controller to Use a SNIB3.....	92
Mx Controller Configuration Worksheet	92
Performing Periodic Maintenance.....	93
Gathering Diagnostic Information.....	94
Interpreting the System Power Status Information	94
Replacing the Memory Battery	95

List of Figures

Figure 1: VMware Settings for OVA File	2
Figure 2: Software Updates Message	3
Figure 3: VMware vSphere Client.....	3
Figure 4: VMware Console Window.....	4
Figure 5: Username Field Sign-In	4
Figure 6: Password Field	5
Figure 7: RHEL Console Screen	5
Figure 8: Terminal Command Line Window	6
Figure 9: Super-User Permissions Command Line	6
Figure 10: Root Prompt Command Line	7
Figure 11: Root Prompt Commands	7
Figure 12: vi Text Editor ifcfg-eth0 File Example	8
Figure 13: Enter Insert Mode.....	9
Figure 14: Running service network restart.....	10
Figure 15: Running service immortal restart.....	10
Figure 16: ICPAM Server Login Window	11
Figure 17: ICPAM Server Administrator Starting Page.....	12
Figure 18: ICPAM Server Administration User Page	13
Figure 19: ICPAM Administrator Network Page	14
Figure 20: ICPAM Administrator DNS Page	16
Figure 21: ICPAM Administrator Email Page	16
Figure 22: ICPAM Administrator Date & Time Page.....	17
Figure 23: ICPAM Administrator Event Page (Pruning Subpage)	18
Figure 24: Server Administrator Event Archive Page	20
Figure 25: ICPAM Administrator License Page	22
Figure 26: ICPAM Server Login Dialog Box with ICPAM Client Link	24
Figure 27: ICPAM Downloads Page	25
Figure 28: Client Installation Welcome Page	26
Figure 29: Target Path Page	26
Figure 30: ICPAM Client Installation	27
Figure 31: Client Log In Dialog Box.....	27
Figure 32: Welcome Page of the ICPAM Client	28
Figure 33: Cisco Physical Access Gateway.....	29
Figure 34: Cisco Gateway Back and Top Views with Labels	30
Figure 35: Three Options for Installing Module Wall Brackets.....	33
Figure 36: Gateway Power Connections	34
Figure 37: Wiegand Interface on Gateway and Reader Modules.....	35
Figure 38: Input Connections: Cisco Physical Access Gateway Input and Reader Modules	36
Figure 39: Input Connections: Cisco Physical Access Gateway and Reader Module	37
Figure 40: Output Connections: Cisco Physical Access Gateway and Reader Module.....	38
Figure 41: ETH 0 Ethernet Connection for the Cisco Physical Access Gateway	39
Figure 42: Network Settings for the Cisco Access Control Gateway	40
Figure 43: Installing Faceplate for EM-100 Controller	43
Figure 44: Wiring EM-100 Controller.....	43
Figure 45: EM-100 Wiring Sample	45
Figure 46: EM-100 Configuration Warning	46
Figure 47: EM-100 Configuration Authentication Required.....	46
Figure 48: EM-100 Basic Network Setup	47
Figure 49: EM-100 Advanced Network Setup 1	47
Figure 50: EM-100 Advanced Network Setup 2	48

Figure 51: EM-100 Controller Status.....	49
Figure 52: Mx Controller Components (in Secure Enclosure)	51
Figure 53: Mx Controller Main Board Connectors and Components	52
Figure 54: M64 Controller	57
Figure 55: Cable Inlets of the Mx Controller's Enclosure.....	61
Figure 56: Current Draw Orientation for MATCH2 Interface	64
Figure 57: Typical Line Module Input Connection	67
Figure 58: Typical Door Relay Connection.....	68
Figure 59: ScramblePad/MATCH Inputs	70
Figure 60: Current Draw Orientation.....	72
Figure 61: Typical Door Wiring Example for an Mx Controller.....	75
Figure 62: Wiegand Door Wiring Example for an Mx Controller	76
Figure 63: Typical Line Module Input Connection	81
Figure 64: Typical Output Connection	83
Figure 65: Typical ScramblePad/MATCH Input Connection	85

ICPAM Server Installation Instructions

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 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 Edge 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
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.

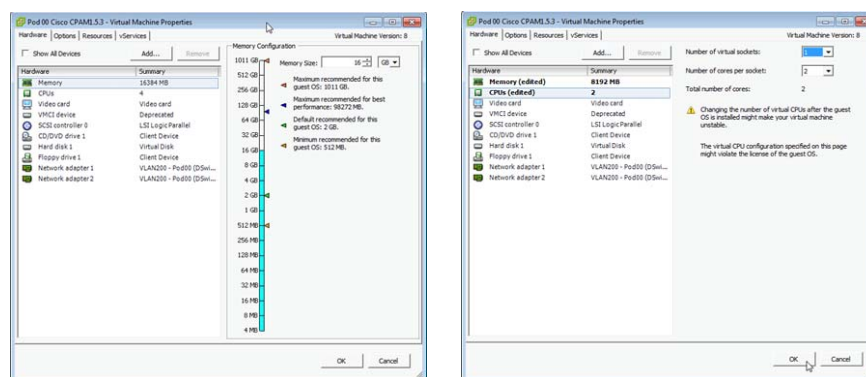


Figure 1: VMware Settings for OVA File

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**.

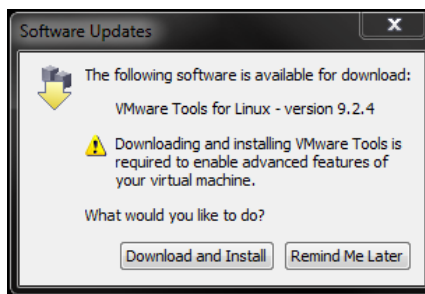


Figure 2: Software Updates Message

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**.



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.

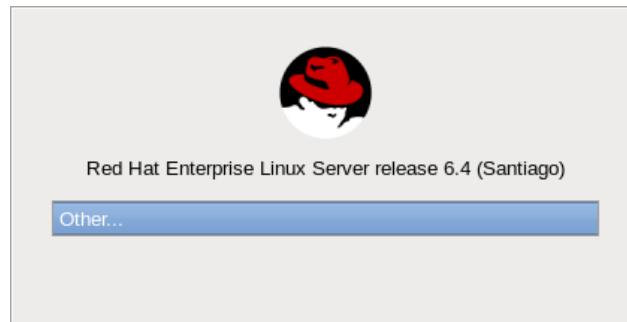


Figure 4: VMware Console Window

 *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.

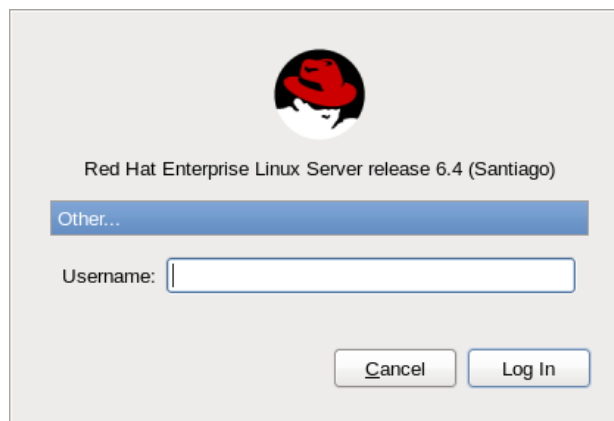


Figure 5: Username Field Sign-In

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

The password screen appears.

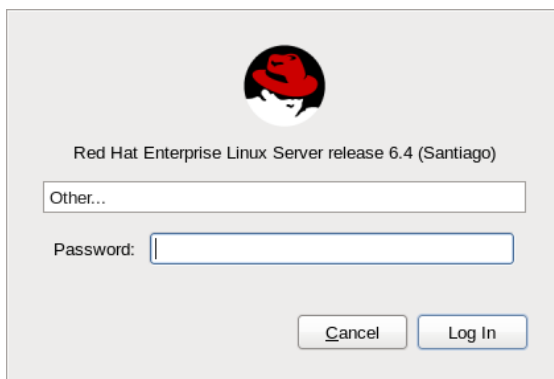


Figure 6: Password Field

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

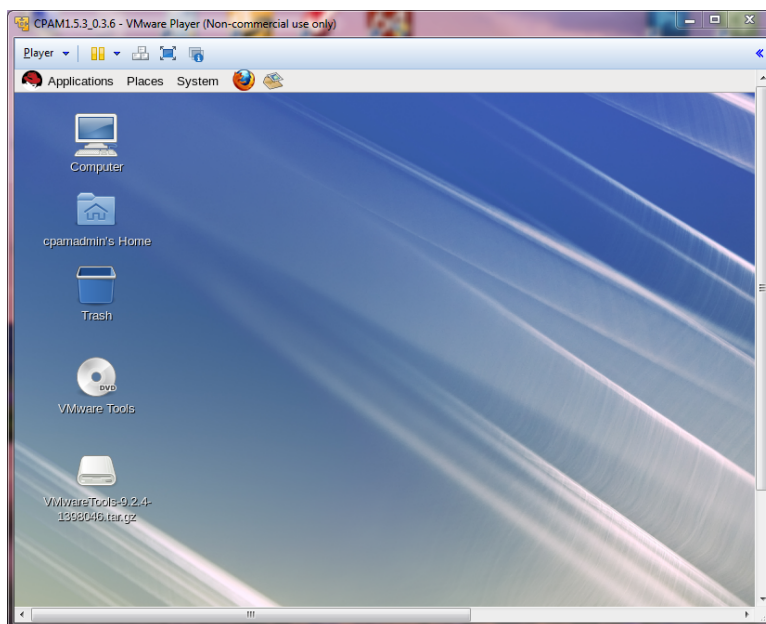


Figure 7: RHEL Console Screen

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.

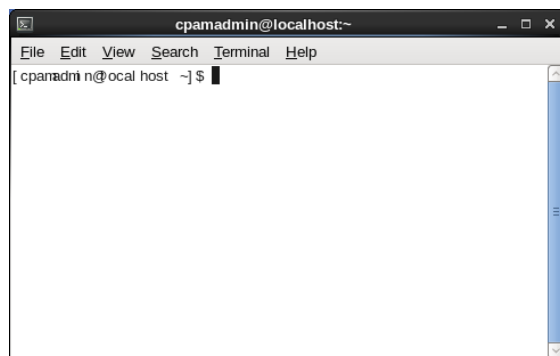


Figure 8: Terminal Command Line Window

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.

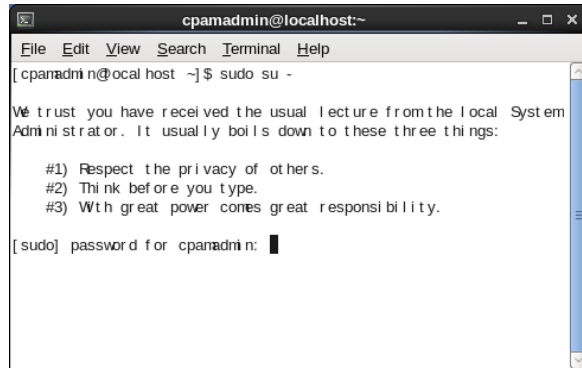


Figure 9: Super-User Permissions Command Line

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:


```

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

```

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.***

Configuring the ICPAM Server

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/cpanadmin/ifcfg-eth0 /etc/sysconfig/network-scripts/`
 where there is a space 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`
4. Press **Enter** again.

```

root@localhost:~
File Edit View Search Terminal Help
[cpanadni n@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:

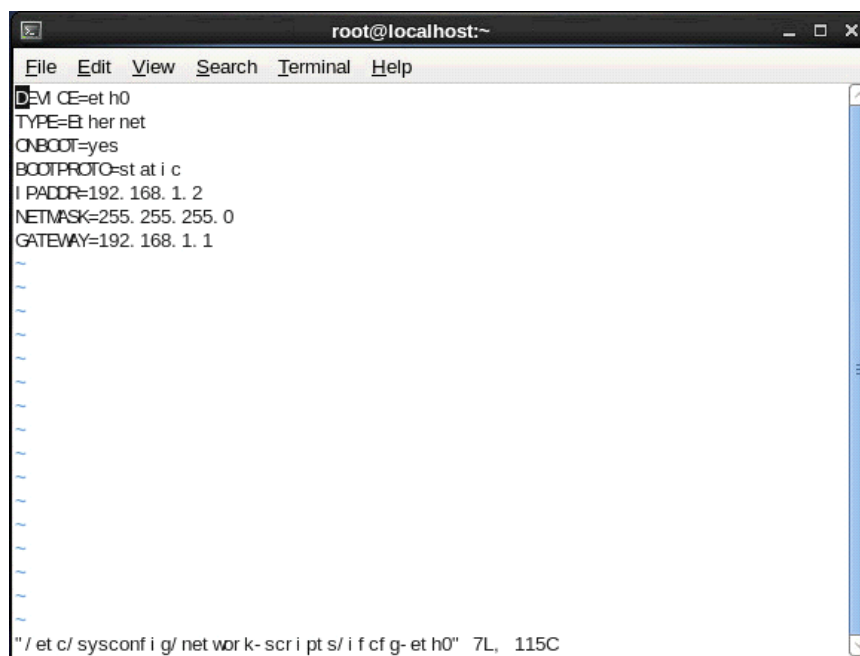
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for cpanadni n:
[r root@ocal host ~]# cp /home/cpanadni n/i f c f g- e t h0 / e t c/ s y s c o n f i g/ n e t w o r k- s c r i p t s
[r root@ocal host ~]# vi / e t c/ s y s c o n f i g/ n e t w o r k- s c r i p t s/ i f c f g- e t h0

```

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).



The screenshot shows a terminal window with the vi text editor open. The window title is "root@localhost:~". The editor's menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The content of the file being edited is as follows:

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

Below the parameters are several tilde (~) characters representing empty lines. At the bottom of the editor, the status bar displays: `"/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).

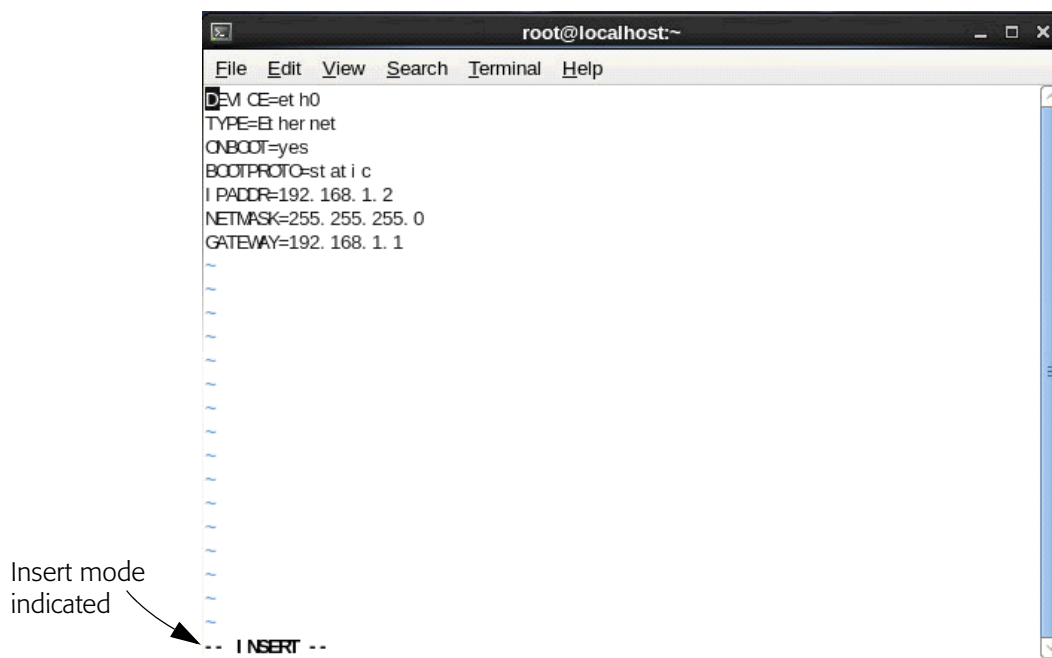


Figure 13: Enter Insert Mode

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 IPADDR 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.

```

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:
[root@ocal host ~]# cp /home/cpanadmin/ifcfg-eth0 /etc/sysconfig/network-scripts
[root@ocal host ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
[root@ocal host ~]# service network restart
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
[root@ocal host ~]# █

```

Figure 14: Running service network restart

- Restart the cpamadmin service by typing:
`service immortal restart`

As shown in Figure 15.

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@ocal host ~]# service immortal restart  
Stopping cpanadmi n.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..  
Sending the cpanadmi n processes a SIGTERM asking them to shut down gracefully..  
Waiting for processes to exit..  
Waiting for processes to exit..  
  
Starting Immortal...  
Sleeping for 10 seconds to start the immortal  
Successfully Started..  
[root@ocal host ~]#
```

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. From the root prompt, run this command:

```
shutdown /r now
```

 This reboots the server.
 The ICPAM server application is now ready for launch.


Configuring 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.



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.



The screenshot shows the 'Initial Setup' page of the ICPAM Server Administration interface. The page has a header with the 'ENTIV' logo and 'Connected PAM Server Administration' text. On the right, there are links for 'Welcome', 'Log Out', 'About', and 'Help'. A 'Setup Steps' sidebar on the left lists steps 1 through 8, with '1 - Server' selected. The main content area contains fields for 'Version:' (2.0.0(0.3.0)), 'Serial Number:' (A46C2A65AD54), 'Type:' (Active Server), and 'Site Name:'. At the bottom right, there are 'Back', 'Next >', and 'Cancel' buttons.

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 the ICPAM Server", starting on page 13.

Configuring the ICPAM Server

To configure the ICPAM server 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.

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.

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. The 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 the check box to enable or disable DHCP. When DHCP is enabled, the IP address fields in this tab are disabled, as the 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.

ENTIV Connected PAM Server Administration

Welcome Log Out About Help

Webapp Log Show Tech

Setup Steps

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

Initial Setup

Primary DNS: 192.235.84.254

Secondary DNS: 192.235.84.1

Domain:

< Back Next > Cancel

Copyright © 2015 Identiv, Inc. All Rights Reserved.

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.

ENTIV Connected PAM Server Administration

Welcome Log Out About Help

Webapp Log Show Tech

Setup Steps

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

Initial Setup

SMTP Server Address:

SMTP Email Address from:

Test

< Back Next > Cancel

Copyright © 2015 Identiv, Inc. All Rights Reserved.

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.

The screenshot shows the 'Initial Setup' page for 'IDENTIV Connected PAM Server Administration'. On the left, a 'Setup Steps' sidebar lists: 1 - Server, 2 - User, 3 - Network, 4 - DNS, 5 - Email, 6 - Date & Time (selected), 7 - Event, and 8 - License. The main content area is titled 'Initial Setup' and contains the following fields: 'Date & Time' with a text input showing '06/16/15 09:21:39' and a calendar icon; 'Time Zone' with a dropdown menu showing 'America/Los_Angeles'; 'NTP Enable' with a checked checkbox; and 'NTP Server Address*' with a text input showing '0.north-america.pool.ntp.org'. At the bottom right of the form are three buttons: 'Back', 'Next', and 'Cancel'. The footer of the page reads 'Copyright © 2015 Identiv, Inc. All Rights Reserved.'

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.

MENTIV Connected PAM Server Administration

Welcome Log Out About Help

Setup Steps

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

Initial Setup

Webapp Log Show Tech

Pruning Archive

Live Event Window(days): 30

Schedule:

☐ Date:

☐ Week day:

☒ Daily:

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

Pruning Hours: 1.0

< Back Finish > Cancel

Copyright © 2013 Mentiv, Inc. All Rights Reserved.

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	<p>Define the time and frequency at which events should be pruned.</p> <p>These radio buttons are available:</p> <p>Date—To schedule pruning for one day per month, select Date and then select a day of the month. For example: 15.</p> <p>Weekday—To schedule pruning once per week, select Weekday and then select a day of the week. For example: Tuesday.</p> <p>Daily—To run pruning every day, select Daily.</p> <p>For other options in Schedule, the Pruning Hours field is read-only.</p>
Time	<p>Enter the time in 24 hour format (hh:mm:ss).</p> <p>For example, to run pruning at 2 p.m., enter 14:00:00.</p> <p>To run pruning at 1 a.m., enter 01:00:00.</p>
Pruning Hours	<p>This field is enabled only when you select Daily from the 'Schedule' field.</p> <p>The default value is 1.</p>



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.

The screenshot displays the 'Initial Setup' page for ICPAM 3.0. On the left, a 'Setup Steps' sidebar lists steps 1 through 8: 1 - Server, 2 - User, 3 - Network, 4 - DNS, 5 - Email, 6 - Date & Time, 7 - Event, and 8 - License. The 'Event' step is currently selected. The main area is titled 'Initial Setup' and contains two tabs: 'Pruning' and 'Archive'. The 'Archive' tab is active, showing fields for 'Password' and 'Re-enter Password' (both masked with asterisks), 'Historic Event Window(days)' set to 60, and a 'Schedule' section with radio buttons for 'Date', 'Weekday', and 'Daily' (which is selected). Below the schedule, there is a 'Time' field set to 01:01:00 and a checkbox for 'Copy to remote server'. At the bottom of the form are buttons for '< Back', 'Next >', and 'Cancel'. The footer of the page reads 'Copyright © 2015 Merit, Inc. All Rights Reserved.'

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

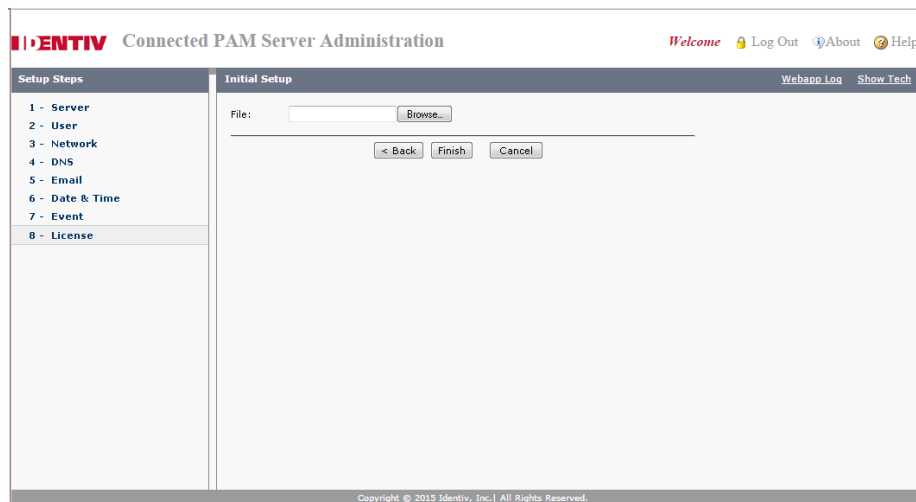





Figure 25: ICPAM Administrator License Page

-  *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 Edge controller.

Before continuing, install the Java 1.6 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 1.6 is not currently installed, go to <https://java.com/en/download/manual.jsp> and download version 1.6 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.



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

3. Login with the cpadmin 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.

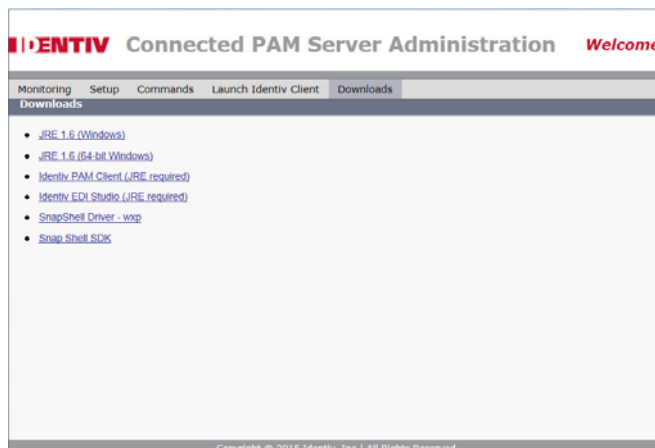


Figure 27: ICPAM Downloads Page

5. Click on the **JRE 1.6 (Windows)** link.
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.



Figure 28: Client Installation Welcome Page

12. Click **Next**.

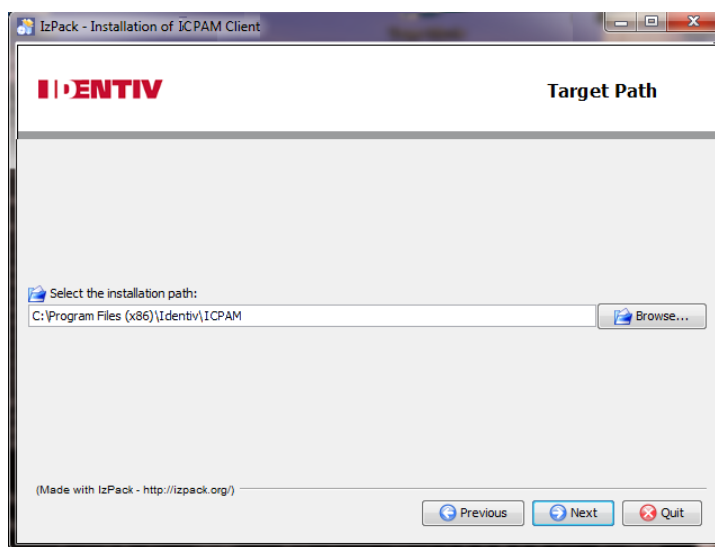


Figure 29: Target Path Page

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.

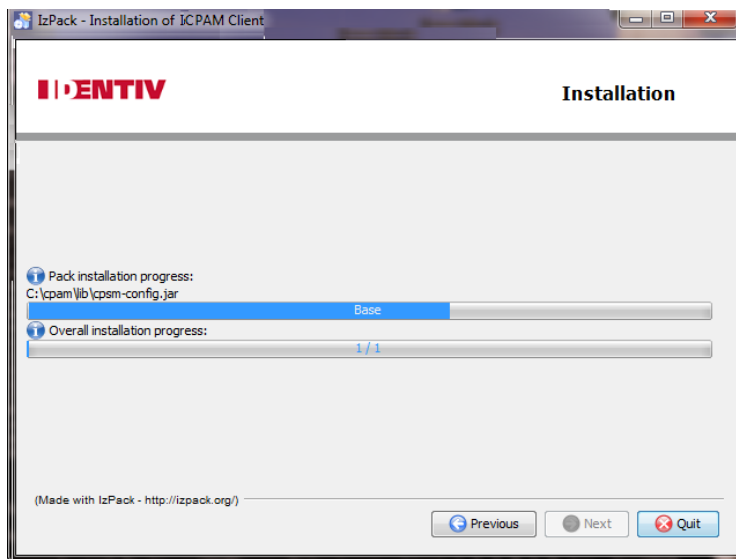


Figure 30: ICPAM Client Installation

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

The Log In dialog box appears:

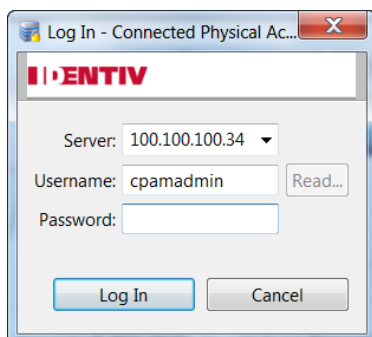


Figure 31: Client Log In Dialog Box

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

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

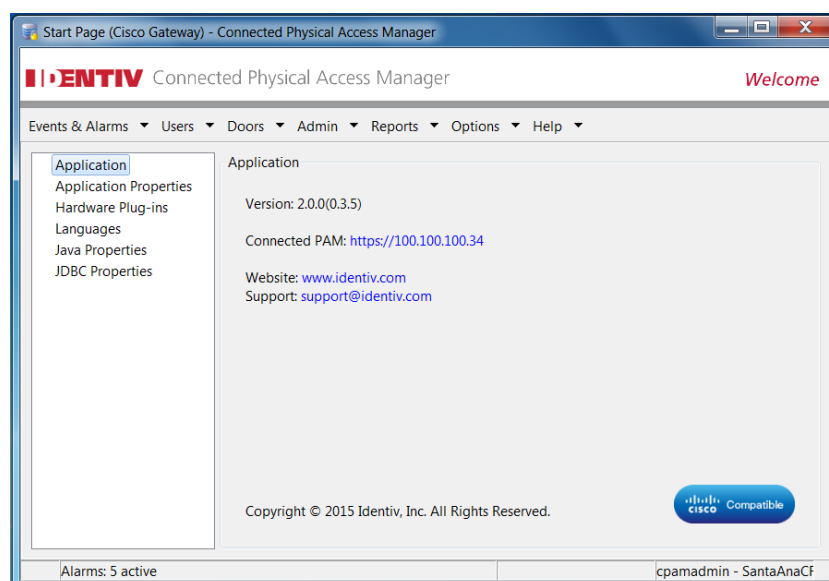


Figure 32: Welcome Page of the ICPAM Client

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
- Identiv EM-100 Edge Controllers

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.

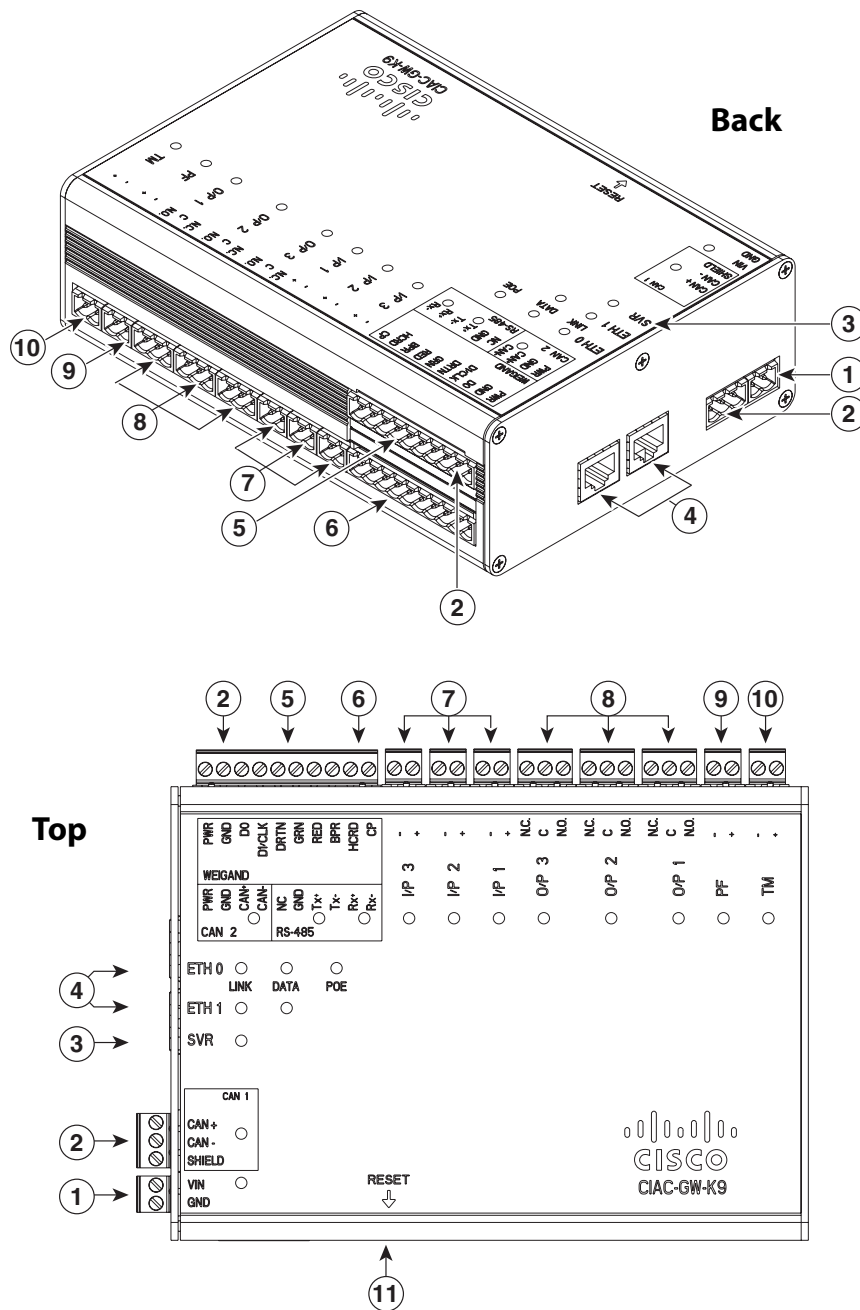


Figure 34: Cisco Gateway Back and Top Views with Labels

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. <i>Note: Modules using this bus are not currently supported in ICPAM.</i>
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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). <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>
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. <ul style="list-style-type: none"> • 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	<p>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).</p> <p>C & NO connection: The relay is normally open. The circuit is closed when triggered.</p> <p>C & NC connection: The relay is normally closed. The circuit is opened when triggered.</p> <p>Notes:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> - 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	<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 port. An unsupervised input indicates only normal or alarm. The corresponding LED is red when circuit is open (when no input is connected)</p>
10	<p>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).</p>
11	<p>Reset – Resets the device.</p>

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.

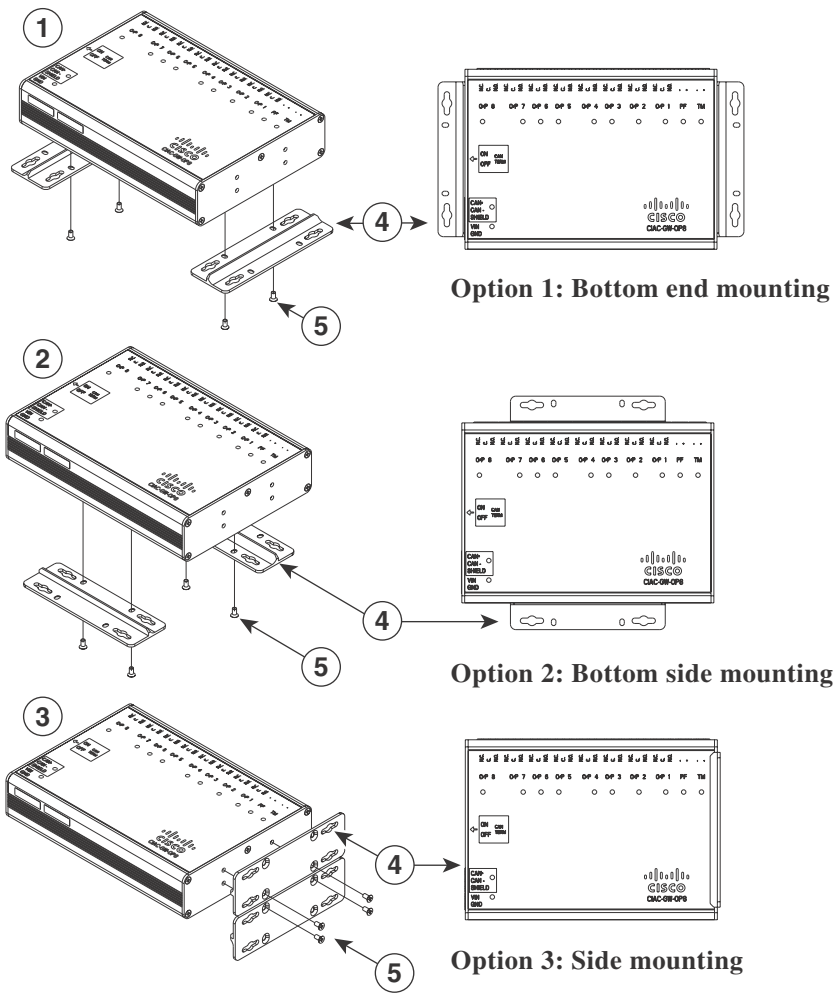


Figure 35: Three Options for Installing Module Wall Brackets

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.

Module	Current Draw Requirement	Notes
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.

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.

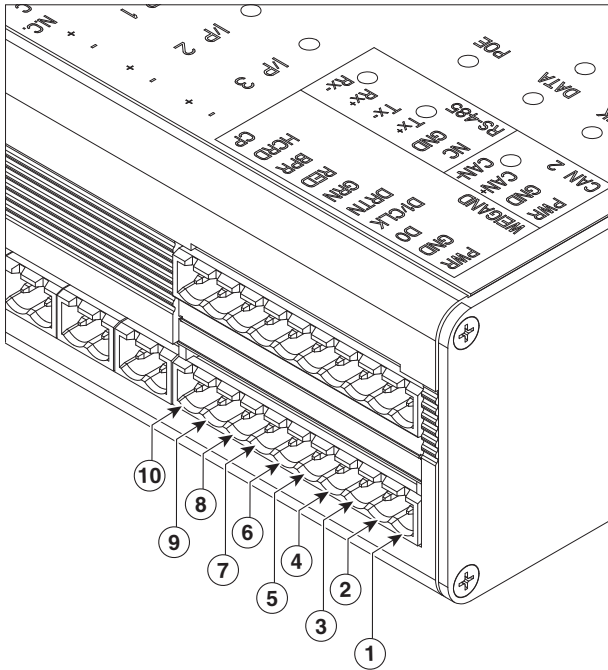


Figure 37: Wiegand Interface on Gateway and Reader Modules

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	HCRD	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.

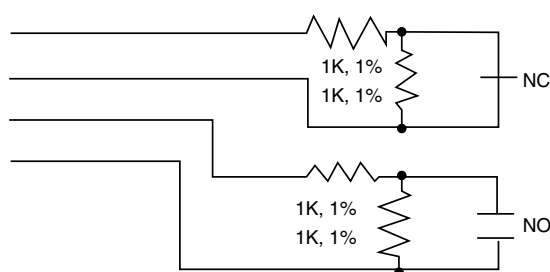


Figure 38: Input Connections: Cisco Physical Access Gateway Input and Reader Modules

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

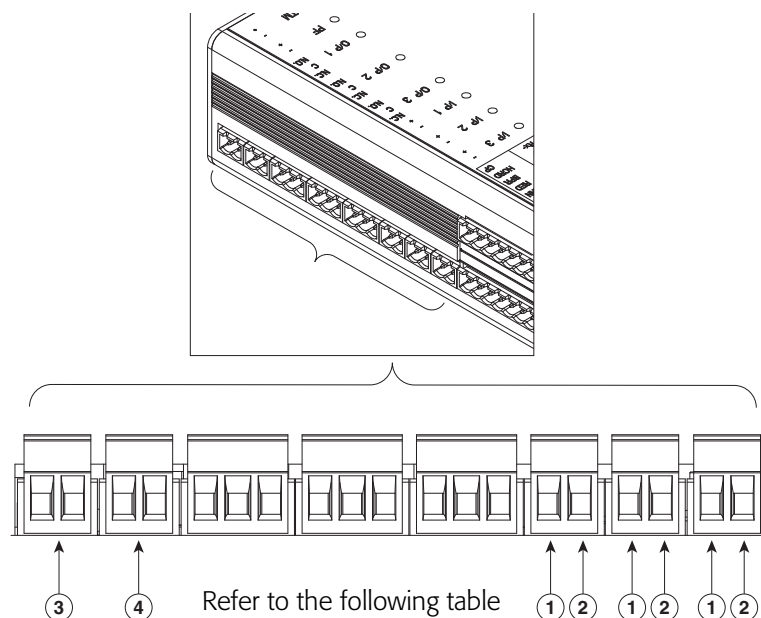


Figure 39: Input Connections: Cisco Physical Access Gateway and Reader Module

- 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). 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.

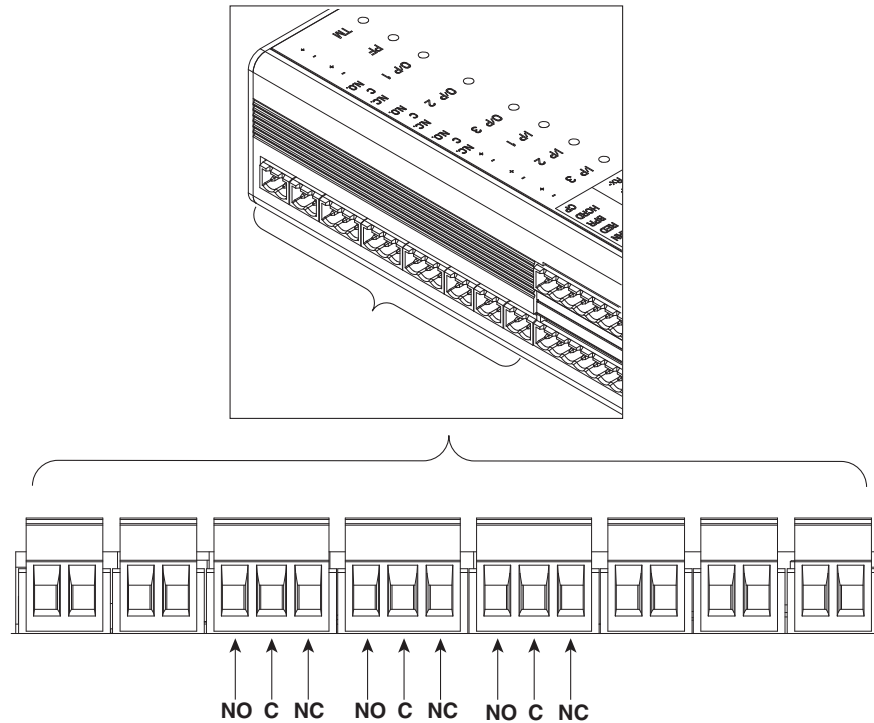


Figure 40: Output Connections: Cisco Physical Access Gateway and Reader Module

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

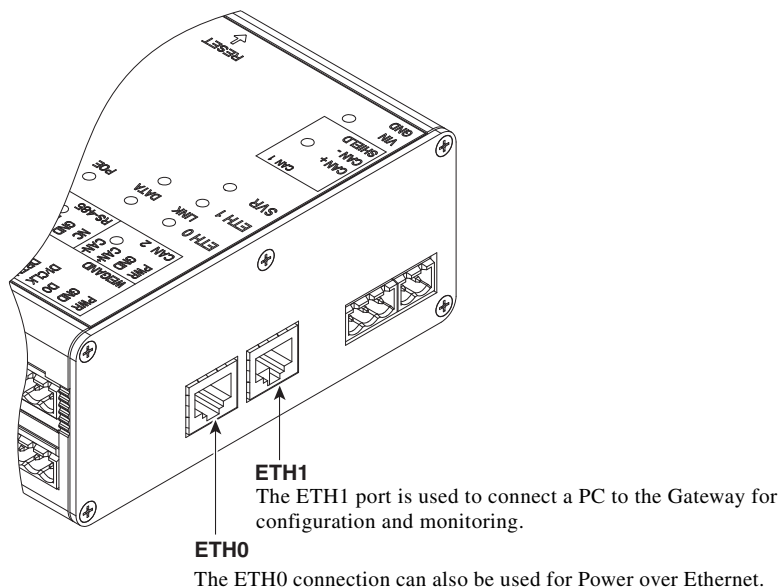


Figure 41: ETH 0 Ethernet Connection for the Cisco Physical Access Gateway

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.

The screenshot shows the 'Cisco Access Control Gateway' web interface. The 'Network Setup' tab is active. Under 'Eth0 Configuration', the 'DHCP' checkbox is checked, and there are input fields for 'IP Address', 'Subnet Mask', and 'Default Gateway'. Under 'DNS Configuration', there is a 'DNS Server' input field. Under 'Cisco PAM Configuration', there are input fields for 'Address' and 'Port' (set to 8020), and a checked 'Enable SSL' checkbox. At the bottom, there are buttons for 'Save', 'Cancel', 'Reset Application', 'Reboot', 'Reset Factory Defaults', 'Delete Events', 'Delete Configuration', and 'Delete Credentials'. The footer indicates '© 2008-2012 Cisco Systems, Inc. All Rights Reserved.'

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 Dynamic Host Configuration Protocol (DHCP) server is configured on your IP network, select the DHCP check box for ETH0 to automatically configure the required IP network settings, including IP address, Subnet Mask, and Gateway. 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 Edge Controller Configuration Instructions

Before installing the EM-100, first calculate the power requirements for the installation, including the controller and all attached components.

The physical dimensions of the EM-100 are:

6.1 W x 4.8 H x 1.5 D in. (154.9 x 122.5 x 37.1 mm)

Door Peripherals Operational Currents

For the door peripherals, consult the vendor data sheets to determine the operational current draw. Typical operational current draw is provided below.



See individual peripheral data sheets for actual operational current draw.

Device	Conditions	Typical Operational Current
Door Position Switch (For example, Securitron MSS)	V _{in} = 12VDC	15mA
	V _{in} = 24VDC	15mA
Mag Lock (For example, Securitron M32)	V _{in} = 12VDC	300mA
	V _{in} = 24VDC	150mA
REX Switch (For example, Securitron EEB)	V _{in} = 12VDC	28mA
	V _{in} = 24VDC	38mA
iCLASS Wiegand Reader	V _{in} = 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_{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.

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.

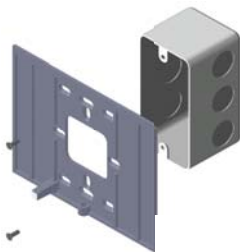


Figure 43: Installing Faceplate for EM-100 Controller

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.

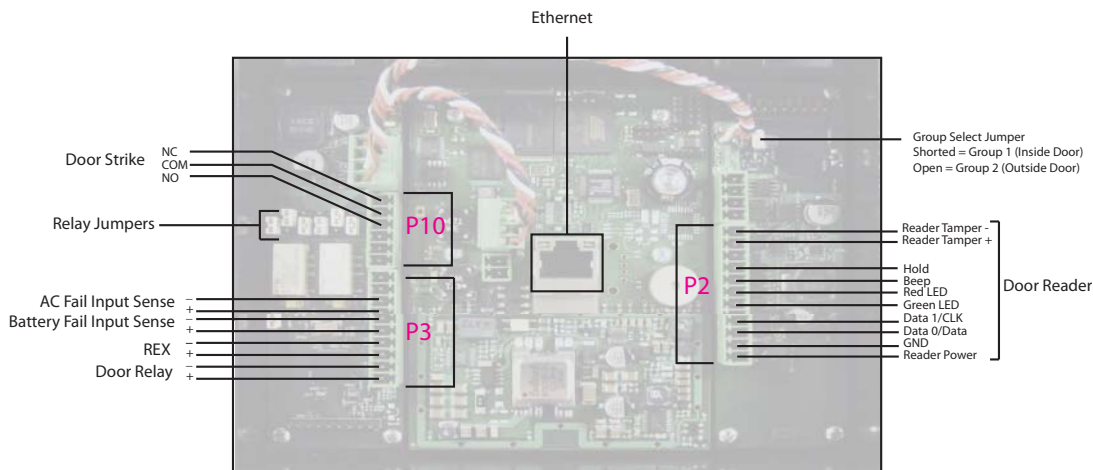


Figure 44: Wiring EM-100 Controller

The most important wiring and setup instructions include:

- a. Set relay jumpers as required.
- b. Specify whether this door is inside (Group 1) or outside (Group 2) by setting the Group Select jumper.
- 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).

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

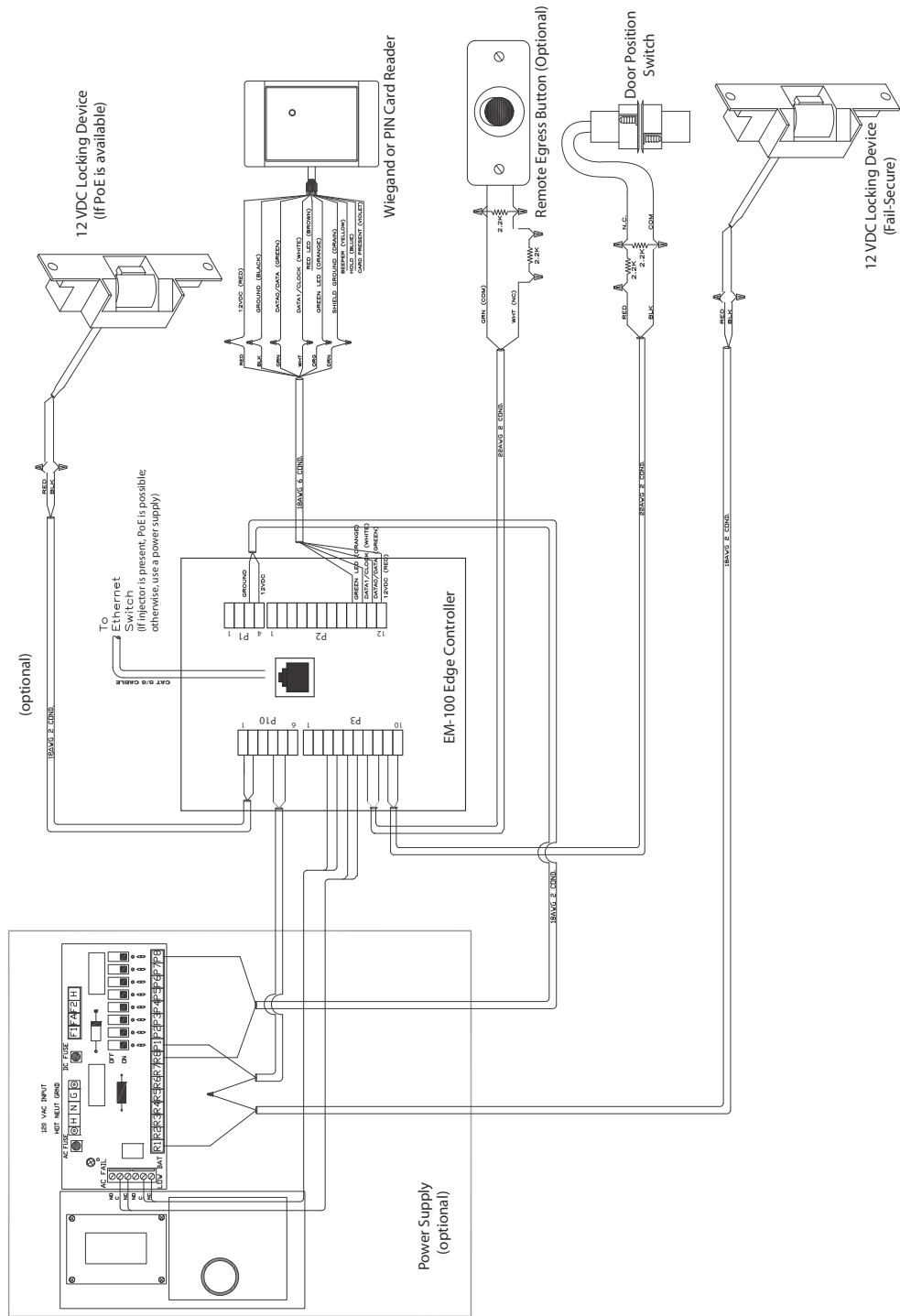


Figure 45: EM-100 Wiring Sample

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.

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.

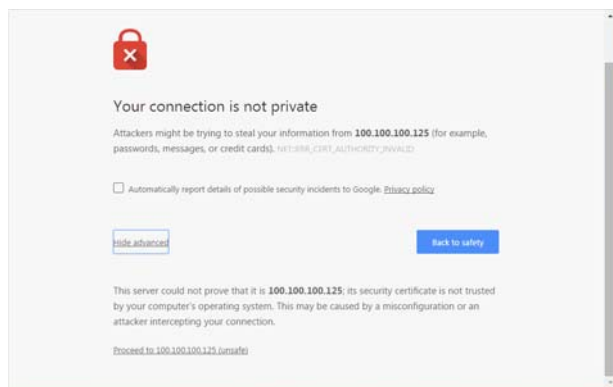


Figure 46: EM-100 Configuration Warning

9. Click the 'Proceed to 169.254.242.121 (unsafe)' link at the bottom of the window.
 An 'Authentication Required' window appears.

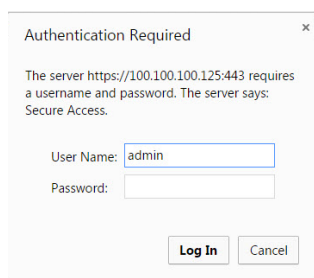


Figure 47: EM-100 Configuration Authentication Required

10. From the Login screen enter **identiv123**. Leave the Password field blank and click **Log In**.

The Basic Network Setup screen appears.

IDENTIV Advanced Setup System Status

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

Subnet Mask: 255.255.255.0

Default Gateway: 100.100.100.245

Primary DNS Server:

Secondary DNS Server:

Host Communications Setup

Host Addressing ☒ IP Address: 100.100.100.121

— OR —

Figure 48: EM-100 Basic Network Setup

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

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

The Advanced Setup window 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

Subnet Mask: 255.255.255.0

Default Gateway: 100.100.100.245

Primary DNS Server:

Secondary DNS Server:

Network Broadcast: 10.19.255.255

Domain Name: identiv.com

Figure 49: EM-100 Advanced Network Setup 1

12. Change or enter values for these fields:
 - Click the Static radio button. The EM-100 must be provided with a fixed address
 - 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:

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:

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):

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:

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:

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 communication between the Vertx and Host controllers.

Encryption Key Seed Value:

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.

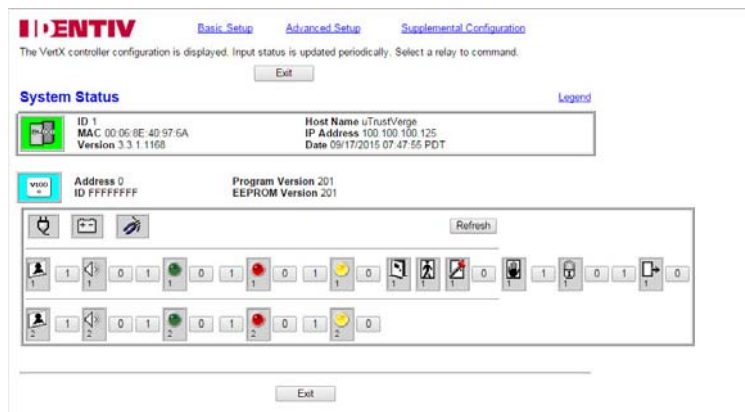


Figure 51: EM-100 Controller Status

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.

13. Click **Exit** to leave the EM-100 setup program.
14. 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.

Mx Controller Configuration Instructions

This chapter provides information about the Mx controller, including:

- Advantages of the Mx controller
- A summary of the different Mx controller configurations
- An overview of the Mx controller's main components
- Design considerations, including battery capacity and power limitations
- Typical connections, such as the wiring for a door
- Setup and installation, including wiring distance limits, and configuration of the integrated SNIB3 capability and the integrated Ethernet port
- A worksheet for an Mx Controller, to help you plan your security system. (Worksheets for other system components are provided in Appendix A.)
- Performing periodic maintenance

There are two Mx Controller configurations supported by ICPAM, which differ only in the number of supervised doors (including alarm inputs) and the capacity of the factory-equipped standby battery.

- The Mx-4 can control up to four doors, and has a 7.2 Ah standby battery.
- The Mx-8 can control up to eight doors, and has a 7.2 Ah standby battery.

The configuration is determined by the model of CCMx that is installed. This enables you to easily upgrade an Mx controller after its initial installation, without affecting the existing wiring. The number of readers and ScramblePads the controller can support is determined by:

- The number of addresses available (16 maximum) for ScramblePads and MATCH2 interfaces
- The total power required by ScramblePads and MATCH2 interfaces attached to the controller. This cannot exceed the power capacity of the controller. To calculate this capacity, see "Power Requirements for Various Devices" on page 72.

Components of the Mx Controller

An Mx-4 or Mx-8 Controller consists of several components in a secure enclosure, as shown in Figure 52 on page 51.

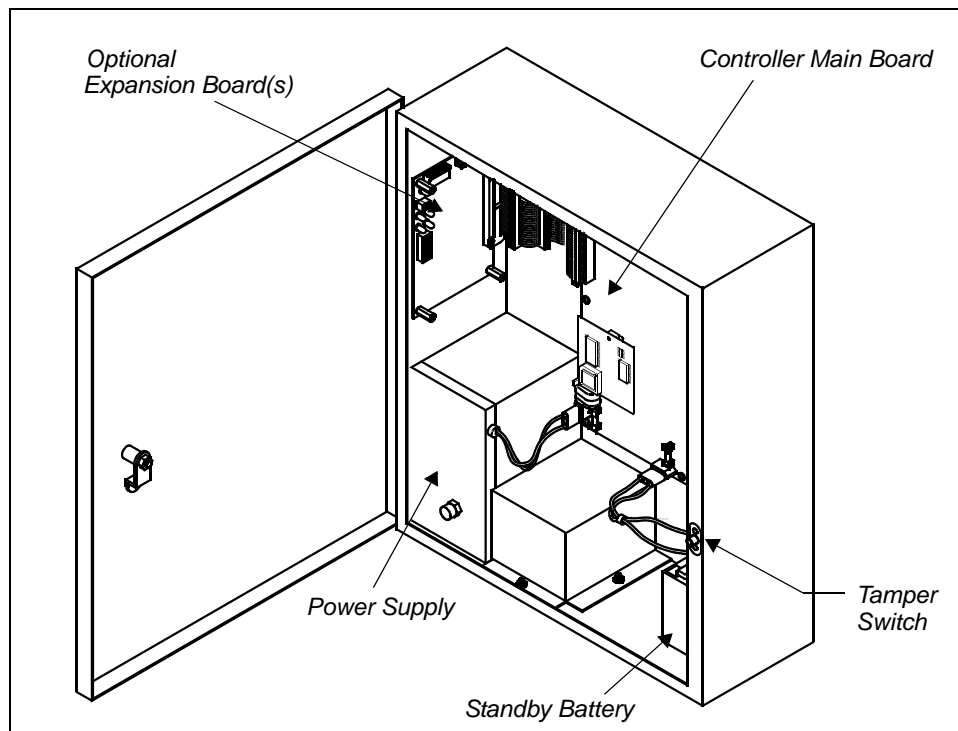


Figure 52: Mx Controller Components (in Secure Enclosure)

The Controller enclosure contains the following major components:

- Controller main board
- Power supply
- Standby battery
- Tamper switch
- Optional expansion boards

Each of these components is explained briefly.

Mx Controller Main Board

The Mx Controller Main Board contains the main connectors to the surrounding system. Through it, you can connect to ScramblePads, MATCH, and Wiegand reader interfaces, input devices, output devices, an Ethernet network, other controllers, and power sources.

The following figure shows the connectors (and other key components) of an Mx Controller's main board.

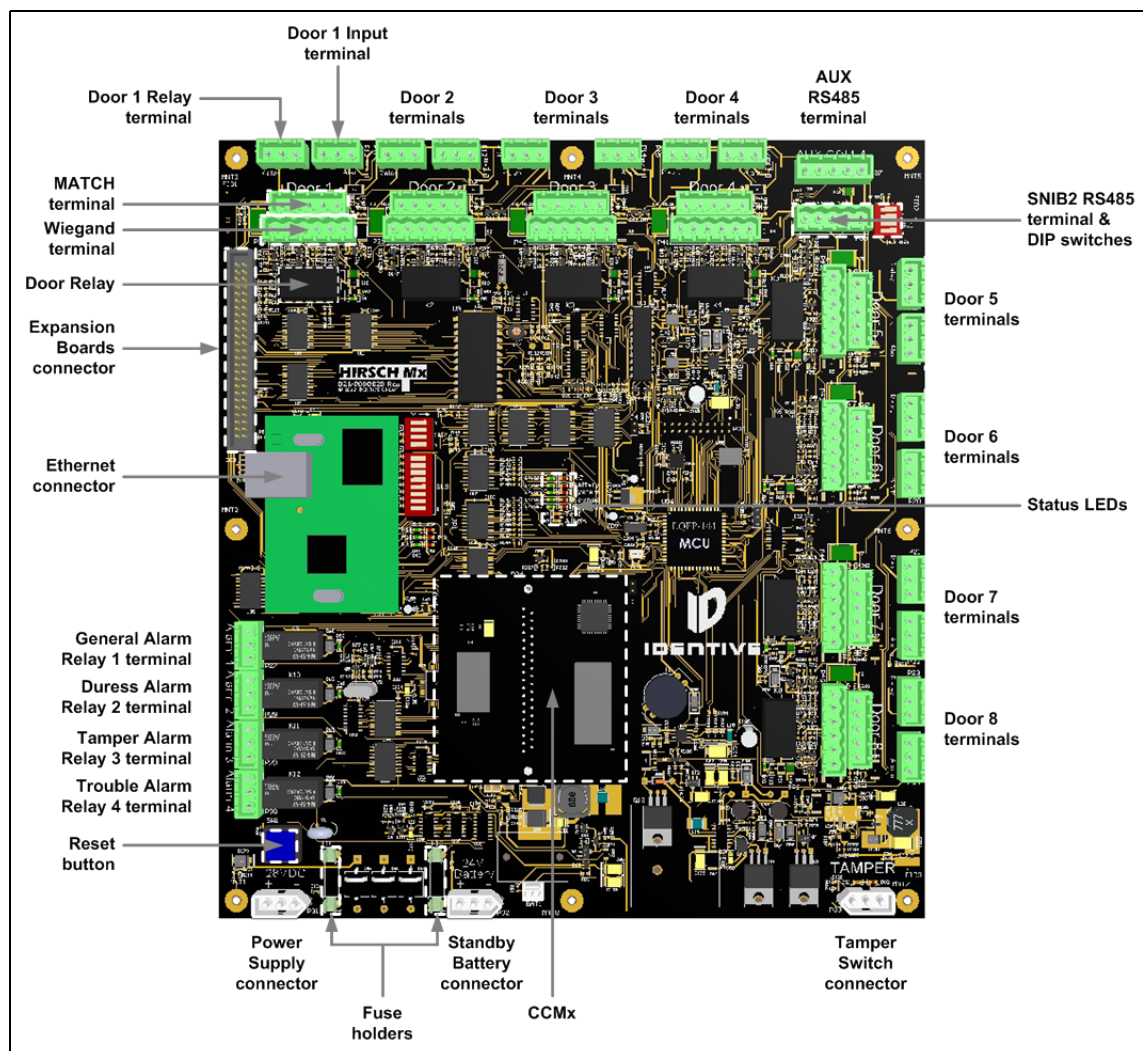


Figure 53: Mx Controller Main Board Connectors and Components

Relays come in two sizes:

- Larger (5 amp, Form C) relays for controlling door access devices, such as magnetic locks and electric strikes, and
- Smaller (2 amp, Form C) relays for executing various types of alarm events.

Terminal Blocks are the green plastic components into which wires are inserted from input/output devices. An Mx Controller provides a certain number of terminal blocks — and through them connections to input/output devices — which you can increase by adding optional expansion boards.

- The 3-wire terminal blocks are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.

- The 5-wire terminal blocks are used for connecting the wiring from ScramblePad keypads or readers (through the MATCH2 Reader Interface Board). These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit.
- The 6-wire terminal blocks are used for connecting the wiring from a 12VDC keypad or reader with a Wiegand interface. These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.

AUX RS485 Terminal is initially unused, but is planned to later enable you to communicate with RS485 serial devices (such as readers and other interfaces), using protocols such as the Open Supervised Device Protocol (OSDP).

SNIB3 RS485 Terminal (and DIP switches) enables you to securely communicate with downstream Mx controllers (managed by the same computer).

Ethernet Connector (and DIP switches) enables you to connect to a LAN/WAN and communicate with a computer running ICPAM.


Fuses are mounted by the power supply connector and the standby battery connector. (All reader terminals are protected with resettable fuses.)

Expansion Board Connector links any expansion boards mounted in the Controller enclosure to the Controller Main Board.

Status LEDs provide quick visual diagnostics on the current operation of the Controller.

Reset Button performs three types of reset depending on how long you hold down the button, as shown in Table 7-3 on page 7-26.

Command and Control Module (CCMx) contains the firmware that embodies the logic and control functions of the controller.

 ***Different models of the CCMx are available, which determine whether the Mx Controller is configured to control up to 4 or 8 doors (and an equivalent number of alarm inputs).***

Power Supply Connector provides cable connection to the Internal Power Supply.

Standby Battery Connector provides cable connection to the backup battery.

Enclosure Tamper Switch Connector provides a cable connection to the Tamper Switch on the Controller enclosure. Whenever the enclosure door is opened, the tamper switch alarm is activated.

Internal Power Supply

The Internal Power Supply can use either a 110 or 240 VAC supply (or 100 VAC for Japan) to provide DC power to the Controller Main Board and attached Expansion Boards. Depending on your controller, this means support for up to 16 ScramblePads or combination of ScramblePads and readers. For input and output devices requiring power – such as electric strikes and magnetic locks, motion detectors, retinal scanners, and surveillance cameras – auxiliary power supplies must be used.

Standby Battery

This component supplies 24 VDC of backup power to the Controller Board even if primary AC power fails. This battery is capable of supplying power to the Controller Board for several hours. The standby time is dependent on the connected devices and can be calculated by using the formula found in "Controller Battery Standby Capacity" on page 62.

The size of the 7.2 Ah battery pack provided with an Mx-4 or Mx-8 controller is approximately 3.69" H x 5.94" W x 5.13" D (94 mm H x 151 mm W x 130 mm D).

Under normal conditions, the standby battery has a life span of 4 to 5 years. For more information, see the topics in the section about "Performing Periodic Maintenance" on page 93.

Tamper Switch

The tamper switch is a contact switch that is normally closed while the door to the controller enclosure is closed. Opening the enclosure door opens a circuit, which generates a message that is sent to ICPAM, enabling the event to be viewed in real-time and logged for later analysis.


Expansion Boards

Optional expansion boards increase the capabilities of Mx Controllers. For example, the Alarm Expansion Board increases the number of line module inputs that the controller can accept, and the Relay Expansion Board extends the number of control outputs that a controller can accommodate. The MEB series increases the controller's available memory, expanding the number of alarm and event buffers or codes the controller can hold.

The following table provides an overview of the available expansion boards. An Mx Controller can accommodate up to 5 expansion boards, subject to the restrictions explained in this table.

Model #	Description	Comments
AEB8	Alarm Expansion Board with 8 Inputs	Adds 8 additional high security alarm inputs, and features removable connectors. Each input requires an appropriate Line Module. ICPAM supports up to 4 of these boards in an Mx Controller.
REB8	Relay Expansion Board with 8 Relays	Adds 8 additional 2 Amp Form C relays. Features status LEDs and removable connectors. ICPAM supports up to 5 of these boards in an Mx Controller.
MEB/BE	Memory Expansion Board - Buffer Expansion	Expands the standard buffer from 1,560 events and 1,560 alarms to approximately 20,000 events and 2,000 alarms. Protected from data loss during power failures for up to 30 days by controller memory battery. ICPAM supports only 1 memory expansion board in an Mx Controller.


Model #	Description	Comments
MEB/CB128	Memory Expansion Board - Code Expansion of 128,000 with Buffer Option	Expands Code Memory by approximately 128,000 (from 4,352 to 135,424) on ICPAM. A portion of the Code Memory may be allocated to alarm and event Buffers, which will reduce the number of users. Protected from data loss during power failures for up to 30 days by controller memory battery. ICPAM supports only 1 memory expansion board in an Mx Controller.
SNIB3	Secure Network Interface Board 3	Adds a 10/100/1000 Ethernet (TCP/IP) port with an RJ45 connector, and an optically isolated multidrop RS-485 serial port. Supports either IPv4 or IPv6 addressing. Can use either the X*NET2 protocol which supports 128-bit AES encryption (and a network of SNIB3s), or the X*NET3 protocol which supports 256-bit AES encryption (if every controller has a SNIB3). ICPAM supports only 1 SNIB3 expansion board in an Mx Controller. If you want to use a SNIB3 expansion board, see "Preparing an Mx Controller to Use a SNIB3" on page 92.

 ***Although ICPAM enables you to reconfigure an unused door so you can use its inputs and relay components for other purposes, the addition of alarm or relay expansion boards does not increase the supervised door capacity of an Mx Controller.***

All boards have the same dimensions and shipping weight:

- Dimensions: 6"H x 4.25"W x 0.75"D (15.2cm x 10.8cm x 1.9cm)
- Shipping Weight: 1 lb (0.5 kg)

The ribbon cable used to connect these boards to the Controller board is the EBIC5, which can link up to five expansion boards. For detailed information on installing expansion boards, refer to the [DIGI*TRAC Design and Installation Guide](#).

 ***If you will be using the Ethernet connector to connect your Mx controller to a LAN/WAN so it can communicate with a computer running ICPAM, **and** you plan to install multiple expansion boards, you should plug in the network cable before installing the expansion boards (while it is easier to access the Ethernet connector).***

Data Capacity of an Mx Controller

An Mx controller includes a base amount of memory which is dedicated to storing data about credentials, events, and alarms. (This memory enables a controller to continue performing its functions even when it is temporarily unable to communicate with the ICPAM server.)

The data capacity of a controller can be increased by adding optional expansion boards. An expansion board can be configured so that its memory is dedicated either solely to additional credentials, or to a mixture of additional credentials, events, and alarms.

The following table shows the maximum data capacity of a controller in its base configuration and with various optional expansion boards configured either way.

Controller configuration	maximum Credentials	maximum Events	maximum Alarms
Base (no expansion boards)	4,352	1,560	1,560
With MEB/CB64	69,888	1,560	1,560
With MEB/CB128	135,424	1,560	1,560

Your system's actual capacity could be less.

Replaceable Parts of the Mx Controller

The following table provides specifications for the replaceable parts of the different models of the Mx controller.

Part	Mx-4	Mx-8
Standby Battery	7.2 Ah 12V rechargeable sealed lead-acid; made by Panasonic, part# LC-R127R2P (or LC-R127R2P1)	7.2 Ah 12V rechargeable sealed lead-acid; made by Panasonic, part# LC-R127R2P (or LC-R127R2P1)
Memory Battery	80 mAh 3.6V rechargeable nickel-metal hydride; made by House of Batteries, part# XVN-H80BC-L3C	80 mAh 3.6V rechargeable nickel-metal hydride; made by House of Batteries, part# XVN-H80BC-L3C
Power Supply Input Fuse	5 A 250V 5 mm x 20 mm; made by Little Fuse Inc., part# 0218005.HXP	5 A 250V 5 mm x 20 mm; made by Little Fuse Inc., part# 0218005.HXP

M64 Controller Design

The M64 Controller comes with a door-mounted SP Controller Board and a special 64-relay expansion board (M64) mounted in the enclosure. The M64 can power ScramblePads and MATCH interfaces from the two ScramblePad/MATCH terminals located on the SP Board or from the four ScramblePad/MATCH terminals located on the M64 Relay Board. The M64 is shown in Figure 54:

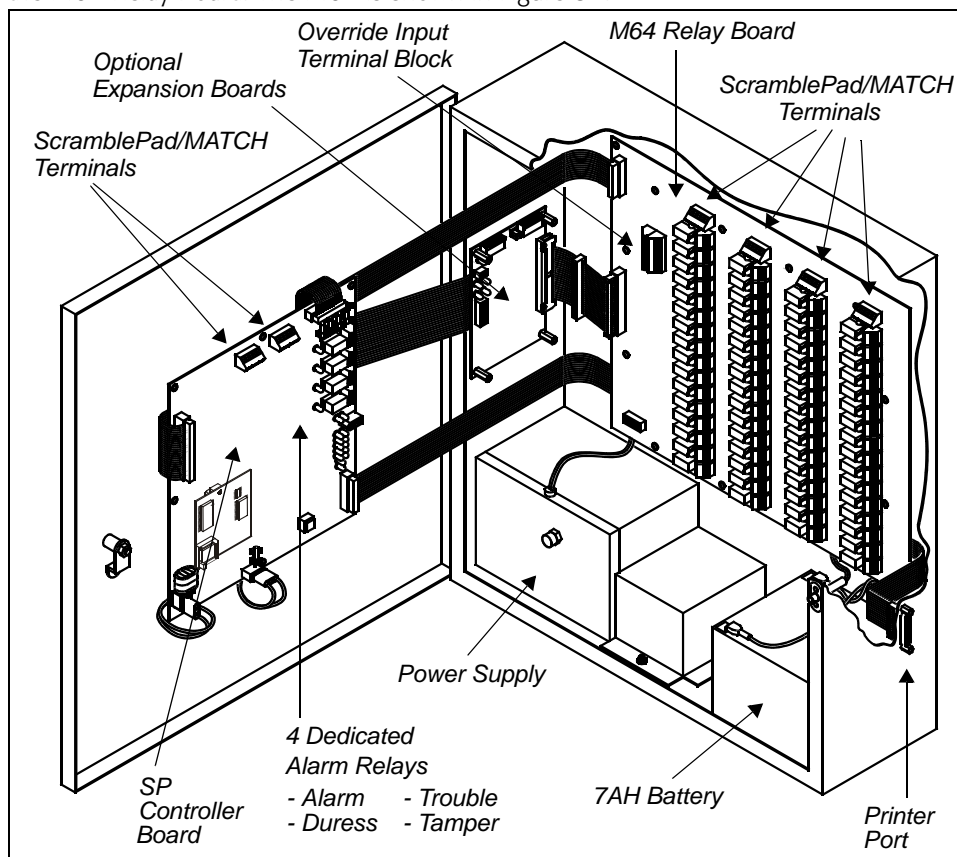


Figure 54: M64 Controller

The M64 Controller is often used for HVAC and lighting control as well as elevator access control. This requires the controller to be located near the elevator control equipment, either in the penthouse or in the basement. Interface between the M64 control relays and the elevator control inputs is usually done by the elevator service company.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller. The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.



Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

The M64 is not designed for door access control. If you require that capability, select an M2, M8, or Mx controller.

Dimension: 22"H x 20"W x 6.25"D (55.9cm x 51cm x 15.9cm)

Shipping Weight: 60 lbs (27.2 kg)

M64 Controller Battery Standby Capacity

The M64 comes factory-equipped with a 24V 7.0 Ah battery.

If still more backup power is required, the internal standby battery can be replaced by larger-capacity external 24VDC batteries (up to a limit of 14 amp-hours), or by a charger and batteries (such as those made by AlarmSafe). A 120/240VAC UPS can also be tied into the main power, providing the controller with both surge protection and emergency power.

When using either external batteries or a charger and batteries, remember:

- When using an external battery pack, remove the controller's internal battery and connect the new power line into the unused standby battery input on the controller board. Remember: connecting two similar batteries in series doubles the voltage.
- When using a UPS, connect the UPS into the AC power line.

To determine how much backup battery power a particular controller requires, use this formula:

$$(I_{\text{Devices}} + I_{\text{Controller}}) \times \text{hours} = \text{Battery Life Required}$$

This is the sum of the load at 24VDC of all the attached devices plus the load at 24VDC of the controller itself multiplied by the hours of battery operation required. The following table provides the extended standby battery requirements (current draw in amps) for typical M64-compatible reader and keypad components, based on quiescent (idle) conditions:

Controller/Attached Devices	Requirements @ 24VDC (Amps)
DS37L (non-illuminated value)	0.07
DS37L-HI (non-illuminated value)	0.10
DS47L (non-illuminated value)	0.04
DS47L-HI (non-illuminated value)	0.04
DS47L-SPX/DS47L-SPX-HI (non-illuminated value)	0.05
MATCH (readers powered separately)	0.07
MATCH (powering 1 or 2 readers)	0.20

For example, suppose an Mx-4 is connected via MATCH Interfaces to 4 doors, each of which is using dual technology: 8 ScramblePads – 4 regular for interior and 4 high intensity for exterior – together with 8 CR11L mag stripe readers.

The installed example system is itemized:

1 Mx-4	x	0.60=	0.60A
4 DS47L	x	0.04=	0.16
4 DS47L-HI	x	0.04=	0.16
8 MRIB	x	0.20=	1.60
Total		=	2.42A

A factory-installed 1.3 AH battery could not support this configuration. However, by using a 7.0 AH battery, the Mx could support this configuration for:

$$\frac{7.0 \text{ Amp-Hours}}{2.42A} = 2.89 \text{ hours}$$

However, if you specify that the extended standby battery backup requirement must be at least 8 hours of operation without primary power:

$$2.42A \times 8 \text{ hours} = 19.36 \text{ amp-hours}$$

Obviously a 7 AH battery is not sufficient for this system. This system will require either an external battery with at least a 20 AH capacity or a front-end UPS in order to operate for a full 8 hours.

Design Considerations for the Mx Controller

This section documents the procedures for mounting, configuring, wiring, and powering an Mx Controller. Controllers are usually located in a safe and secure area, such as an electrical room, telephone equipment room, closet, or the security operations office. An environmentally managed room is not required as long as the temperature ranges don't exceed the Controller's specifications.

In addition to monitoring, reporting, and controlling a variety of devices, each controller can power a specific number of ScramblePads, MATCH2 interfaces, and attached readers. Other devices, such as interior motion sensors and some readers, may require power from a separate power supply.

Electrical Ratings

An Mx controller has the following electrical ratings:


- Input: 120 V, 1.25 A; Two batteries connected in series at 12 V DC, 7.2 Ah provided with an Mx-4 or Mx-8.
- Output: 5-pin MATCH terminal at 24 V DC - 28 V DC, 1 A; 6-pin Wiegand terminal at 12 V DC, 0.5 A.
- Door Relays (dry contact): 30 V DC, 5 A, 0.6 pF.

Mx Controller Design

Depending on its configuration, an Mx Controller provides for 2, 4, or 8 supervised doors: this includes 5Amp door relays with line module inputs. Each door is represented by a ScramblePad/MATCH terminal block, a Weigand terminal block, a relay terminal block, and an input terminal block (for connecting a line module). An Mx Controller can power ScramblePads and MATCH2 interfaces from the 5-pin MATCH terminal blocks, or it can power Weigand card readers from the 6-pin Weigand terminal blocks.

An Mx Controller includes an integrated SNIB3 for direct connection via RS-485 to a SCRAMBLE*NET network, and an integrated Ethernet port for easy connection to a computer running ICPAM. It also supports certain expansion boards, as discussed in "Expansion Boards" on page 54.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller. The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

 ***Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage, and void the manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.***

- Dimensions: 18"H x 15.25"W x 5.5"D (45.7cm x 38.7cm x 14cm)
- Shipping Weight: 30 lbs (13.6 kg)

Separation of Circuits

To maintain a safe separation between different types of circuits, the Class 1 high voltage AC input power for an Mx controller is routed through either one of the two knock-outs

at the bottom of the enclosure, while the other cables for the controller's Class 2 circuits, HI/LO inputs, MATCH terminals, and Wiegand terminals are routed through several knock-outs located across the top and sides of the enclosure as shown in Figure 55.

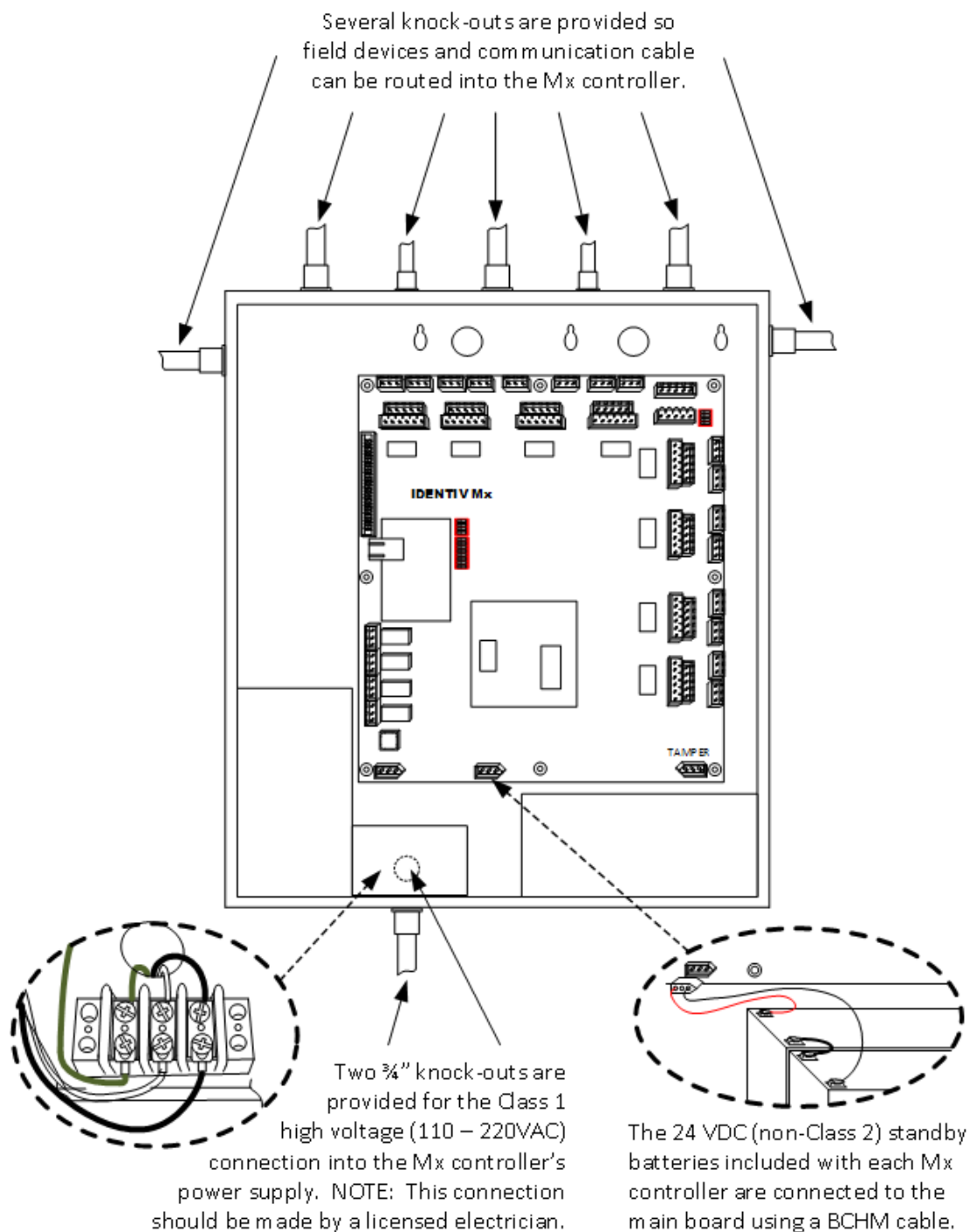


Figure 55: Cable Inlets of the Mx Controller's Enclosure

The Mx controller's Class 2 limited power circuits have the following connections (as shown in Figure 53 on page 52):

- 8 3-wire HI/LO analog input terminal (for the line modules used to supervise doors, tamper circuits, and RQE devices).
- 8 5-wire terminal blocks (for connecting keypads or readers through the 28 VDC MATCH2 Reader Interface Board). These are *digital* circuits which support MATCH2 boards and DS47L series keypads.
- 8 6-wire terminal blocks (for connecting the wiring from a 12VDC keypad or reader with a Wiegand interface). These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.

All reader circuits are protected by resettable thermal fuses, which automatically restore circuit integrity after the overcurrent has been removed.

Controller Battery Standby Capacity

The Mx-4 and Mx-8 controllers come factory-equipped with a 24V 7.2 Ah battery, to comply with the standby power requirements of UL 1076 Section 40. Each battery kit consists of two 12-volt batteries connected in series for a full 24-volt standby unit.

If still more backup power is required, the provided internal standby battery can be replaced by larger-capacity external 24VDC batteries (up to a limit of 14 amp-hours), or by a charger and batteries (such as those made by AlarmSafe). A 120/240VAC UPS can also be tied into the main power, providing the controller with both surge protection and emergency power.

When using either external batteries or a charger and batteries, remember:

- When using an external battery pack, remove the controller's internal battery and connect the new power line into the unused standby battery input on the controller board. Remember: connecting two similar batteries in series doubles the voltage.
- When using a UPS, connect the UPS into the AC power line.

To determine how much backup battery power a particular controller requires, use this formula:

$$(I_{\text{Devices}} + I_{\text{Controller}}) \times \text{hours} = \text{Battery Life Required}$$

This is the sum of the load at 24VDC of all the attached devices plus the load at 24VDC of the controller itself, multiplied by the hours of battery operation required. The following table provides the extended standby battery requirements (current draw in amps) for the Mx Controllers and typical Mx-compatible reader and keypad components, based on quiescent (idle) conditions:

Controller or Attached Device	Requirements @ 24VDC
Mx controller	0.53 A
DS47L (non-illuminated value)	0.04 A
DS47L-HI (non-illuminated value)	0.04 A
DS47L-SPX/DS47L-SPX-HI (non-illuminated value)	0.05 A
MATCH2 (readers powered separately)	0.07 A
MATCH2 (powering 1 or 2 readers)	0.20 A

For example, suppose an Mx controller is connected via MATCH2 Interfaces to four doors, each of which is using dual technology: 4 ScramblePads – 2 regular for interior and 2 high intensity for exterior – together with 4 CR11L mag stripe readers.

The installed example system's current draw is itemized:

1 Mx	x	0.53	= 0.53A
2 DS47L	x	0.04	= 0.08A
2 DS47L-HI	x	0.04	= 0.08A
4 MRIB	x	0.20	= 0.80A
Total			= 1.49A

A factory-installed 7.2 Ah battery (supplied with an Mx-4 or Mx-8 controller) could support this configuration for:

$$\frac{7.2 \text{ Amp-hours}}{1.49 \text{ A}} = 4.83 \text{ hours}$$

However, if you specify that the extended standby battery backup requirement must be at least 8 hours of operation without primary power:

$$1.49\text{A} \times 8 \text{ hours} = 11.92 \text{ Amp-hours}$$

Obviously the included 7.2 Ah battery is not sufficient for this system. To operate this system without primary power for a full 8 hours, you will need to provide either an external battery or a front-end UPS, with at least a 12 Ah capacity.


Power Provided at the Terminal Blocks

An Mx Controller provides 12VDC power at the Wiegand terminal blocks, and 24VDC at the MATCH terminal blocks.

The following table shows the power provided for Wiegand and MATCH@ keypads/readers by an MX Controller.

Terminal Type	Max. Current Draw (Amps) per Controller	Max. Current Draw (Amps) per Channel
Wiegand	2.0	0.25
MATCH	2.9	1.0

ScramblePad/MATCH2 Power Requirements

 *The following topic illustrates power calculations using ScramblePads and MATCH2 interfaces, because we know their power requirements. If you are using keypads/readers with a Wiegand interface (from another vendor), you can perform similar power calculations using the power requirements of your particular devices, and the information in the Wiegand row of previous table.*

To determine how many ScramblePads and MATCH2 interfaces an Mx controller can power, you must calculate the current draw of the ScramblePads and MATCH2 Interfaces and compare it to the maximum current draw available from the Mx controller (which is shown in the MATCH row of the table above).

The controller powers ScramblePads and the MATCH2, then the MATCH2 powers one or two readers. The Mx controller has an integrated MATCH terminal and an integrated Wiegand terminal for each door, which can power the readers directly wired to those terminals.

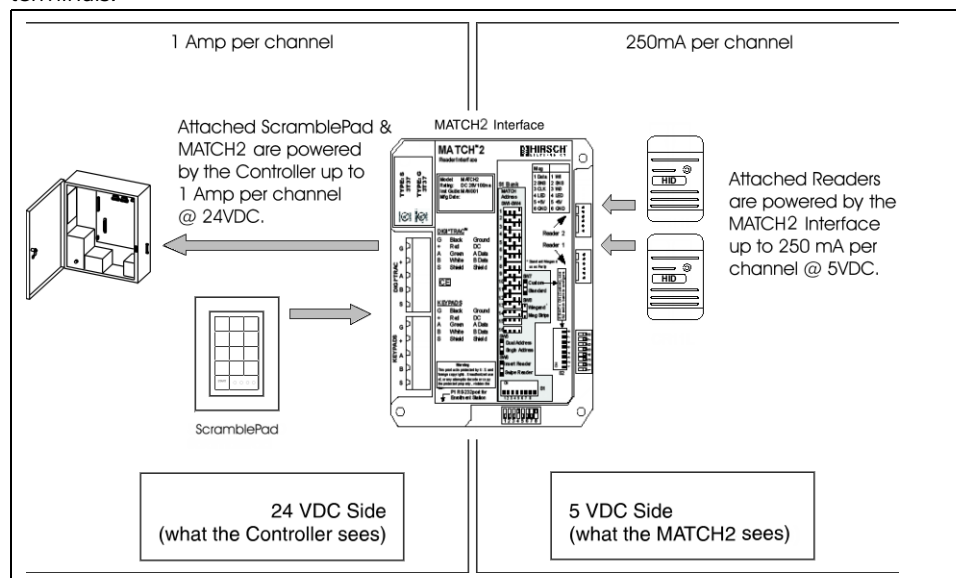


Figure 56: Current Draw Orientation for MATCH2 Interface

As shown in Figure 56, voltage from the Controller to the MATCH2 and ScramblePads is 24VDC, while voltage from the MATCH2 to its connected readers is 5VDC. (Although ScramblePads may be connected through the MATCH2 to the controller, the ScramblePads are powered by the controller, not the MATCH2.)

To determine how many ScramblePads and MATCH2 interfaces the controller can power, use the following procedure:

1. Determine what devices you will be using. For example, an Mx-4, DS47L ScrambleProx, an MRIB MATCH2 Interface, and MATCH-compatible readers.
2. Determine the quantity of each device you'll need. For example, 1 Mx-4, 1 DS47L-SPX and 1 DS47L-SPX-HI ScrambleProx, 1 MRIB, and 2 CR31L readers.
3. Determine whether the MATCH2 Interface will be able to power the connected readers. Make sure the readers' 5VDC draw does not exceed the MATCH2's 250mA at 5VDC limit. If the MATCH2 powers readers, it draws more current from the controller than if the readers were separately powered.

4. To determine the current draw of each attached device on the controller at 24VDC, multiply the number of devices by the current draw for each device, then add the total for each device to calculate the Total Current Draw required from the controller, using the values shown in the following table:

Device	Draw per Device (Amps) @ 24VDC
DS47L ScramblePad (illuminated value)	0.125
DS47L-SPX ScrambleProx (illuminated value)	0.135
DS47L-SPX-HI ScrambleProx (illuminated value)	0.25
MATCH2 Interface (powering 1 or 2 readers)	0.20
MATCH2 Interface (readers powered separately)	0.07



Do not include the reader's 5VDC current draw in the calculation.

As shown in the previous table, it doesn't matter to the controller whether a MATCH2 is powering one or two readers, because the MATCH2 is using a switching power supply. The MATCH2 can provide up to 250 mA @ 5VDC to each of two readers and present a load to the controller of only 200 mA @ 24VDC. If readers attached to a MATCH2 are self-powered, the MATCH2 presents a load to the controller of only 70 mA.

For this example, given both entry and exit dual technology – 1 DS47L-SPX-HI ScrambleProx and 1 CR31L Wiegand Swipe Reader on the entry side, and a DS47L-SPX ScrambleProx and 1 CR31L on the exit side – tied into a MATCH2 interface, the following calculations would result:

$ \begin{array}{rcl} 1 \text{ DS47L-SPX} \times 0.135\text{A} & = & 0.135\text{A} \\ 1 \text{ D437L-SPX-HI} \times 0.25\text{A} & = & 0.250\text{A} \\ 1 \text{ MRIB} \times 0.20\text{A} & = & 0.200\text{A} \\ \hline \text{Total Current Draw} & = & 0.535\text{A} \end{array} $

5. Determine whether an Mx controller can power the ScramblePads/MATCH2s connected to it, by comparing the Total Current Draw required against the maximum current draw available from the controller (which is shown in the MATCH row of the table in "Power Provided at the Terminal Blocks" on page 63).
6. Verify that current from any one ScramblePad/MATCH terminal block does not exceed 1.0 Amp.

The preceding total of 0.535A is well within an Mx Controller's 1.0A per channel limit and 2.9A total capacity limit. If the total current draw required exceeds an Mx controller's limits, use a remote power supply for one or more of the attached devices.

Typical Connections

Mx controllers can connect to a number of input and output devices.

All interconnecting devices must be UL Listed, low-voltage Class 2 power limited.

Wiring for a Door

For each door, an Mx controller provides the following terminal blocks:

- A 3-pin Input terminal for analog inputs such as multi-state alarm inputs from the line modules. For more on this, refer to “Typical Line Module Inputs” on page 67.
- A 3-pin Relay terminal for two-state outputs such as magnetic locks and electric strikes. For more on this, refer to “Typical Door Relay Outputs” on page 68.
- A 5-pin MATCH terminal for connecting ScramblePad keypads or readers through a MATCH2 Reader Interface Board. These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit. For more on this, refer to “ScramblePad/MATCH Inputs” on page 70.
- A 6-pin Wiegand terminal for directly connecting a reader or keypad which has a Wiegand interface. For more on this, refer to “ScramblePad/MATCH Inputs” on page 70.

For each door, you will use either the 5-pin MATCH terminal or the 6-pin Wiegand terminal, depending on your needs:

- For basic access control applications that only need an entry reader on a door, you can use the 6-pin Wiegand terminal to directly connect the Mx controller to a reader or keypad which has a Wiegand interface (without a separate MATCH2 board).
- You must use the 5-pin MATCH terminal to connect the Mx controller to a MATCH2 interface board or ScramblePad reader for a more advanced access control application that needs both entry and exit readers on a door, or wire runs longer than 500 feet.

CAUTION *To avoid possible damage to your Mx controller, make sure it is powered off before you add or remove a reader connected to a 6-pin Wiegand terminal.*

Typical Line Module Inputs

The Line Module is an intermediate connection between Door Contacts (or Alarm Sensors), RQE devices, and the controller's input terminal blocks.

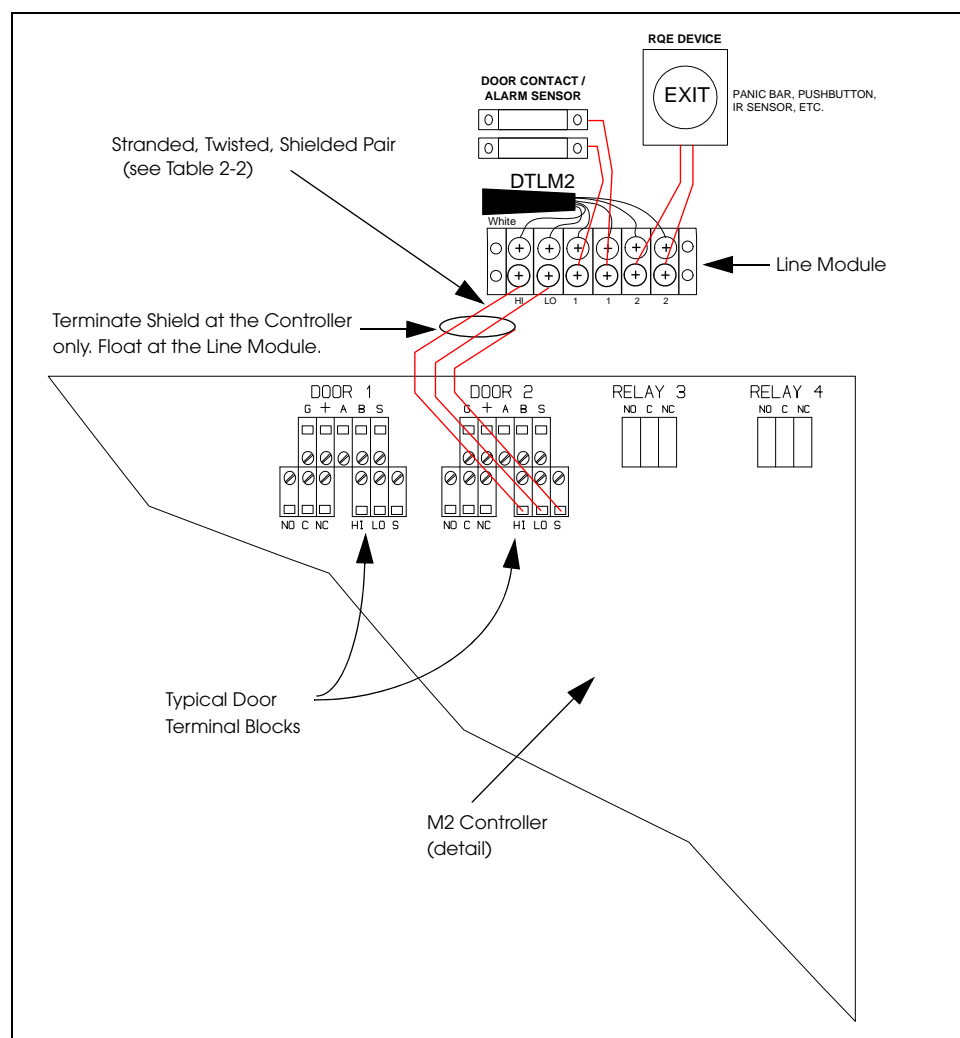



Figure 57: Typical Line Module Input Connection

The recommended gauge and maximum distances for a cable between the Controller and the Line Module are shown in the following table:

Wire (AWG)	DTLM/MELM 1		DTLM/MELM 2		DTLM/MELM 3		Belden Ref. No.
	Feet	Meters	Feet	Meters	Feet	Meters	
22	5,200	(1,575)	2,500	(750)	900	(275)	8761
20	8500	(2,500)	4,500	(1,375)	1,200	(350)	8762
18	13,000	(3,975)	7,500	(2,275)	2,000	(600)	8760

Wire (AWG)	DTLM/MELM 1		DTLM/MELM 2		DTLM/MELM 3		Belden Ref. No.
	Feet	Meters	Feet	Meters	Feet	Meters	
16	20,000	(6,100)	11,500	(3,500)	3,100	(950)	8719
14	32,000	(9,750)	18,000	(5,500)	5,000	(1,525)	8720
12	50,000	(15,250)	28,000	(8,550)	8,000	(2,450)	8718

 **MELM3s are included with the controller purchased from CCW.**

Typical Door Relay Outputs

The typical door relay output terminal block provides the connection between a door lock and the controller.

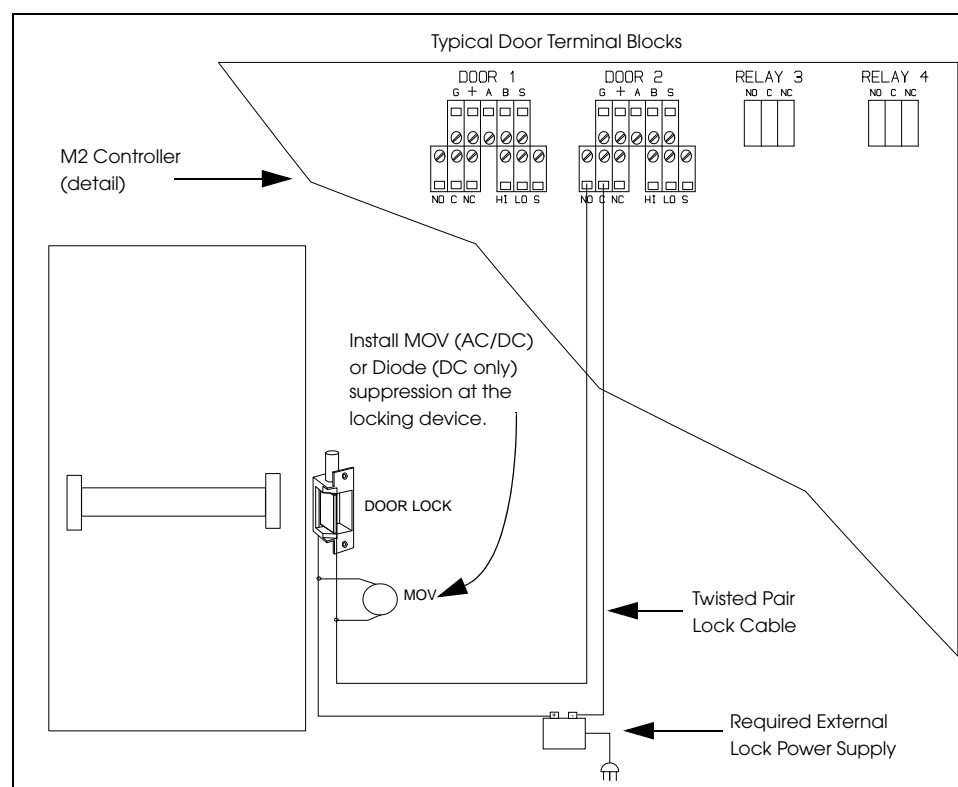


Figure 58: Typical Door Relay Connection

Cable runs for electric and magnetic locks must be separated by at least 6 inches (15cm) from ScramblePad and DTLM circuits, unless you use twisted-pair cable for all circuits. Zip cord is not acceptable.

All electronic locks induce electrical noise or interference on their control lines. These lines, when connected to the relays inside the controller, can interfere with normal controller function.

Surges, spikes, and noise produced by the lock can be suppressed by adding either an MOV or diode near the locking device. Some door locks include suppression. However, in many cases, you must install a Metal Oxide Varistor (MOV) or Diode at the lock. You can use an MOV with either AC or DC locks. An MOV is available from Hirsch as Part No. MOV35 (Thomson VE09M00250K, GE V39ZA1 or equivalent). Use a diode with DC locks only. The diode required is a 1A, 400V diode and is available from Hirsch as Part No. DIODE. Since a diode has a cathode and anode side, it is polarity-sensitive. Make sure to connect the cathode side of the diode to the positive (striped) side of the locking device.

When connecting to a door lock or some other output device requiring more than the Contact Ratings of the controller's relays, an intermediate relay is required. The Relay Contact Ratings are shown in this table:

Relay Type	Ratings
Door Relays	24V DC, 10A, resistive
Alarm/Control Relays	24V DC, 2A, resistive

The maximum length for lock power runs (in feet and meters) depends on this formula and the wire gauge table associated with it:

$$W \times \frac{V_L}{I_L} = \text{maximum distance (in feet and meters)}$$

where:

W = Cable Impedance Multiplier

V_L = Lock Voltage

I_L = Lock Current

W , the *Cable Impedance Multiplier*, is calculated using this table:

Wire Gauge (AWG)	Cable Impedance Multiplier	
	Feet	Meters
22	5	1.52
20	9	2.74
18	14	4.27
16	22	6.70
14	35	10.67

The lock cable can be run in the same conduit with ScramblePad/MATCH circuits or line module input circuits, but the lock cable must always be a twisted pair.

For example, if the lock voltage is 24 VDC and the lock current is 0.125 Amps, and the lock is connected to the controller with 18 AWG cable, then the maximum allowed distance is:

$$14 \times \frac{24}{.125} = 2688 \text{ feet}$$

ScramblePad/MATCH Inputs

The typical ScramblePad or MATCH input terminal block provides the connection between the controller and a ScramblePad or MATCH Interface.

An example of such a connection is shown in Figure 59.

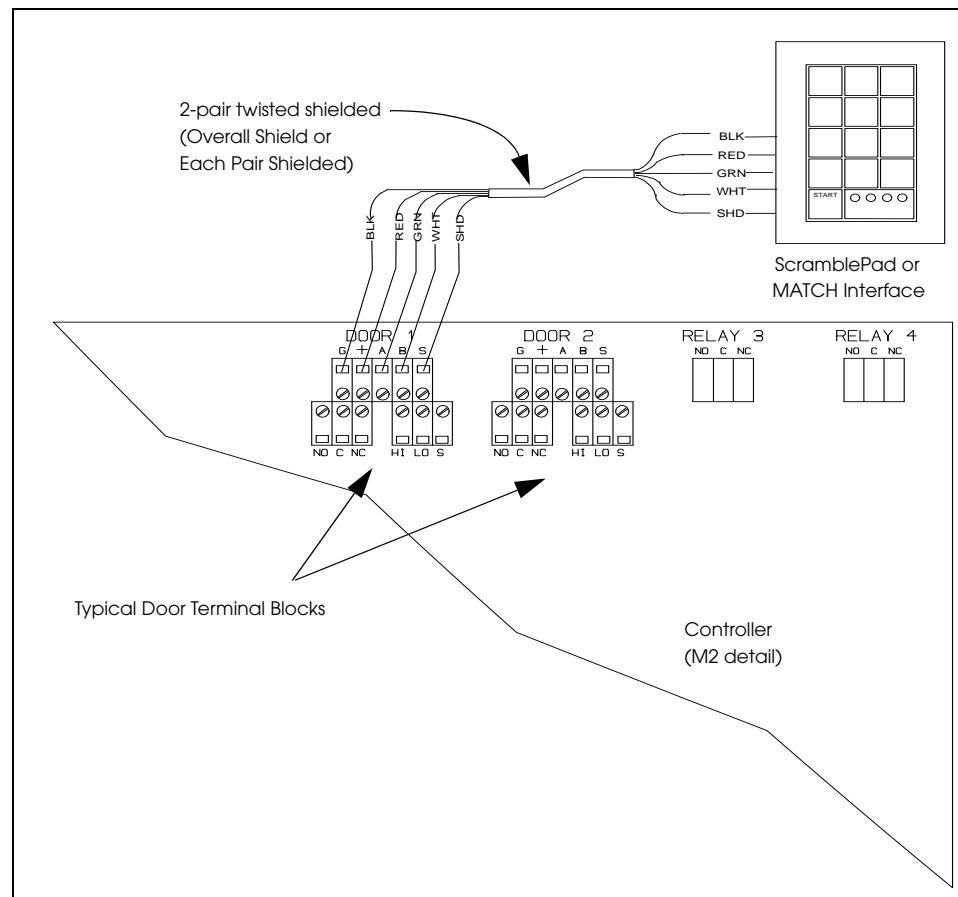



Figure 59: ScramblePad/MATCH Inputs

The following table shows absolute maximum cable distances allowed in feet and meters between the controller and any one or two ScramblePad combinations according to wire gauge:

Cable Gauge (AWG)	Maximum Distance in feet (meters) from Controller to:									
	1 L		1 H		2 L		L + H		2 H	
22	750	(228.6)	500	(152)	375	(114)	280	(85)	230	(70)
20	1,200	(366)*	800	(244)	600	(183)	460	(140)	375	(114)
18	1,800	(549)*	1,200	(366)*	935	(285)*	720	(219)	585	(178)
16	3,000	(914)*	1,875	(571)*	1,500	(457)*	1,150	(350)*	935	(285)*

In the previous table, the DS37L/DS47L/DS47L-SPX keypads are abbreviated as L and the DS37L-HI/DS47L-HI (or weatherized versions, DS37L-HW/DS47L-HW) are abbreviated as H. The MATCH Interface is abbreviated as M. Items followed by asterisks (*) indicate cable capacitance must not exceed 100,000 pf.

 **Use half of these distances when the controller is supplying power to a ScramblePad with an SPSH-1 heated back cover.**

The following table shows absolute maximum cable distances in feet and meters between the controller and any MATCH and/or 1 or 2 ScramblePad combinations according to wire gauge:

Cable Gauge (AWG)	Maximum Distance (feet/meters) from Controller to:					
	M	M + L	M+H	M+2L	M+L+H	M+H+H
22	1875 (572)*	535 (183)	375 (114)	310 (94)	250 (76)	205 (62)
20	3000 (914)*	860 (262)	600 (183)	500 (152)	400 (122)	330 (100)
18	4500 (1371)*	1340 (408)*	935 (285)	780 (238)	625 (190)	515 (157)
16	7500 (2286)*	2150 (655)*	1500 (457)*	1250 (381)*	1000 (305)	825 (251)

In the previous table, the DS37L/DS47L/DS47L-SPX keypads are abbreviated as L and the DS37L-HI/DS47L-HI (or weatherized versions, DS37L-HW/DS47L-HW) are abbreviated as H. The MATCH Interface is abbreviated as M. Items followed by asterisks (*) indicate cable capacitance must not exceed 100,000 pf.

The previous is applicable for MATCH-powered 5VDC readers, as allowed by the MATCH Interface's 28V/5V switch power supply efficiency. A reader drawing 200 mA at 5VDC translates to only about 40 mA at the MATCH Interface's 24VDC input side. Since the MATCH uses a switching power supply, the load presented by two 5VDC readers is no greater than that for one 5 VDC reader. Therefore, this table is valid whether one or two readers are powered by the MATCH Interface.

Overall shield or individual shielded pairs are acceptable. Color coded cable – black, red, green, white – is recommended. Pair one, the black and red wires, provides power to the ScramblePad or the MATCH Interface; pair two provides data communications between the Controller and the ScramblePad or MATCH Interface.

If two ScramblePads are installed at the same door – one for entry and the other for exit – they can share the same cable run. Connect the second ScramblePad to the removable connector of the first ScramblePad. For longer cable runs, provide a local auxiliary power supply to the ScramblePad or MATCH Interface.

Power Requirements for Various Devices

To determine how many ScramblePads and MATCH interfaces an Mx controller can power, you must figure both the current draw of the ScramblePads and MATCH Interfaces and compare it to the maximum current draw available from the controller.

The MATCH powers one or two readers, while the controller powers ScramblePads and the MATCH. The controller cannot power readers directly.

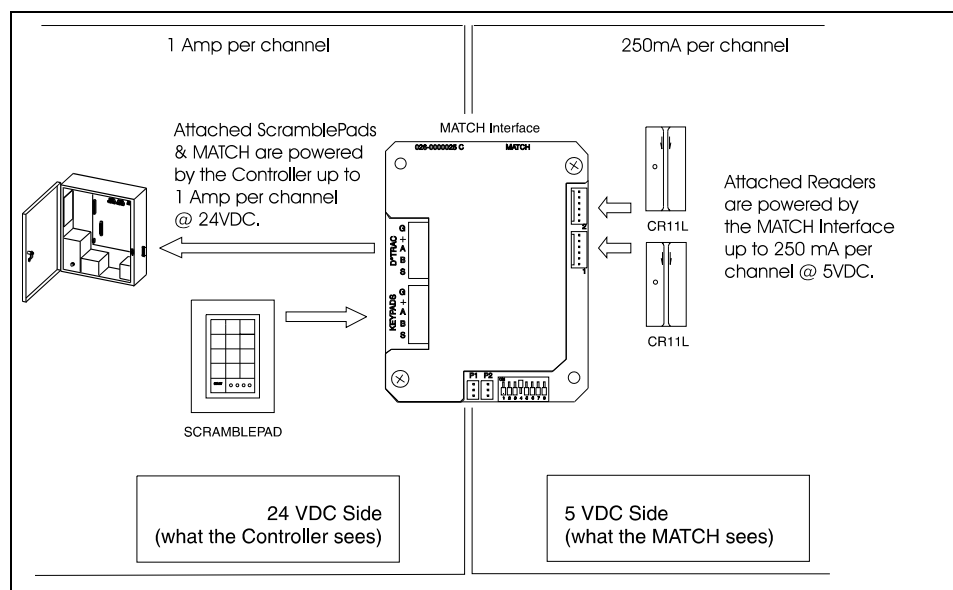


Figure 60: Current Draw Orientation

As shown in Figure 56, voltage from the Controller to the MATCH and ScramblePads is 24VDC while voltage from the MATCH to its connected readers is 5VDC. (While ScramblePads may be connected through the MATCH to the controller, the ScramblePads are powered by the controller, not the MATCH.)

In order to determine how many ScramblePads and MATCH interfaces the controller can power, use this procedure:

1. Determine what devices you will be using. For example, an M2, DS-37L ScramblePads, an MRIB MATCH Interface, and MATCH-compatible readers.
2. Determine the quantity of each device you'll need. For example, 1 M2, 1 DS37L and 1 DS37L-HI ScramblePads, 1 MRIB, and 2 CR31L readers.

3. Determine whether the MATCH Interface will be able to power the connected readers. Make sure the readers' 5VDC draw does not exceed the MATCH's 250mA at 5VDC limit. If the MATCH powers readers, it draws more current from the controller than if the readers were separately powered.
4. To determine the current draw of each attached device on the controller at 24VDC, multiply the number of devices by the current draw for each device, then add the total for each device to calculate the Total Current Draw required from the controller using the values shown in the following table.

Device	Draw per Device (Amps) @ 24VDC
DS37L ScramblePad (illuminated)	0.15A
DS37L-HI / DS47L-HI ScramblePad (illuminated)	0.25A; 0.04A
DS47L ScramblePad (illuminated; non-illuminated)	0.125A; 0.04A
DS47L-SPX-H / DS47L-SPX-I ScrambleProx (illuminated; non-illuminated)	0.135A; 0.05A
DS47L-SPX-H-HI / DS47L-SPX-I-HI ScrambleProx (illuminated; non-illuminated)	0.25A; 0.05A
DS47L-SSP-HID (illuminated; non-illuminated)	0.205A; 0.12A
DS47L-SSP-HID-HI (illuminated; non-illuminated)	0.32A; 0.12A
MATCH Interface (powering 1 or 2 readers @ 5VDC; readers powered separately) date code 010327 or later	0.20A; 0.07A
NetMux4	0.15A
SNIB3	0.125A
AEB8	0.08A
REB8 (all relays on; standby)	0.135A; 0.12A
Memory Expansion Board (MEB/BE, MEB/CE16, MEB/CE32, MEB/CE64, or MEB/CE128)	0.08A



Do not include the reader's 5VDC current draw in the calculation.

As shown in the previous table, it doesn't matter to the controller whether a MATCH is powering one or two readers, because the MATCH is using a switching power supply. The MATCH can provide up to 250 mA @ 5VDC to each of two readers and present a load to the controller of only 200 mA @ 24VDC. If readers attached to a MATCH are self-powered, the MATCH presents a load to the controller of only 70 mA.

For this example, given both entry and exit dual technology – 1 DS47L-HI ScramblePad and 1 CR31L Wiegand Swipe Reader on the entry side and a DS47L ScramblePad and CR31L on the exit side – tied into a MATCH interface, the following calculations would result:

1 DS47L x 0.125A	=	0.125A
1 DS37L-HI x 0.25A	=	0.250A
1 MRIB x 0.20A	=	0.200A
Total Current Draw	=	0.525A

- Determine whether a controller can power the ScramblePads/MATCHs connected to it by comparing the Total Current Draw required against this table:

Controller	Max. Current Draw per Controller (Amps)	Max. Current Draw per Channel (Amps)	Controller's Own Current / Power Draw
M1N	0.125A*	0.125A	0.28A (92 BTU)
M2	1.05A	1.0A	0.60A (215 BTU)
M8	2.90A	1.0A	0.80A (425 BTU)
M16	1.15A	1.0A	0.60A (215 BTU)
Mx	2.90A	1.0A	0.53A (186 BTU)
MSP-8R	1.25A	1.0A	
M64	2.15A	1.0A	

* maximum *peak* current draw per M1N controller is 0.50 A.

- Verify that the current from any one ScramblePad/MATCH terminal block does not exceed 1.0 Amp.

The preceding total of 0.60A is well within the M2's 1A per channel limit and 1.05A total capacity limit.

When the total current draw required exceeds a controller's limits, you can either purchase another controller or use a remote power supply for one or more of the attached devices.

The PS2 power supply's current draw depends on its load. For example:

- 0.11 A when driving normally OFF door strikes
- 0.17 A when driving one magnetic lock (or crash bar)
- 0.22 A when driving a pair of magnetic locks

Here is another data point: an M64N2 controller (at 110VAC) with 2 AEB8 expansion boards draws 0.32 A (0.43 A when all 64 relays are ON).

Figure 61 shows the logic of the typical wiring for a door supervised by an Mx controller, with a card reader wired to a MATCH2 board which is wired to the 5-pin MATCH terminal for a door.

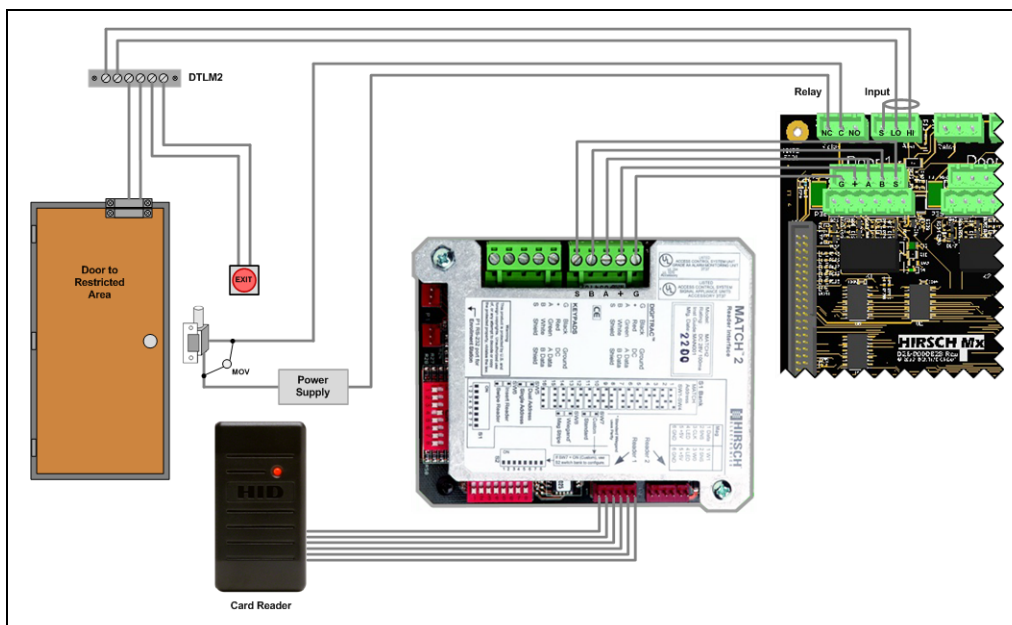


Figure 61: Typical Door Wiring Example for an Mx Controller

For information about setting up and installing Wiegand readers using a MATCH board, see the [DIGI*TRAC Design and Installation Guide](#).

If you are using a reader or keypad which has a Wiegand interface, you can use the 6-pin Wiegand terminal block instead of the 5-pin MATCH terminal block, as shown in the following diagram.

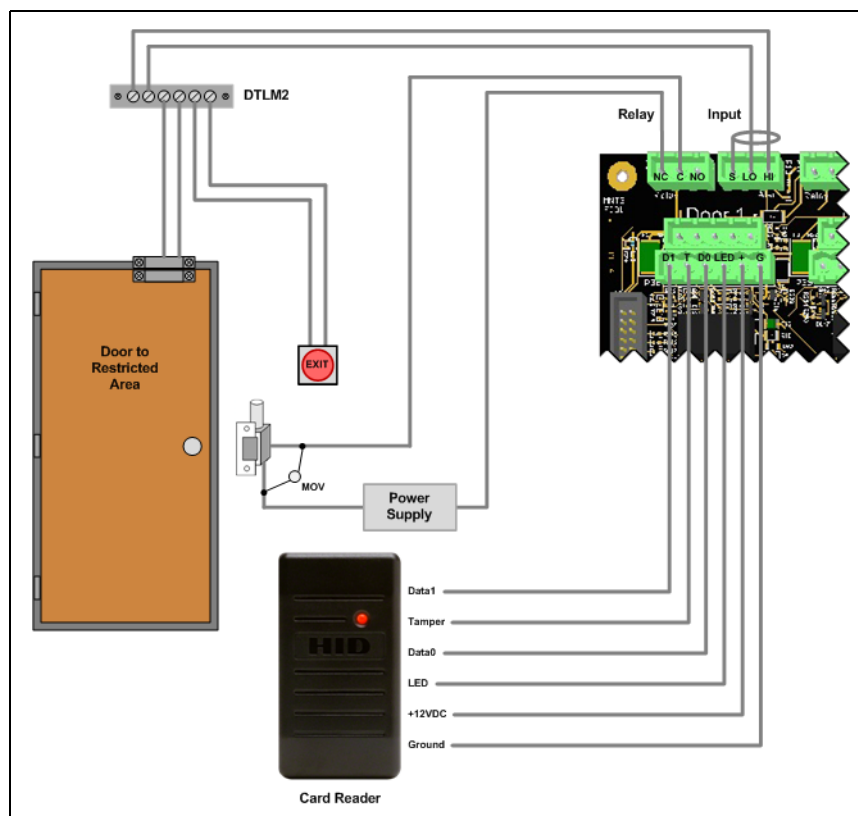


Figure 62: Wiegand Door Wiring Example for an Mx Controller



Always refer to the actual wiring diagram provided with the specific reader that you are installing.

Wiring Diagram for the TS-8010 Reader

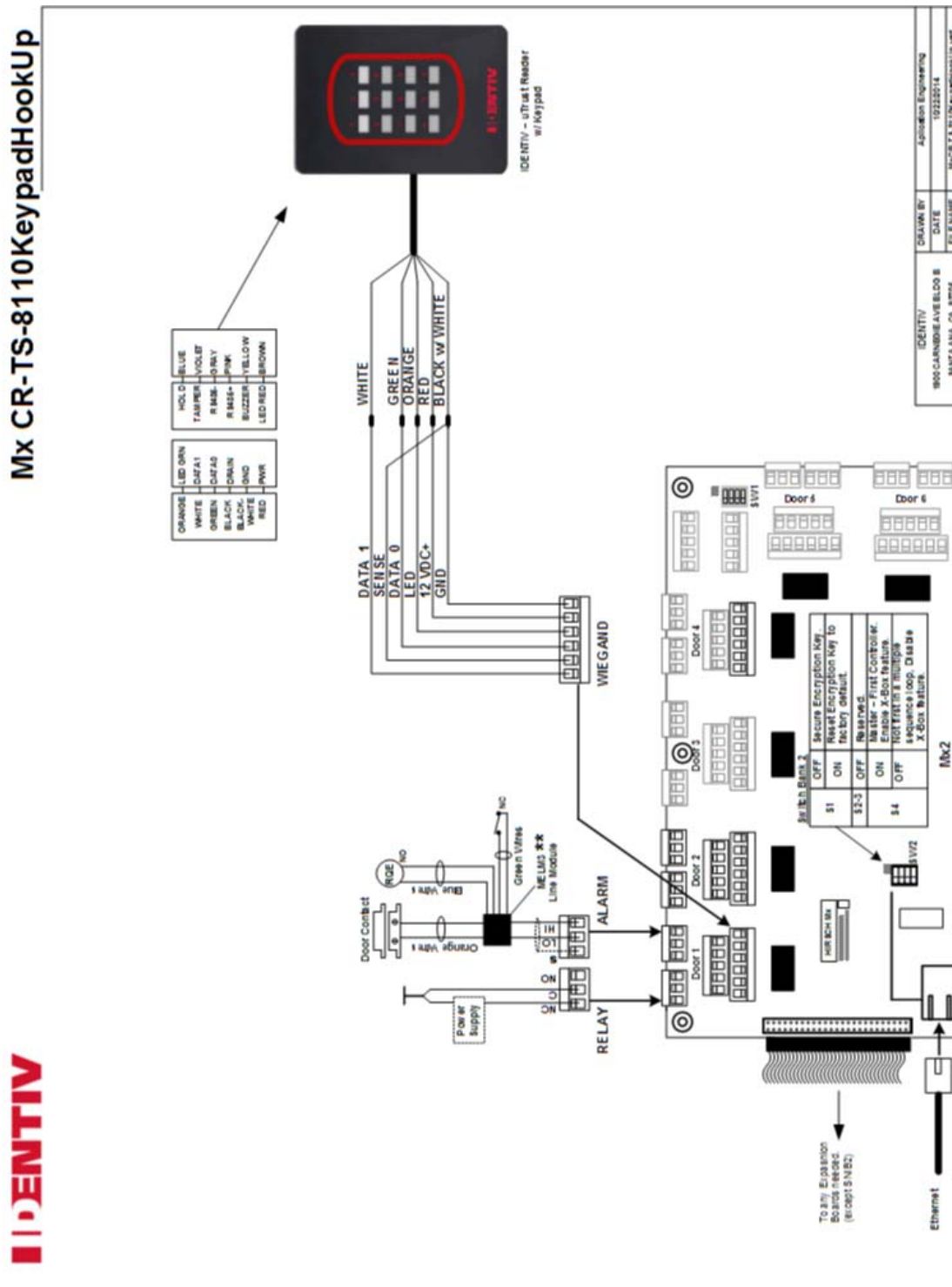
The following wiring diagram shows how to connect a TS-8010 reader to a Wiegand terminal on the main board of an Mx controller. It includes the connections for an electric lock and a door contact.

CR-TS-8010



Wiring Diagram for the TS-8110 Reader

The following wiring diagram shows how to connect a TS-8110 reader to a Wiegand terminal on the main board of an Mx controller. It includes the connections for an electric lock and a door contact.



Setup and Installation of an Mx Controller

An Mx controller can be operated in ambient temperatures of 0 degrees Centigrade to 49 degrees Centigrade, with a maximum relative humidity of 93%. It must be installed indoors, within the protected premises.

- Refer to “Controller Set Up” on page 17 for instructions on setting up an Mx Controller. For information about setting DIP switches, refer to “Configuring the Integrated SNIB3” on page 86.
- Refer to “Mounting the Controller” on page 17 for instructions on mounting the controller.
- Refer to “Wiring to the Controller” on page 18 for instructions on wiring the Mx to other devices. Also, refer to Figure 53 on page 52.

For detailed information on installing the Mx Controller, refer to [DIGI*TRAC Design and Installation Guide](#).

Mounting the Controller

To Mount the Controller:

1. If it makes the job easier, remove the controller door by lifting it straight up off its hinges.
The M64's door has six cables tied to it. For this reason, it isn't recommended that you remove this door unless you absolutely have to. If, for some reason, you have to remove the door, disconnect the cable plugs from the SP controller board.
2. Punch out the knockouts needed for the conduits and cables. In most installations the top entry knockouts are used for conduit and cable installation. Side entry knockouts may be more convenient for expansion boards. Bottom or back knockouts are recommended for power cabling.
3. If this is an Mx-4, use the three keyhole mounting holes along the top of the controller cabinet to hang the controller. Holes are 4¾ inches (12cm) apart.
If this is an Mx-8 or M64, use the two keyhole mounting holes along the top of the cabinet to hang the Controller. Holes are 16 inches (40.6cm) apart. Use the two bottom mounting holes for additional security.



For best results, mount the Controller to a ¾-inch plywood backboard.

4. Because most controller cabinets (except for M64) are too narrow to mount on a pair of wall studs, use the center keyhole to catch a stud. Use molly bolts or similar hardware in the other two keyholes to secure the cabinet to the wall. Use the bottom mounting holes for further mounting security.
5. If you're installing a local printer at this site, make sure the printer connector on the right side of the cabinet has room to connect to the printer cable. The parallel printer cable can only be 12 feet long. Also, the printer requires a power outlet.
6. If you're installing a ScramblePad for programming at the controller site – this is not normally required for networked system installations – consider using a portable ScramblePad and a flexible cable. This enables the programmer or operator to hold the ScramblePad (or sit with it) during command entry and proves more comfortable than programming on a wall-mounted ScramblePad.

Wiring to the Controller

Although the M64 Relay Board resides in the position within the M64 Controller cabinet usually reserved for the controller board, it can be best thought of as a large expansion relay board. The MSP controller board is actually mounted on the door and is connected to the relay board by ribbon cables. The M64 contains several override terminal blocks. These blocks enable an external shunt to force off all M64 relays. There is an override on the M64 for each bank of 8 relays.

During operation, the Status LEDs that reside on the controller boards can prove useful in diagnosing problems that may occur.

Connecting Line Module Inputs

The typical line module input features a connection between a Door Contact or Alarm Sensor, an RQE button, a line tamper, and the Controller. The Mx or M64 Controller uses a line supervision module device called a *line module* to supervise the input circuit. It should be located as close to the door contact or alarm sensor as possible. The DIGI*TRAC Line Module (DTLM) uses terminal blocks for connections. The Miniature Embedded Line Module (MELM) uses flying leads. The MELM is normally small enough to fit inside the monitored device.

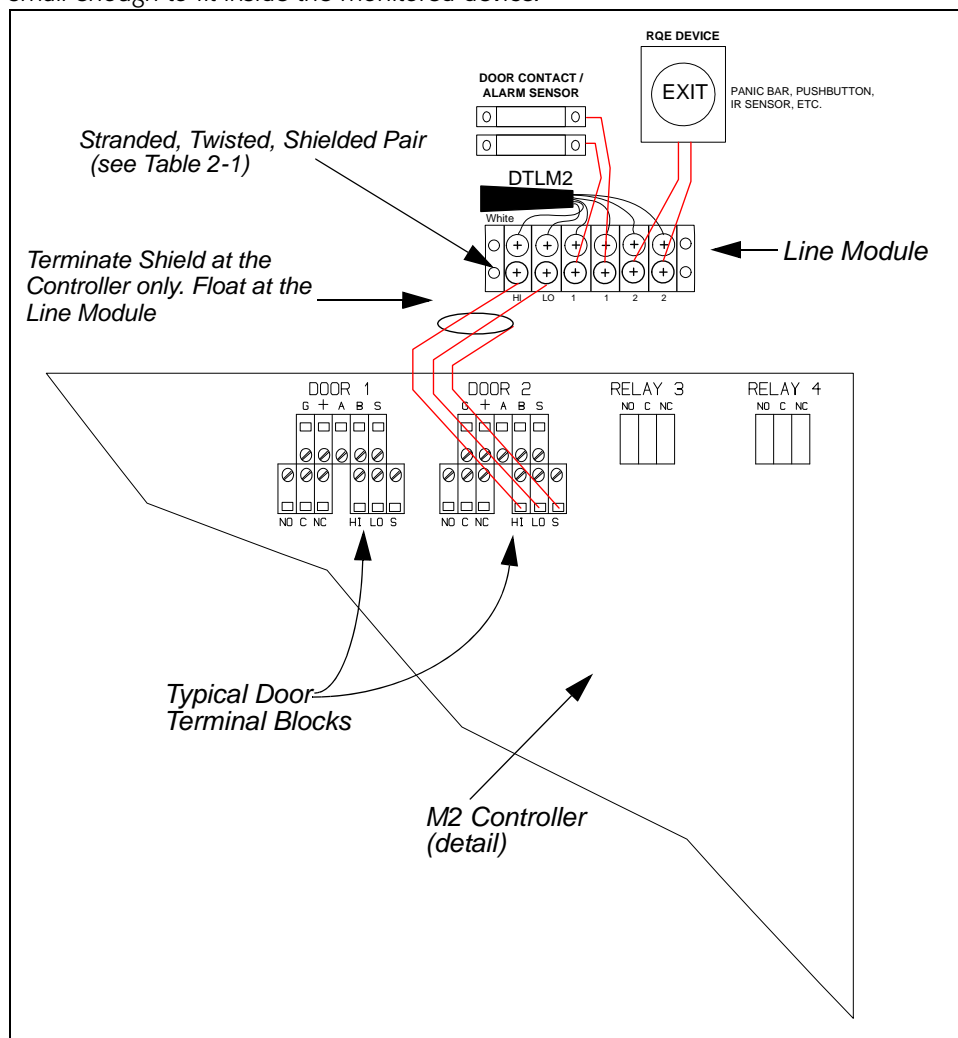



Figure 63: Typical Line Module Input Connection

To Connect Line Module Inputs to the Controller's Line Module Input Terminals:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Run the HI, LO, and Shield wire from the Line Module to the Controller.
3. Punch out the knockout(s) in the enclosure through which you plan to route the wires. Typically cables are brought in from the top.
4. Route the wires through the knockout hole.

 ***Don't run a wire through a knockout without a sleeve or conduit.***


5. Loosen the screws on each connector block you plan to use.
6. Remove excess insulation from the wire and insert the specified wires into the green connectors at the required slots, as shown in Figure 63 on page 81.
7. Connect the HI, LO, and shield wires at the controller.
8. Connect the HI and LO wires at the line module. Make sure you observe polarity: HI must go to HI; LO must go to LO.

 ***Only connect the shield wire at the controller; float it at the line module.***

The line module connected to an input terminal block on the Controller is automatically assigned the door ID to which it is connected. For example, if a line module is connected to the DOOR 1 terminal block, it is associated with the ScramblePad/MATCH assigned an ID of 1 or 9; a line module connected to DOOR 2 is associated with the ScramblePad/MATCH assigned ID 2 or 10.

The ID of a ScramblePad/MATCH is not associated with the terminal block to which it's connected; IDs for ScramblePads/MATCHs are assigned by their DIP switches, and are independent of their physical connection to the Controller board. For example, a ScramblePad assigned an ID of 3 on an M2 Controller can be connected to the DOOR 2 terminal block and still control the relay for DOOR 3. However, connecting the proper ScramblePad/MATCH to the same group of Door Terminals as the associated line module input makes troubleshooting much easier.

For more about installing and wiring Line Modules, refer to "Typical Line Module Inputs" on page 67.

 ***It is necessary for ScramblePads and MATCH Interfaces to have the same address as the relays they control for door access control.***

Connecting Outputs

The typical output requires a connection between an output device (such as a door lock/strike) and an output relay on the controller board. An example of such a connection is shown in this figure.

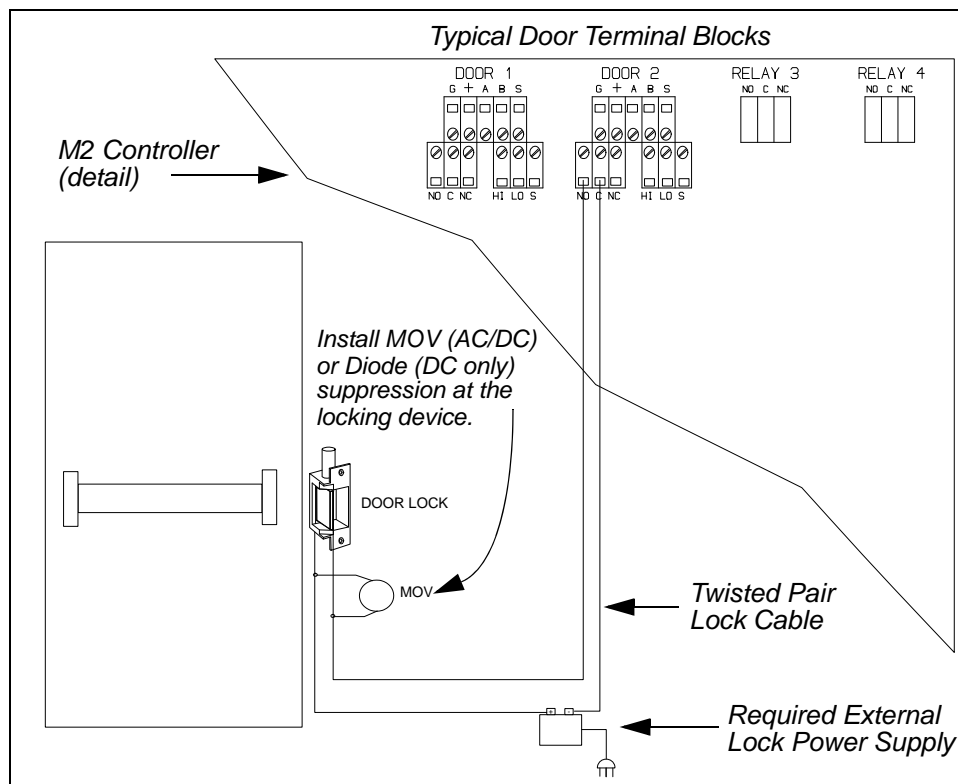


Figure 64: Typical Output Connection

To Connect Outputs to the Controller:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Run the control wires (N.O. or N.C. and Common) from the Output device to the Controller.
3. Punch out the appropriate knockout(s) in the enclosure to route the wires. Typically, output cables are brought in from the top.
4. Route the wires through the knockout hole.



Don't run a wire through a knockout without a sleeve or conduit.

5. Loosen the screws on each terminal block to be used.
6. Remove excess insulation from the wire and insert the specified wires into the green connectors at the required slots.
7. Connect the two wires. N.O. connects to N.O., N.C. to N.C., and C to C. Never connect to both NO and NC. An output device is either Normally Open or Normally Closed, but not both.

To determine which set of contacts to connect to (N.O. or N.C.), refer to the device's installation manual. The choice is usually determined by the type of lock it is.

8. Install MOV suppression at the lock end. Use Hirsch Part# MOV35, Thomson VE09M00250K, GE #V39ZA1, or equivalent. If this is a DC lock, you can use a diode instead. Use a 1A, 400V diode (available as Hirsch Part # DIODE).
Many locks come with suppression included. Make sure your lock does not have built-in suppression before adding an MOV or diode to the circuit.




Don't attempt to run lock or strike cable within 6 inches (15cm) of ScramblePad/MATCH cables or line module cables unless the lock cable is a twisted pair. Zip cord is not acceptable. When connecting to an electric strike/lock or other output device requiring more than the relay's contact ratings, an intermediate relay is required. Remember: Hirsch relays do not output voltage; separate power is required for output devices.

The terminal block to which the device is connected determines the device's ID assignment. For example, if an electric strike is connected to DOOR 2, it is associated with ID 2. If connected to DOOR 1, it is associated with ID 1.

Connecting ScramblePad and MATCH Interfaces

The typical ScramblePad/MATCH input features a connection between a ScramblePad keypad or MATCH Interface and the Controller. An example is shown in Figure 65.

 Card Readers communicate with the controller through the MATCH Interface Board.

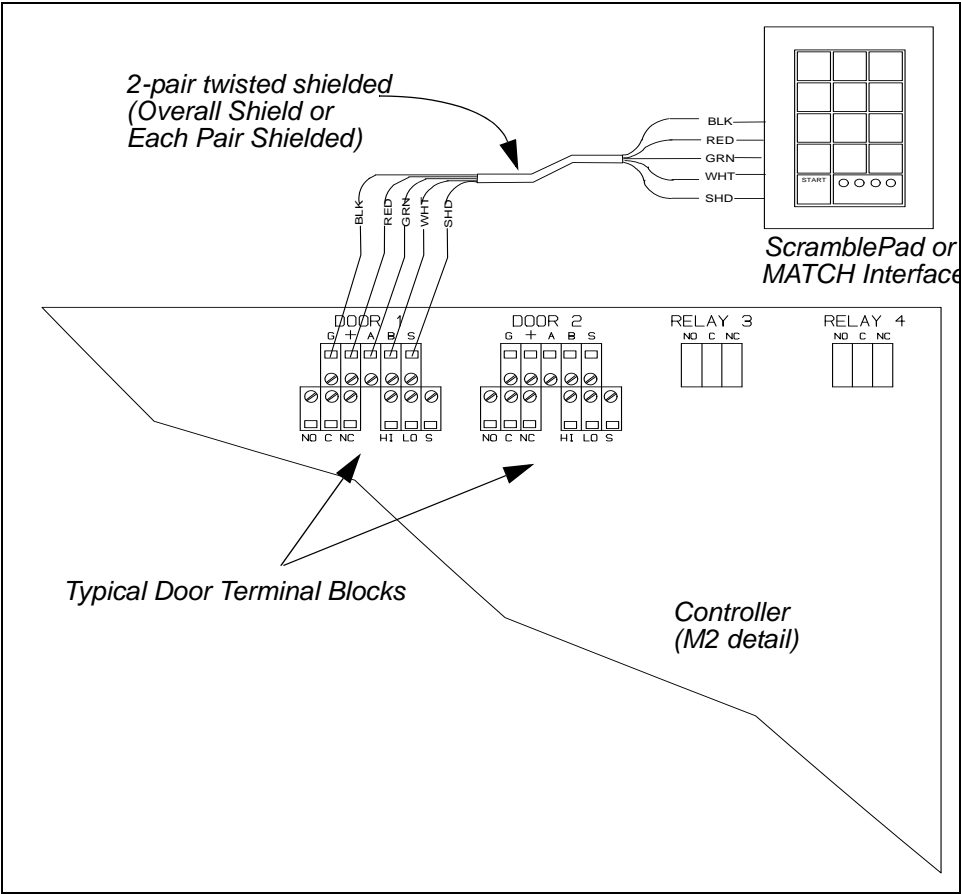


Figure 65: Typical ScramblePad/MATCH Input Connection

To Connect ScramblePad/MATCH Interfaces to the Controller:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Run the black, red, green, white, and shielded wires from the DIGI*TRAC connectors on the back of the ScramblePad or MATCH (MR1A or MR1B) to the corresponding terminals on the Controller's ScramblePad/MATCH terminal blocks.

Terminals are color-coded as shown in the following table:

Wire Color	Terminal Designation
Black	G
Red	+
Green	A
White	B
Shield	S

3. Punch out the knockout(s) in the Controller enclosure to route the wires. Typically ScramblePad/MATCH cables are pulled in from the top.
4. Route the wires through the knockout hole.
5. Loosen the screws on each connector block to be used.
6. Remove excess insulation from the wire and insert the specified wires into the green connectors at the required slots.
7. Connect the five wires to the appropriate ScramblePad/MATCH terminal blocks: G (Ground), + (Plus Voltage), A (Data A), B (Data B), and S (Shield). Always observe polarity.

For more about connecting to the ScramblePad, refer to “ScramblePad/MATCH Inputs” on page 70. For more about connecting to the MATCH, refer to “ScramblePad/MATCH Inputs” on page 70.

The ID of a ScramblePad/MATCH is not associated with the terminal block to which it's connected; IDs for ScramblePads/MATCHs are assigned by their DIP switches and are independent of their physical connection to the Controller board. For example, a ScramblePad assigned an ID of 3 on an M2 Controller can be connected to the DOOR 2 terminal block and still control the relay for DOOR 3. However, connecting the appropriate ScramblePad/MATCH to its associated line module input makes troubleshooting much easier.

If two ScramblePads are installed at the same door – one for entry and the other for exit – they can share the same terminal block connection; however, the ScramblePads must have different IDs. The Controller's firmware recognizes that IDs 1-8 are for entry, and IDs 9-16 are for exit.

Wiring Distance Limits

The following table shows the wiring distance limits between the Mx Controller and various components, which is important information when you are designing a security system for a large facility.

Type of Wired Connection	Maximum Distance
RS-485 (between two controllers) using 22 gauge wires	4,000 feet (1,220 meters)
MATCH protocol (between controller and keypad, reader, or MATCH2 board) using 18 gauge wires	1,800 feet (550 meters)
MATCH protocol (between controller and keypad, reader, or MATCH2 board) using 22 gauge wires	750 feet (225 meters)
Wiegand protocol (direct wiring between controller and Wiegand device) using 18 gauge wires	500 feet (150 meters)



The wires must be stranded and pair twisted, with an overall shield.

Configuring the Integrated SNIB3

An Mx Controller has integrated SNIB3 capability, with a 5-wire RS-485 connector that enables multi-drop or long hardwired serial connections, and an RJ-45 Ethernet connector for communication between the ICPAM host and the master controller.



An Mx Controller does not include the 4-wire RS-232 connector which is provided on the separate SNIB3 expansion board.

To install a set of controllers connected using SNIB3s, perform the following procedure:

1. Run the required network cable to the controller(s) with the master SNIB3s.
The Ethernet cable you are connecting to each master SNIB3 should be connected to the ICPAM host through a hub or switch.
2. Run RS-485 cable downstream from the master SNIB3.
The run between the master SNIB3 and the second SNIB3 must be wired according to the instructions in "Configuring a Master SNIB2 on the Same Subnet" on page 61.
3. Set the DIP switches on each SNIB3, which vary depending on whether it is the master, one in the middle, or the last one.

The location of the three banks of DIP switches on a SNIB3 expansion board is shown in Figure 52 on page 51.

On an Mx Controller's main board (shown in Figure 53 on page 52):

- SW1 is located near the upper-right corner, by the SNIB3 terminal.
- SW2 is located in the left middle, to the right of the Ethernet daughterboard.
- SW3 is located below SW2.

In general, set the DIP switches as shown in the following table.

SW1

1

2

3

4

SW2

1

2

3

4

SW3

1

2

3

4

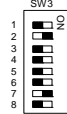
5

6


7

8

Bank	Switch	Setting	Comments	
Master SNIB3:				
SW1	S1-S4	all ON	Indicates this is the first/master SNIB3 (or the last one) in the run	
	SW2	S1	OFF	The SNIB3 communicates with the ICPAM host PC in XNET 2, using the encryption keys stored in memory
			ON	Return the encryption keys to their default settings. If this switch is set when the SNIB3 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. Because this is the master SNIB3, you must also 'Reset Encryption' on the ICPAM Port settings. All downstream units must have their encryption keys reset as well.
		S2-S3	OFF	Reserved
		S4	ON	This SNIB3 is first in the sequence (the master) and is connected to the host via Ethernet or direct RS-232 connection (not dial-up). This SNIB3 controls polling.
	SW3	S1	OFF	Set downstream RS-485 speed (38400 in this example)
S2		ON		
S3-S8		—	Address as required (Address 1 shown)	



Bank	Switch	Setting	Comments
SNIB3s in the middle:			
SW1	S1-S4	all OFF	Indicates this SNIB3 is in the middle of the run
SW2	S1	OFF	The SNIB3 communicates with the ICPAM host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB3 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. All downstream units must have their encryption keys reset as well. Because this is a downstream unit, the master SNIB3 automatically detects that the keys have been reset.
	S2-S3	OFF	Reserved
	S4	OFF	This SNIB3 is not the first/master (or you only have one controller)
SW3	S1	OFF	Set downstream RS-485 speed (38400 in this example)
	S2	ON	
	S3-S8	—	Address as required (Address 2 shown)



Bank	Switch	Setting	Comments
Last SNIB3 in run:			
SW1	S1-S4	all ON	Indicates this is the last SNIB3 (or the first/master) in the run
	S1	OFF	The SNIB3 communicates with the ICPAM host PC in XNET 2, using the encryption keys stored in memory
SW2		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB3 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. All downstream units must have their encryption keys reset as well. Because this is a downstream unit, the master SNIB3 automatically detects that the keys have been reset.
	S2-S3	OFF	Reserved
	S4	OFF	This SNIB3 is not the first/master (or you only have one controller)
SW3	S1	OFF	Set downstream RS-485 speed (38400 in this example)
	S2	ON	
	S3-S8	—	Address as required (Address 3 shown)

Refer to "Setting Up the SNIB2" on page 54 for more configuration options.

4. Plug the RJ-45 connector from the cable into the Ethernet connector on the Mx Controller's main board.
5. Connect the RS-485 cables to their respective SNIB3.
6. Reconnect and power up the controllers.
7. At the host, open ICPAM and configure the new SNIB3s.

SNIB3 Network Configuration Options

Mx and M64 controllers can be networked together and managed by a computer running ICPAM, if they use an optional SNIB3 expansion board. For details, see the [DIGI*TRAC Design and Installation Guide](#).

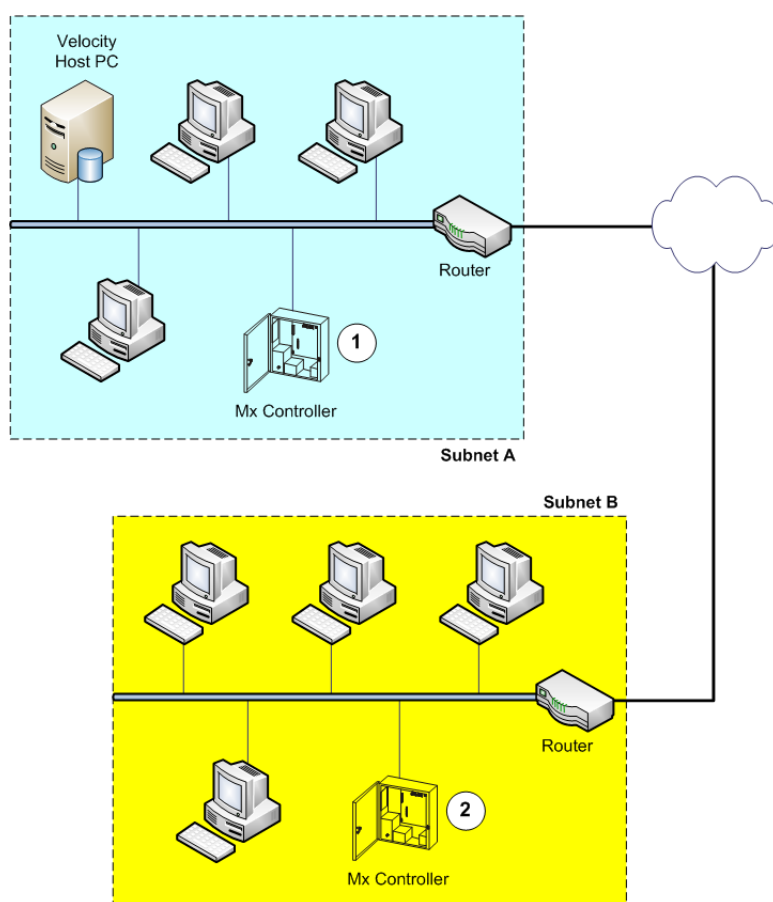
An Mx controller can be included in that network. The primary difference is that an Mx controller does not require a SNIB3 expansion board, because the Ethernet connector and the RS485 terminal are integrated onto the controller's main board, as shown in Figure 53 on page 52.

Deploying the SNIB3

Each master SNIB3 (ICPAM port) must be assigned a unique IP address so it can communicate with ICPAM on the host PC. Depending on the network location of the master SNIB3, this is accomplished in one of two ways:

- If the SNIB3 is located within the same subnet as the host PC, then you can use ICPAM to assign the IP address. For more about this, refer to “Configuring a Master SNIB2 on the Same Subnet” on page 61.
- If the master SNIB3 is located outside the host PC’s subnet, you must use the SNIB3 Configuration Utility. For more about this, refer to “Configuring a Master SNIB2 in a Different Subnet” on page 64.

What is a subnet? Put simply, it is any group of PCs and other devices, such as printers and scanners, connected by network cable to a network router. Anything behind the router is considered part of the subnet. Anything beyond this router is not part of the subnet.



In the preceding illustration, the master SNIB3 on the Mx controller labeled 1 is located in the same subnet as the host PC (Subnet A). This SNIB3 can therefore be configured using ICPAM; however, the master SNIB3 on the Mx controller labeled 2 is located behind a different router, in a different subnet (Subnet B), and must be configured using the SNIB3 Configuration Utility.

Any number of computers and devices can be behind a single router, but for reasons of security and speed, a company network often incorporates many routers. It isn't uncommon to find that each department within a company has its own router. Routers not only find the quickest way to ferry packets of information between two points, but also could serve as a rudimentary firewall against potential intrusion.

Preparing an Mx Controller to Use a SNIB3

Before the SNIB3 board was available, every Mx controller provided SNIB3 functionality using a daughterboard (with an Ethernet connector) attached to the main board, as shown in Figure 53 on page 52. Now when you order a new Mx controller, you have the option to instead have a SNIB3 board installed in an expansion slot.

But if you want to use the SNIB3 with an existing Mx controller that has a SNIB3 daughterboard, you must first remove that daughterboard from the Mx controller's main board. To do so, perform the following steps:

1. Make sure the controller shows its CCM firmware version as 7.5.37 or later.
If necessary, update the CCM firmware.
2. Power down the Mx controller.
 - a. Disconnect the battery backup power from the controller.
 - b. Disconnect the AC power cables to the controller.
3. Remove the screw in the middle of the SNIB3 daughterboard.
The SNIB3 daughterboard is mounted on the Mx controller's main board above the Mx logo, and it includes one RJ-45 Ethernet connector.
4. Carefully unplug the daughterboard from the Mx controller's main board.
This usually requires holding opposite corners or ends of the daughterboard, and carefully rocking it out of its socket.
5. After the daughterboard has been removed, install the SNIB3 expansion board in the normal way. For more on this installation process, refer to

Mx Controller Configuration Worksheet

The following figure provides a worksheet for an Mx Controller, to help you plan your security system.

Mx Controller Configuration Worksheet



Controller Name: _____

Description: _____

Address: _____

Time Zone Location: _____

Port Type: ☐ S*NET ☐ X*NET

Port Name: _____

Expansion Boards

Board 1 = _____

Board 2 = _____

Board 3 = _____

Board 4 = _____

Board 5 = _____

Doors / Readers / Outputs / Inputs

Door 1 _____

Door 2 _____

Door 3 _____

Door 4 _____

Door 5 _____

Door 6 _____

Door 7 _____

Door 8 _____

Expansion Inputs (Red Icons = Installed; Black Icons = not installed)

X11	X16	X111-	X116	X21	X26	X31
X12	X17	X112	X117	X22	X27	X32
X13	X18	X113	X118	X23	X28	X33
X14	X19	X114	X119	X24	X29	X34
X15	X20	X115	X120	X25	X30	X35

Network Info:

☐ TCP/IP

IP Address: _____

IP Port: _____

Max Retry Attempts: _____

Expansion Relays/Virtual Relays (Red Icons = Installed; Black Icons = not installed)

XR1-	XR12-	XR23-	XR34-	XR45-	XR56-
XR2-	XR13-	XR24-	XR35-	XR46-	XR57-
XR3-	XR14-	XR25-	XR36-	XR47-	XR58-
XR4-	XR15-	XR26-	XR37-	XR48-	XR59-
XR5-	XR16-	XR27-	XR38-	XR49-	XR60-
XR6-	XR17-	XR28-	XR39-	XR50-	XR61-
XR7-	XR18-	XR29-	XR40-	XR51-	XR62-
XR8-	XR19-	XR30-	XR41-	XR52-	XR63-
XR9-	XR20-	XR31-	XR42-	XR53-	XR64-
XR10-	XR21-	XR32-	XR43-	XR54-	XR65-
XR11-	XR22-	XR33-	XR44-	XR55-	XR66-

To Configure an Mx Controller:

From Velocity Configuration: Select DIGI*TRAC Configuration folder > Click Port > From Components pane, double-click Add New Controller. Fill out General page.

Performing Periodic Maintenance

The Mx controller was designed to be a reliable long-lasting product, with periodic maintenance consisting of:

- gathering diagnostic information (including the voltage status of the standby battery and the memory battery) once every 6 months
- visually inspecting the controller once every year for signs of:
 - corrosion around the battery terminals
 - damaged battery leads
 - exposed wires or loose connections
- replacing the standby battery or the memory battery when necessary (after several years)

Gathering Diagnostic Information

The ICPAM software includes a Diagnostic Window which enables you to gather diagnostic information about a connected controller. To access this tool, go to ICPAM's Hardware Tree, select the Mx controller you want to review and look at the information in the right pane.

Interpreting the System Power Status Information

The results of the 25 - System Power Status diagnostics command are somewhat cryptic. Here is what those results mean.

Main Power: This is the voltage of the main power after it has been transformed from AC to DC. The normal range is 28 - 29 VDC. AC Failure is reported if the voltage drops below 27.5 VDC.

UPS Battery: This is the DC voltage of the standby battery, which performs the function of an Uninterruptible Power Supply. The "under charge" number shows the voltage when the standby battery is being charged. The "open cell" number shows the voltage when the charging circuit is bypassed. The normal range is 24 - 28 VDC. The voltage is considered Low when it is 17 - 24 VDC. UPS Failure is reported if the voltage drops below 17 VDC. A weak battery will have a high "under charge" number and a low "open cell" number.

Memory Battery: This is the DC voltage of the memory protection battery, which provides up to 30 days protection of the controller's data. The normal range is 3.47 - 4.5 VDC. If the value remains below 3.47 VDC, the memory battery should be replaced.

Replacing the Memory Battery

The Mx controller's memory battery is a 3.6 V rechargeable nickel-metal hydride battery pack which can protect against data loss for up to 30 days. It should provide several years of reliable service, but will eventually have to be replaced when its voltage remains below 3.47 VDC. The location of this battery on the Mx controller's main board (within the enclosure) is shown in the following photograph:



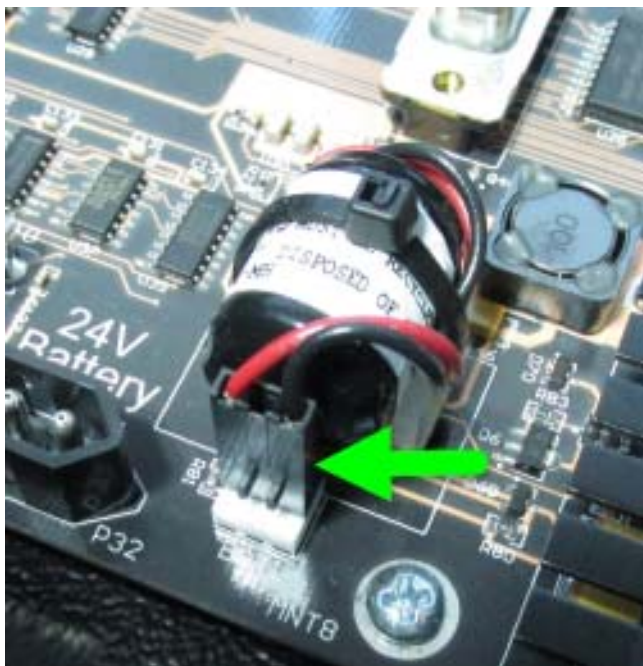
When diagnostic information determines that there is a problem with the performance of the memory battery, you should replace it by performing the following procedure:

1. Contact Identiv (or your dealer) and order part number MPB1.
2. After the new memory battery arrives, take it and a small wire cutter to the Mx controller.
3. Open the Mx controller's enclosure, and locate the existing memory battery (as shown in the previous photograph).



The controller's power should remain on while you replace its memory battery.

4. Carefully unplug the memory battery connector from the controller's main board at location BAT1 (as shown in the following photograph).



5. Use a small wire cutter to cut through the existing cable tie (shown in the following photograph), and remove it.



6. Replace the old memory battery with the new one, and plug in its connector at location BAT1 on the controller's main board. Make sure the connector is aligned so that the red positive wire is on the left side.
7. Use a new cable tie to secure the new memory battery and its connecting wires to the plastic mount on the controller's main board.
8. Close the Mx controller's enclosure.

If the Mx controller is online and communicating with the ICPAM software during this procedure, the Alarm Viewer will display a "Memory Battery Failure" alarm when the old memory battery is unplugged, and a "Memory Battery Restored" event when the new memory battery is plugged in.

If the Mx controller lost data because you replaced the memory battery while the main board was disconnected from both the main AC power and the standby battery power, you can download its data again using ICPAM.

