eINTELLI-M®
POWER OVER ETHERNET

Web Interface User’s Guide

infinias

www.infinias.com

Preface

This manual is a guide for the Intelli-M® Web Interface. The web interface enables configuring of an eIDC (ethernet Integrated Door Controller) access control security system by way of a web browser. An overview of setting up eIDC access control for a single door is provided, as well as a description of the web pages displayed for configuring an eIDC controller.

Trademarks

All brand or product names mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

infinias, the infinias logo, and Intelli-M are registered trademarks of infinias, LLC

In*telli-M Web Interface User's Guide*

Printed in the United States.

Note: The information in this document is subject to change without notice or obligation.

Table of Contents

Introduction To The Intelli-M® Web Interface

Contents

This section provides an introduction to the Intelli-M “Web Interface User’s Guide.” A brief description of the eIDC Web Interface and each Chapter and Appendix within this document can be found here.

The following topics can be found within this section:

Introduction

Intelli-M®'s eIDC (ethernet Integrated Door Controller) provides access control and alarm services for a single door. One way to access the services provided by the eIDC is via the internet, because each eIDC device is configured with an internal web server that is capable of serving web pages for configuring and using the device. The internal web service within an eIDC can be accessed with most web browsers available in today's market. This manual describes how to install an eIDC for a single door, access the eIDC via the internet, and customize the eIDC software configuration to the access control security needs required by your site.

Using This Manual

Here is a quick overview of this manual's Chapters and Appendices

- **Chapter 1: eIDC Installation** -- This Chapter provides instructions on installing an eIDC controller, wiring the eIDC for a single door, powering up the eIDC, and determining the IP address.
- **Chapter 2: Browser Configuration And Initial Startup** -- This Chapter provides instructions on configuring web browsers to enable the Intelli-M Web Interface from an eIDC controller, logging into the web interface, and loading the default configuration into the eIDC controller.
- **Chapter 3: Global Configuration For Card Reader** -- This Chapter provides instructions on using the Wiegand Format Editor found within the Global Configuration section of the Intelli-M Web Interface. The Wiegand Format Editor within the Intelli-M Web Interface provides a platform where you can modify Wiegand style cards to your site specifications.
- **Chapter 4: Schedules, Holidays, Calendars** -- This Chapter provides instructions on how to set up time and schedules within the Intelli-M Web Interface.
- **Chapter 5: Programming Access Control Devices** -- This Chapter provides instructions on how to set up the network configuration within the Intelli-M Web Interface by programming various access control devices. Access control devices for the Intelli-M Web Interface are the eIDC controller, and the input and output devices connected to the eIDC controller.
- **Chapter 6: Services** -- This Chapter provides instructions on how to program Access Services and Alarm Services within the Intelli-M Web Interface.
- **Chapter 7: Card Holders And Badging** -- This Chapter describes how access cards can be added to the system and programmed to grant access permissions to individuals. Also included are how options for the cards can be defined in the system.
- **Chapter 8: Monitoring The System** -- This Chapter discusses how an operator can monitor the system for events such as access being granted or restricted at the door. Also discussed is how to view an alarm that may be trigger within the system, and appropriate responses to alarm types.
- **Chapter 9: History Searches And Reports** -- This Chapter discusses how to perform a search of all the stored events for a specific event or events, and also how a report can then be generated.
- **Appendix A: eFamily Update Utility** -- This Chapter describes how to use the eFamily Update Utility. This utility provides the ability to update the firmware of an eFamily device (such as an eIDC), backup a device configuration (including card holders, schedules, and services) and event history log, and/or restore a backup configuration.
- **Appendix B: Web Interface Translator Utility** -- This Chapter describes how to use the utility to translate text strings within a web interface eFamily device (such as an eIDC) to languages other than U.S. English default.

Chapter 1: eIDC Installation

Contents

This Chapter provides instructions on installing an eIDC controller, and wiring the eIDC up for electronic access control of a single door. Information on powering up the eIDC controller and determining the IP address of the eIDC is also provided in this section.

The following topics can be found within this Chapter:

eIDC Controller Overview

Intelli-M's eIDC (ethernet Integrated Door Controller) provides access control and alarm services for a single door. The cutting-edge technology of Power over Ethernet (PoE) allows you to run a single cable carrying both power and data for the controller and all peripheral door hardware. The controller has LEDs built into it for verifying connections to peripherals in the security system.

Intelli-M eIDC

The footprint of the controller is 1.70" W x 2.82" H x 1.30" D. It has flash-base memory capability, and can be updated with the latest firmware data via a simple flash upgrade. Instructions on how to perform an update to the eIDC can be found within this manual in "Appendix A: eFamily Update Utility."

Technical Features

The Intelli-M eIDC has the following technical features:

- Embedded Web server provides complete control of the device without the need of a server for a stand-alone door
- Supports a local database of 64,000 card holders in managed mode, or up to 8,500 card holders in stand-alone Web server mode
- 16,000 local event buffering
- Two reader ports for entry and exit configurations (with or without keypads)
- Supports DHCP or Static IP addresses
- Provides encrypted communication (AES 128 bit)
- Integrated, non-mechanical, infrared tamper sensor for high reliability and precision
- Built-in warning buzzer provides a local alarm without requiring an external alarm device

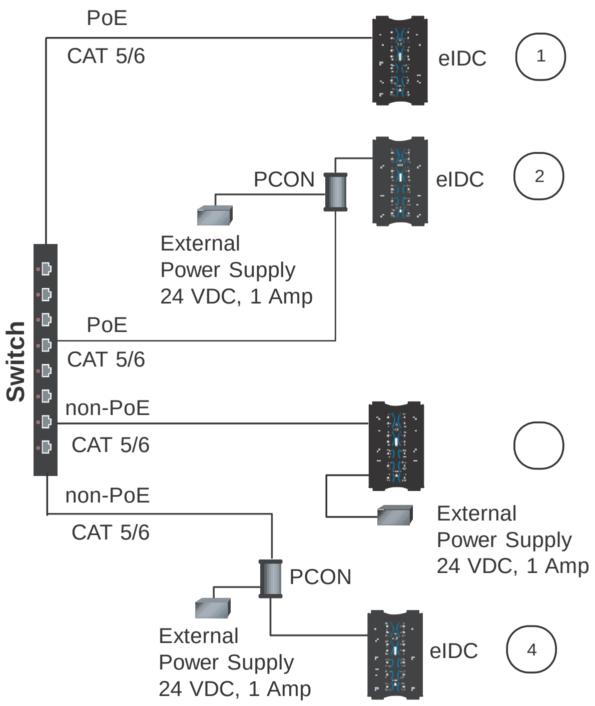
Installation Of Intelli-M Hardware Components

The installation of Intelli-M hardware components should be done in the following order:

1. Connect eIDC and/or PCON to Ethernet Switch.
2. Determine the eIDC IP Address.
3. Configure the eIDC with its built-in Web Server.
4. Wire the eIDC door components.

Connecting eIDC And/Or PCON To Ethernet Switch

Four Power Options



Option 1

Step 1: Using PoE, run a standard network cable (Cat 5 or 6) directly from Switch to eIDC.

Step 2: Refer to the “Determine The eIDC IP Address” section below.

Option 2

Step 1: Using PoE, run a standard network cable (Cat 5 or 6) directly from Switch to PCON.

Step 2: Optional: Wire to PCON a 24 VDC power supply. The terminal block is removable for ease of wiring.

> **Important:** With PoE, the External Power Supply connected to the PCON may not be required. Note that if both a PoE enabled switch and DC power are connected to the PCON, priority is given

to the DC power supply. In such instances, PoE power is still being allocated by the PoE switch and counts toward the aggregate total power budget of the switch. That is, an eIDC will request the maximum power of 15.4 watts from the PoE switch port to which it is connected. A PoE enabled switch has a total power budget that is divided among all the PoE switch ports; therefore, the total power draw from all PoE equipment connected to the switch cannot exceed the switch power budget. Make sure that the aggregate power draw of all PoE powered devices does not exceed the total power budget of the switch. Exceeding the power budget of a PoE enabled switch will cause an eIDC to randomly fail.

If a 24 VDC power supply is installed, the PCON power status LED will be one of the following when power is applied:

• Green	which is	> 22 VDC -- Very Good
• Yellow	which is	20-22 VDC -- Below average but usable
• Red	which is	< 20 VDC -- Not enough power

Step 3: Run another standard network cable (Cat 5 or 6) from PCON connector (RJ-45 labeled “Out To eIDC”) to the eIDC ethernet connector.

Step 4: Refer to the “Determine The eIDC IP Address” section below.

Option 3

Step 1: Using non-PoE, run a standard network cable (Cat 5 or 6) directly from Switch to the eIDC.

Step 2: Wire a 24 VDC power supply to the eIDC and apply power.

Step 3: Refer to the “Determine The eIDC IP Address” section below.

Option 4

Step 1: Using non-PoE, run a standard network cable (Cat 5 or 6) directly from Switch to PCON,

Step 2: Wire to PCON a 24 VDC power supply. The terminal block is removable for ease of wiring.

Step 3: Apply Power to PCON. The PCON power status LED will be one of the following:

• Green	which is	> 22 VDC -- Very Good
• Yellow	which is	20-22 VDC -- Below average but usable
• Red	which is	< 20 VDC -- Not enough power

Step 4: Run another standard network cable (Cat 5 or 6) from PCON connector (RJ-45 labeled “Out To eIDC”) to the eIDC ethernet connector.

Step 5: Refer to the “Determine The eIDC IP Address” section below.

Determining The eIDC IP Address

The eIDC controller will appear as a full IP client on the data network, and thus will require an IP address. The network connection for the eIDC will be for either static addressing or DHCP (Dynamic Host Configuration Protocol) addressing. Use of either a DHCP permanently leased IP address or a static IP address is required by the eIDC.

Whenever power is initially applied to the eIDC, the eIDC will signal the current IP address that it is receiving. (Signaling also will occur when the eIDC is rebooted, that is, disconnected and then connected.) To determine the IP address type, connect power to the eIDC and note the address reported by the device as follows:

1. Use the LEDs on the eIDC unit when you are ready to note the IP address. If you look at the eIDC closely, each of the top five LEDs on each side have a number (left side 1-5 and right side 6-0).
2. Disconnect the power from the eIDC and then reconnect the power. The eIDC unit will boot and then attempt to acquire an IP address. (This happens because the eIDC is shipped from the factory set for DHCP addressing).
3. If the following sequence occurs when power is connected to the eIDC, the network IP address type may or may not be DHCP:
   - All LEDs will flash three times to begin the sequence. (The eIDC is fully operational during IP address flashing.)
   - A numbered (LED) will flash representing each number in the IP address. Each number group is separated by all LEDs flashing once.
     For example: 145.198.1.1 interprets as #1 flash #4 flash #5 flash <all flash> #1 flash #9 flash #8 flash <all flash> #1 flash <all flash> #1 flash <all flash>.
   - Once the sequence has repeated 3 times, the eIDC LEDs will return to normal operation mode.

   Important: If DHCP addressing is to be used, the DHCP address must be a permanently leased address. This means the address assigned by the network to the eIDC will not expire (expiring causes the network to assign the eIDC a different address that will cause random failures with the eIDC and Supervisor Plus software). Thus, *do not use DHCP addressing with an expiration time limit*. Always check with the network administrator to make sure that the network will be using Permanently Leased DHCP addressing if DHCP addressing is to be used with an eIDC.
4. If the following sequence occurs when power is connected to the eIDC, the network IP address type is static:
   - All of the LEDs on the eIDC unit flash continuously for about 10 seconds (more than 3 times) after the eIDC receives power.

   This means a DHCP IP address cannot be determined (i.e., there is no DHCP connection). When this occurs, the eIDC will revert to its built in default static address of 169.254.1.1

   Note: The default static address can be changed when the eIDC is configured. Refer to "Change The eIDC To DHCP Or Static IP Mode" below in the "Configuring The eIDC With The Web Server" section.
5. Use the IP address given by the eIDC (either DHCP or Static) in a Web Browser (i.e., Internet Explorer) to browse to and then configure the eIDC. Refer to the "Configuring The eIDC With The Web Server" section below for further instruction on how to do this.

Configuring The eIDC With The Web Server

If static addressing is to be used, obtain a valid static IP Address, Subnet Mask, and Gateway from the Network Administrator of the facility where the eIDC is located. You will need this in order to change out the default static IP address (of 169.254.1.1) that is built into the eIDC.

Connecting To The eIDC

Step 1: Launch the web browser (e.g., Internet Explorer).

Step 2: In the "Address" field type in the IP address of the eIDC, and then hit the <Enter> key to go to that address.

Step 3: The "Intelli-M Supervisor (Web Edition)" screen should appear. Click the "Click Here to Start" button to be presented with a login screen.

Step 4: The login screen may appear. The word "admin" (no quotes) should be used for both the default user and password. The word admin should be typed in all lower case.

Note: If the Name and/or Password have been changed in the device and are unknown, the eIDC will need to be reset to its factory defaults to enable access. Refer to the eIDC section of the "Intelli-M Hardware Installation and Reference" manual to perform a hardware reset.

Change The eIDC To DHCP Or Static IP Mode

Step 1: Click the "System" button and then click "Controllers."

Step 2: Select the eIDC controller (i.e., click to highlight the line) and then click the "Modify" button.

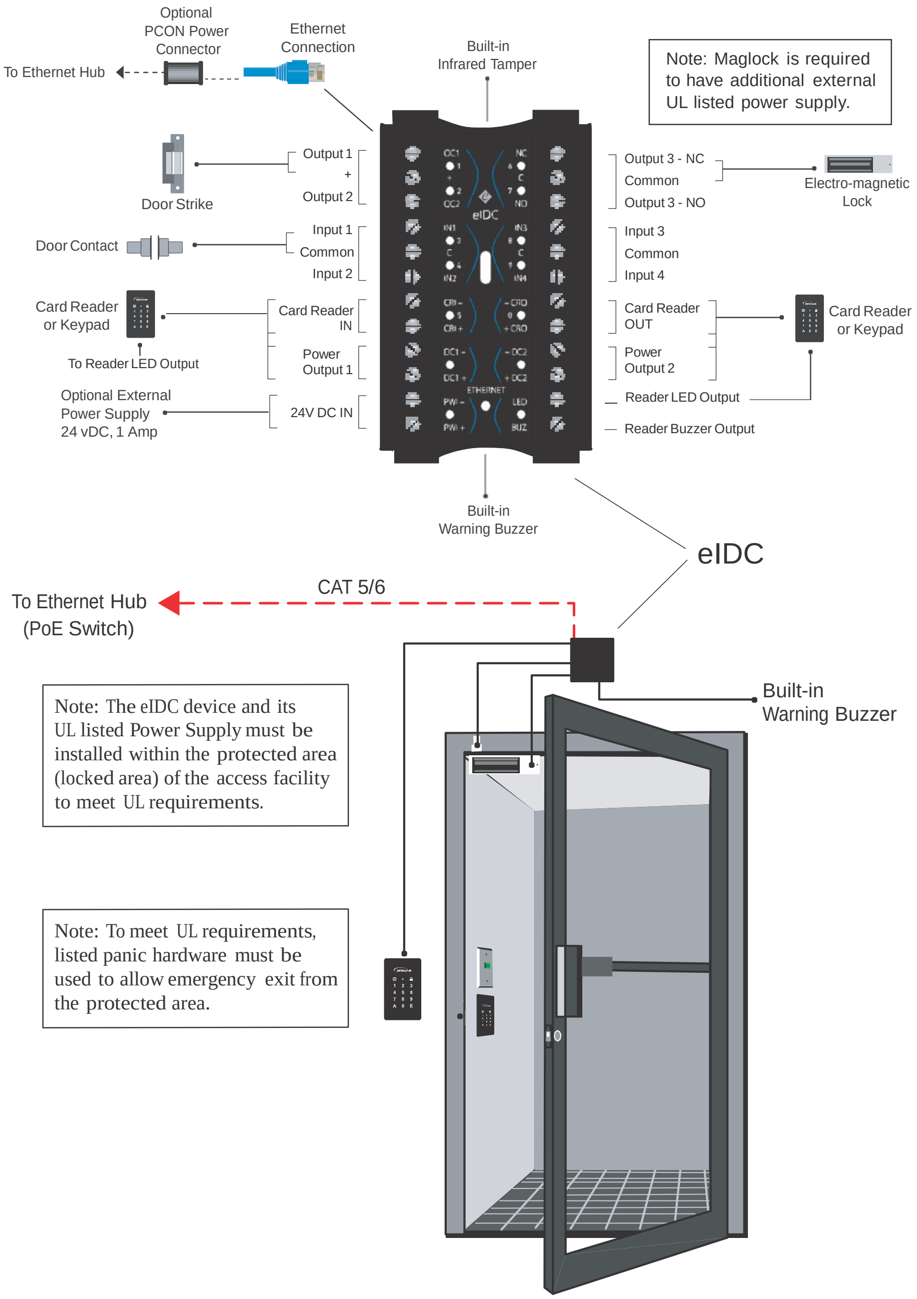
Step 3: If static addressing is to be used, uncheck the "Use DHCP" box by clicking it. This enables the IP Address, Subnet Mask, and Gateway fields so that they can be changed. Then type the new IP Address, Subnet Mask, and Gateway information into the appropriate fields.

If DHCP addressing is to be used, make sure that the "Use DHCP" box has a check mark in it. If unchecked, click the box to add a check mark to it. This enables DHCP addressing for the eIDC. Additional information on DHCP addressing can be found in the "Intelli-M Hardware Installation and Reference" manual.

Step 4: Click "Ok" and then "Done" to set the changes. Proceed to the "Wiring eIDC Door Components" section below.

Wiring eIDC Door Components

Up to 1 Amp of power is provided through the eIDC for peripheral devices. An illustration of wiring an eIDC for a single door, and the steps necessary to do so, are as follows:



Note: Maglock is required to have additional external UL listed power supply.

Note: The eIDC device and its UL listed Power Supply must be installed within the protected area (locked area) of the access facility to meet UL requirements.

Note: To meet UL requirements, listed panic hardware must be used to allow emergency exit from the protected area.

Step 1: Connect lock. Refer to the illustration above. The following information may be pertinent when dealing with locks:

- A lock can be powered by the eIDC (12 VDC @ 450 mA or less).
- The two Open Collector outputs (OC1 and OC2) provide a maximum of 12 VDC @ 450 mA combined. For example, a lock drawing 450 mA @ 12 VDC can be powered by the eIDC on OC1 or OC2.

- Locks drawing more power can be wired to output 3 (form C relay 5A @ 30 VDC) and powered externally.
- Outputs 1 and 2 each have their own “-” terminal but share a “+” terminal.
- Outputs 1 and 2 are software configurable “E” (energized) or “DE” (de-energized).
- Output 3 has separate terminals for “Com” (Common), “NO” (Normally Open), and “NC” (Normally Closed) but the software designation must match for proper status reporting.

Step 2: Wire the status, shunt, and exit inputs. Keep in mind the following points:

- Input devices can be wired to eIDC Inputs 1-4.
- “NO” or “NC” is software configurable with Inputs 1-4.
- “EOLR” (End Of Line Resistance) supervision is software selectable, and is supported with 1k ohm resistors.

Step 3: Wire readers.

- Reader IN and Reader OUT are internally configured each having their own Data 0 (CR-), Data 1 (CR+), DC+, and DC-.
- There is a single terminal for optional Reader LED control and optional Buzzer control.
- Only Readers can be wired to the Reader’s Data 0 (CR-), and Data 1 (CR+) terminals.

Chapter 2: Browser Configuration And Initial Startup

Contents

This Chapter provides instructions on configuring web browsers to enable the Intelli-M® Web Interface. Instructions on logging into the web interface, changing the user name and password, and loading the default configuration into the eIDC controller are also provided in this section.

The following topics can be found within this Chapter:

Web Browser Overview

Each eIDC device is configured with an internal web server that is capable of serving web pages for configuring and using the device. Most popular web browsers are supported. The following web browsers are known to work with the Intelli-M Web Interface:

- Internet Explorer 6.0 and Higher
- Mozilla Firefox 1.0.7 and Higher
- Opera 8.5 and Higher

Other browsers may work as well. However, in order for the web pages to appear and operate properly, certain configuration requirements specific to the browser being used must be met. Also, in order for the pages to display and operate properly, the web browser must have support for JavaScript as well as Asynchronous XML calls. These technologies are often referred to together as AJAX (Asynchronous JavaScript and XML).

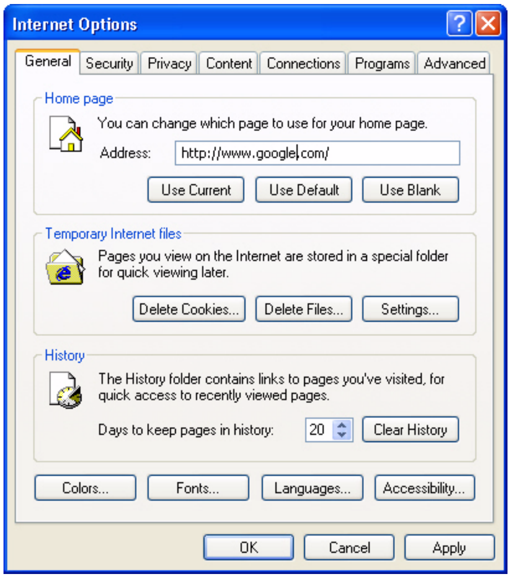
> **Important:** The Intelli-M Web Interface uses the ECMA v3 specification for the implementation of scripting in web browsers. This is equivalent to JavaScript 1.5 or JScript 5.5. In order to properly communicate with the eIDC device and provide configuration services, the web browser must allow JavaScript to run on the page.

Instructions on configuring Internet Explorer, Mozilla Firefox, and Opera to work properly when accessing the Intelli-M Web Interface are provided below.

Configuring Internet Explorer 6.0 and Higher

In Internet Explorer, be sure that JavaScript is enabled for the device web pages. Although your security policy may disable JavaScript for most sites, the device can be given special authority to run JavaScript. To do this, perform the following steps:

1. From within Internet Explorer, select the “Tools” menu and choose the “Internet Options” menu item.



Home page

You can change which page to use for your home page.

Address: http://www.google.com/

Temporary Internet files

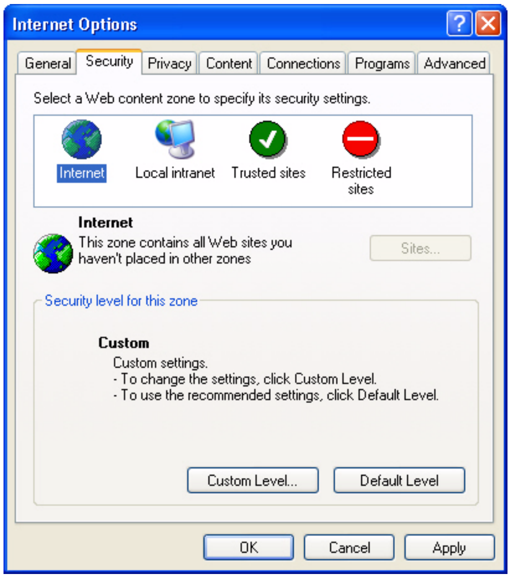
Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

2. Select the “Security” tab.



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

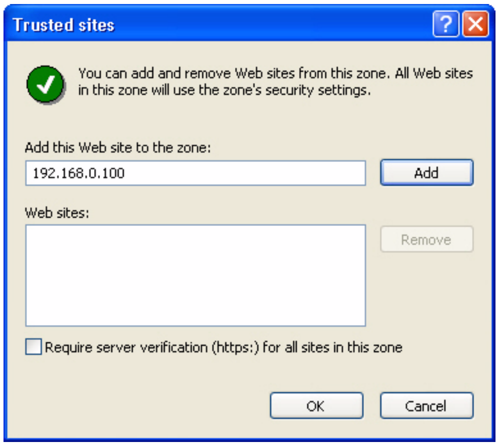
Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

3. Select the “Trusted Sites” icon, and then click the “Sites…” button.

4. Make sure the “Require server verification...” checkbox is unchecked. Then enter the URL or IP address of your eIDC device into the text box.



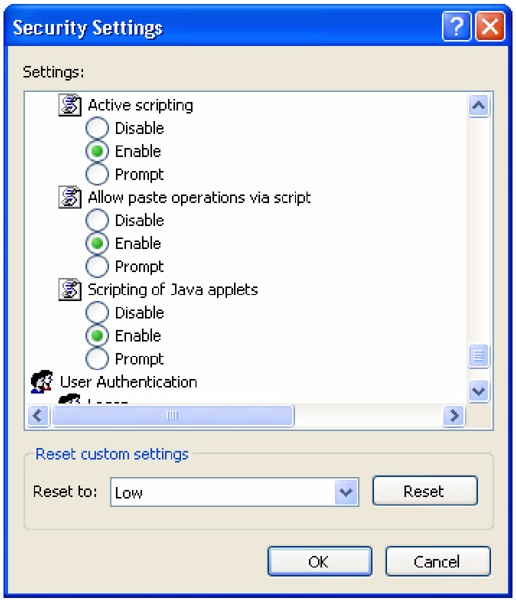
You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone: 192.168.0.100

Web sites:

□ Require server verification (https:) for all sites in this zone

5. Click the “Add” button, and then click “OK.”
6. From the “Security Tab,” click the “Custom Level” button.
7. Scroll down to the Scripting section. Verify that the Active Scripting option is set to enable. Click “OK” to exit this dialog, and then “OK” again to accept the changes to the security policy.



Settings:

Active scripting
○ Disable
● Enable
○ Prompt

Allow paste operations via script
○ Disable
● Enable
○ Prompt

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

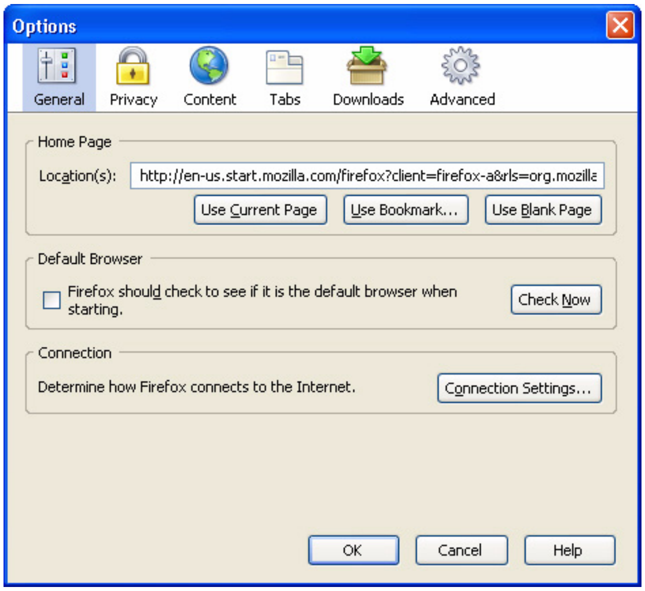
Reset custom settings

Reset to: Low

Configuring Mozilla Firefox 1.0.7 and Higher

In Mozilla Firefox, make sure that JavaScript is enabled. To do this, perform the following steps:

1. From within your Mozilla Firefox browser, select the “Tools” menu and then choose the “Options...” menu item.



Home Page

Location(s): http://en-us.start.mozilla.com/firefox?client=firefox-a&rls=org.mozilla

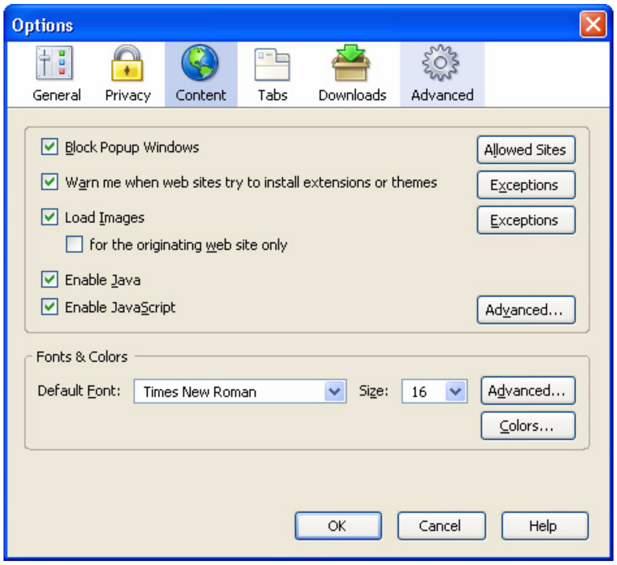
Default Browser

□ Firefox should check to see if it is the default browser when starting.

Connection

Determine how Firefox connects to the Internet.

2. Select the “Content” icon.



☑ Block Popup Windows

☑ Warn me when web sites try to install extensions or themes

☑ Load Images

□ for the originating web site only

☑ Enable Java

☑ Enable JavaScript

Fonts & Colors

Default Font: Times New Roman Size: 16

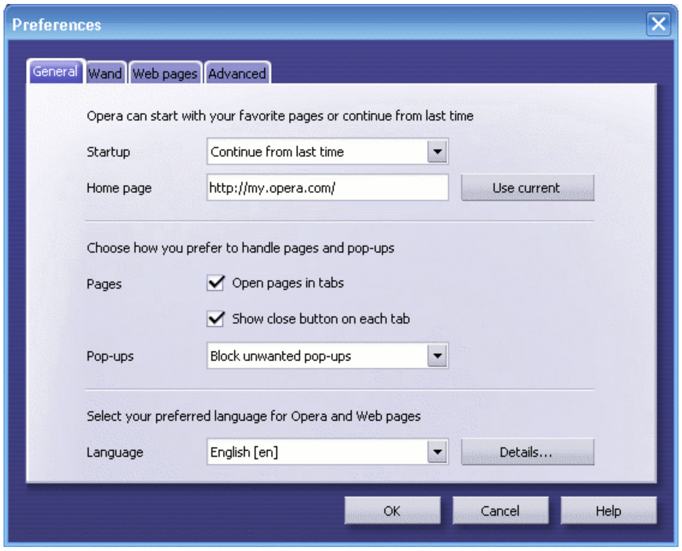
3. Verify that the “Enable JavaScript” checkbox is checked. If it is not checked, then click the checkbox to check it.

4. Click the “OK” button to exit the dialog.

Configuring Opera 8.5 and Higher

In Opera, make sure that JavaScript is enabled. To do this, perform the following steps:

1. From within your Opera web browser, select the “Tools” menu and then select the “Preferences…” menu item.



Opera can start with your favorite pages or continue from last time

Startup: Continue from last time

Home page: http://my.opera.com/

Choose how you prefer to handle pages and pop-ups

Pages: ☑ Open pages in tabs

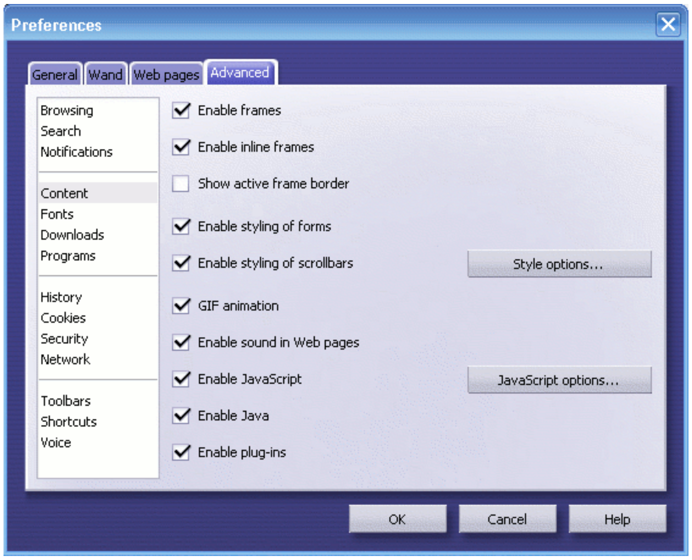
☑ Show close button on each tab

Pop-ups: Block unwanted pop-ups

Select your preferred language for Opera and Web pages

Language: English [en]

2. Select the “Advanced” tab.



☑ Enable frames

☑ Enable inline frames

☐ Show active frame border

☑ Enable styling of forms

☑ Enable styling of scrollbars

☑ GIF animation

☑ Enable sound in Web pages

☑ Enable JavaScript

☑ Enable Java

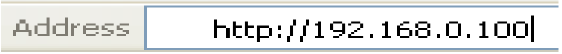
☑ Enable plug-ins

3. Verify that the “Enable JavaScript” checkbox is checked. If it is not checked, then click the checkbox to check it.
4. Click “OK” to exit this dialog.

Connecting Browser To An eIDC

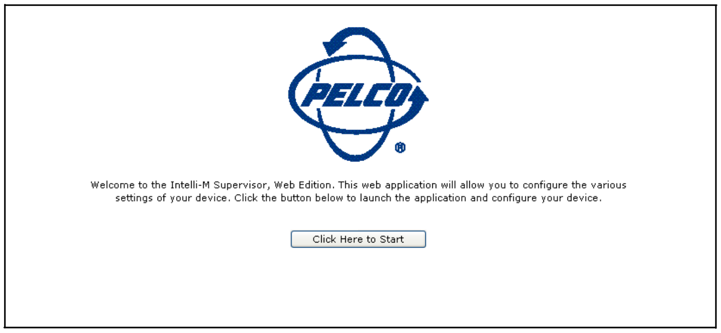
Each eIDC has a built-in web server which allows you to have electronic access control to a single door. To connect your web browser to the eIDC, perform the following steps:

1. Launch the web browser.
2. In the address field of the web browser, type in the IP address of the eIDC. After the IP address has been typed, hit the <Enter> key on the keyboard to go to that address. An example of the IP address of an eIDC being used in the browser Internet Explorer is as follows:



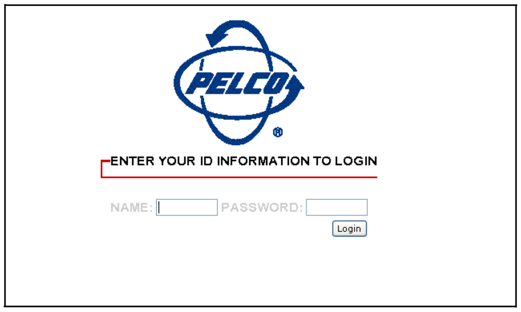
http://192.168.0.100

3. The Intelli-M web interface screen should appear as shown below. Click the "Click Here to Start" button.



Welcome to the Intelli-M Supervisor, Web Edition. This web application will allow you to configure the various settings of your device. Click the button below to launch the application and configure your device.

The login screen should appear after the "Click Here To Start" button is clicked.

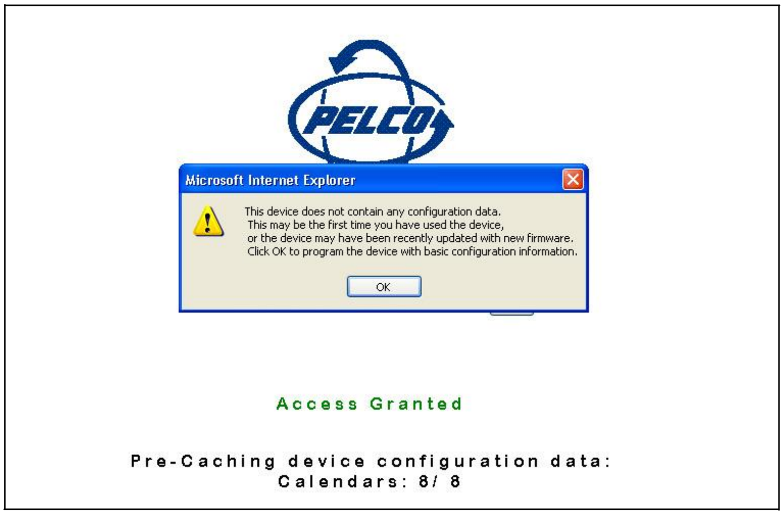


4. Enter the default login Name (admin) and Password (admin), and press <**Enter**> on your keyboard.

   Important: The default administrative password permits access to all areas of the Intelli-M Web Interface. After you log in the first time, you should change the default login Name and Password.

Loading The eIDC Default Configuration

When the default Name and Password have been entered for the very first time, a dialog box will be displayed stating that the controller contains no configuration data and requesting permission to program the eIDC with a default configuration. The default configuration will save you time configuring the eIDC because it will program the eIDC with the basic data needed for any such controller.



This device does not contain any configuration data.
This may be the first time you have used the device,
or the device may have been recently updated with new firmware.
Click OK to program the device with basic configuration information.

Access Granted

Pre-Caching device configuration data:
Calendars: 8/ 8

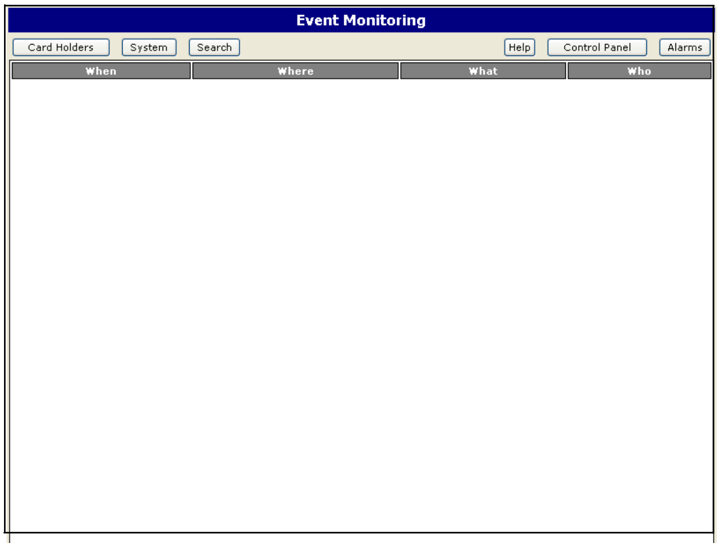
Clicking the “**OK**” button will download default configuration data to the eIDC. It is highly recommended that you click “OK” and allow the basic programming/configuration of the eIDC controller in this manner.

Changing The Administrative Name and Password

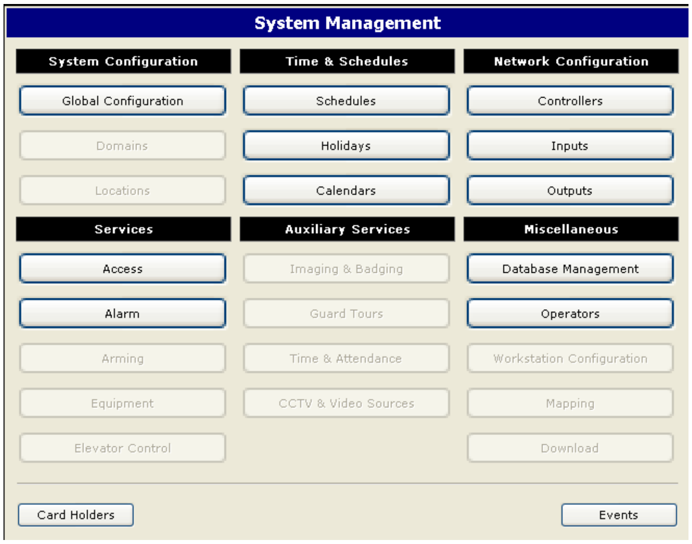
Before fully using the Intelli-M Web Interface, you should change the Administrative Name and Password to maintain system integrity. If the default name and password are not changed, security of the system could be compromised.

To change the Administrative Name and Password, complete the following steps:

1. From the “**Event Monitoring**” screen, click on the “**System**” button.

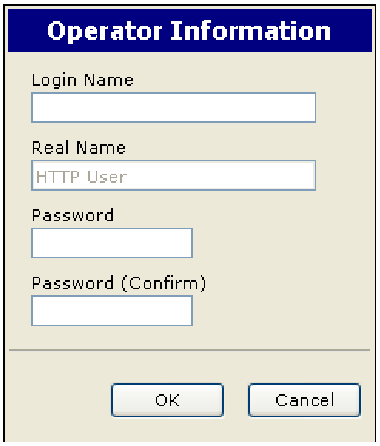


2. Click on the “**Operators**” button on the “**System Management**” screen.



3. Double-click to highlight the line of the type of “Real Name” user you are (either FTP or HTTP), and then click the “**Modify**” button.

   After the “Modify” button is clicked, an “**Operator Information**” screen similar to the one shown below will be displayed.



Operator Information

Login Name

Real Name

HTTP User

Password

Password (Confirm)

4. Enter a new Login Name. The Login Name is limited to 20 characters and is case-sensitive.

5. Enter a new, personalized password. The password field is limited to 16 characters and is case-sensitive.

6. Re-enter the new password in the “**Password (Confirm)**” field. This allows the system to verify the password was entered correctly in order to avoid any mistakes that may be made while changing the new password.

7. When all fields are complete, click “**OK**” to apply the changes. The default “Admin” login name and password are no longer valid.

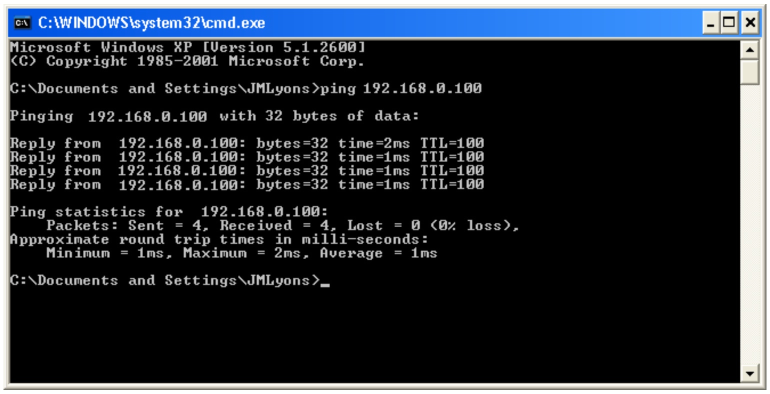
8. Click “**Done**” on the **Operators** screen to return to the **System** screen.

Browser Communication Troubleshooting

If you are unable to establish communication with the eIDC (Ethernet controllers), check the following:

- Verify that the network addressing is correct (IP Address, Subnet mask, Gateway, and Ports) and that all equipment is powered on.
- If you are still unable to connect, you can perform a PING to the device as follows:

    1. Click “**START**” and then **RUN**.
    2. Type **CMD** and click “**OK**.”
    3. In the Command Window, type PING and the IP Address assigned to the controller. Press Enter.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\JMLyons>ping 192.168.0.100

Pinging  192.168.0.100 with 32 bytes of data:

Reply from  192.168.0.100: bytes=32 time=2ms TTL=100
Reply from  192.168.0.100: bytes=32 time=1ms TTL=100
Reply from  192.168.0.100: bytes=32 time=1ms TTL=100
Reply from  192.168.0.100: bytes=32 time=1ms TTL=100

Ping statistics for  192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\JMLyons>_
```

When communication has been established, you can monitor the status of the devices directly from the Intelli-M Web Interface. For direct status monitoring, complete the following steps:

1. On the “**Event Monitoring**” screen, click the “**Control Panel**” button on your keyboard.
2. On the “**Control Panel – Services Status**” screen, click “**Network Sta...**” (i.e., Network Status.
3. On the “**Control Panel – Network Status**” screen, click on the desired tab to monitor the device status.

    --By clicking on the appropriate tab (Controllers, Inputs or Outputs), you can view the status of the respective item.

    --From the “**Controller**” tab, you can check the firmware version.

4. After viewing the selected device, click “**Events**” to return to the “**Event Monitoring**”screen.

For more information on event status monitoring, see “Chapter 8: Monitoring The System.”

You are now ready to configure your system for a card reader (via Global Configuration), and then setup time and schedules (via Schedules, Holidays, Calendars).

Chapter 3: Global Configuration For Card Reader

Contents

This Chapter provides instructions on using the Wiegand Format Editor found within the Global Configuration section of the Intelli-M® Web Interface. Wiegand is a trade name for a technology used in cards, card readers, and sensors that allows data to be placed on a card that can be read or "sensed." The Wiegand Format Editor within the Intelli-M Web Interface provides a platform where you can modify Wiegand style cards to your site specifications.

The following topics can be found within this Chapter:

Overview

The Intelli-M® Supervisor Plus software provides the ability to create custom Wiegand card formats. Cards can be created with a diverse range of format flexibility that include:

- Formats up to 64 bits
- Customized facility (site) and card code sizes
- Even and Odd parity masking

However, there are significant hardware differences between IDC controllers and eIDC controllers in regards to acceptable card formats within Intelli-M. Table 3-1 provides a summary of these differences.

Table 3-1

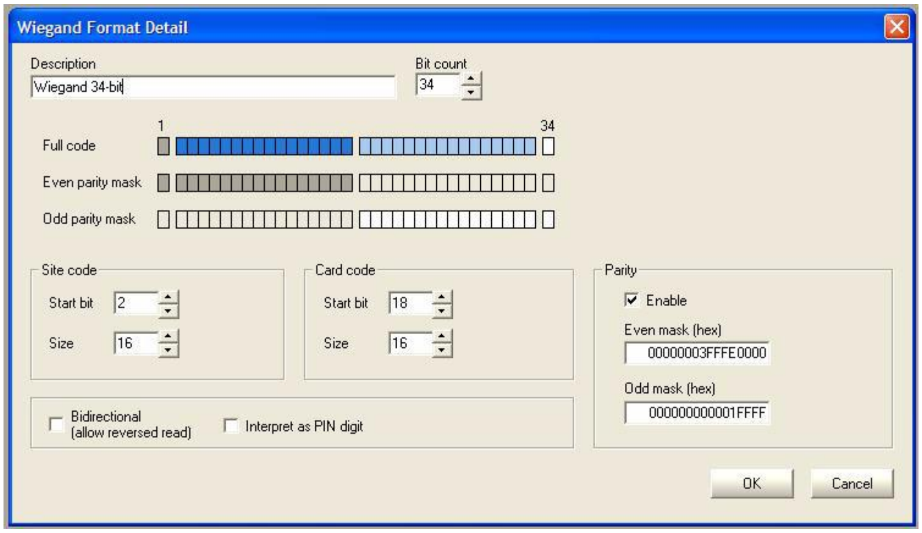
	IDC	eIDC
Maximum Bit Length	40 bits	64 bits
Maximum Custom Site Code	16 bits (65535)	32 bits (4294967295)
Maximum Custom Card Code	16 bits (65535)	32 bits (4294967295)

Intelli-M currently allows for a total of eight unique bit-length formats to simultaneously function within the Supervisor Plus software. The eight formats are as follows:

- Infinity 37
- Wiegand 34-bit
- Wiegand 26-bit
- ProxPro Keypad 4-bit Key
- 8-bit Burst Key
- 27-bit (indala)
- 29-bit (indala)
- 35-bit Corp 1k

Important: Infinity 37 is a proprietary format that cannot be shown, edited, or deleted at this time.

The above listed default formats within Supervisor Plus that can be edited (or deleted) are shown below. Unless specified otherwise, the formats shown below can be used with both IDC and eIDC controllers.



Wiegand Format Detail

Description: Wiegand 34-bit

Bit count: 34

Full code, Even parity mask, Odd parity mask: bits 1 to 34

Site code: Start bit 2, Size 16

Card code: Start bit 18, Size 16

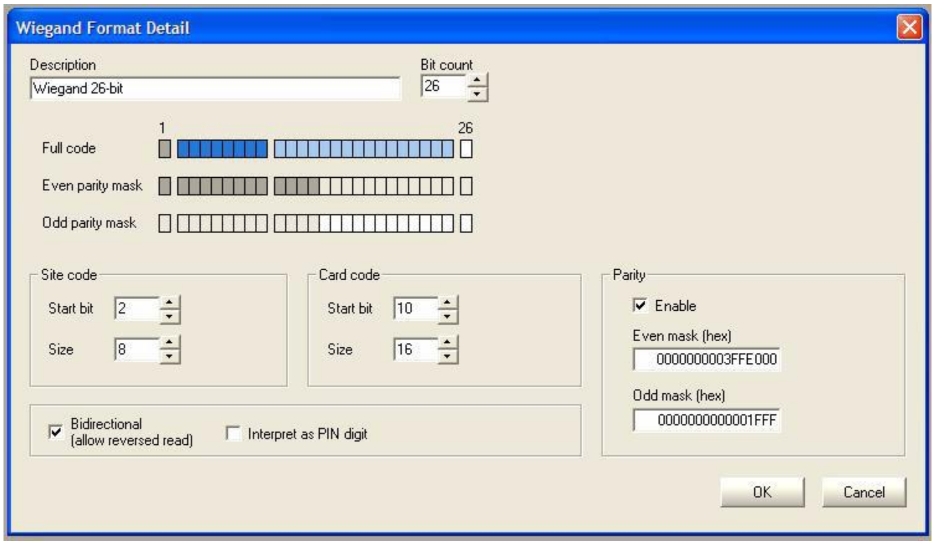
Parity: ☑ Enable

Even mask (hex): 00000003FFFE0000

Odd mask (hex): 000000000001FFFF

☐ Bidirectional (allow reversed read)

☐ Interpret as PIN digit



Wiegand Format Detail

Description: Wiegand 26-bit

Bit count: 26

Full code, Even parity mask, Odd parity mask: bits 1 to 26

Site code: Start bit 2, Size 8

Card code: Start bit 10, Size 16

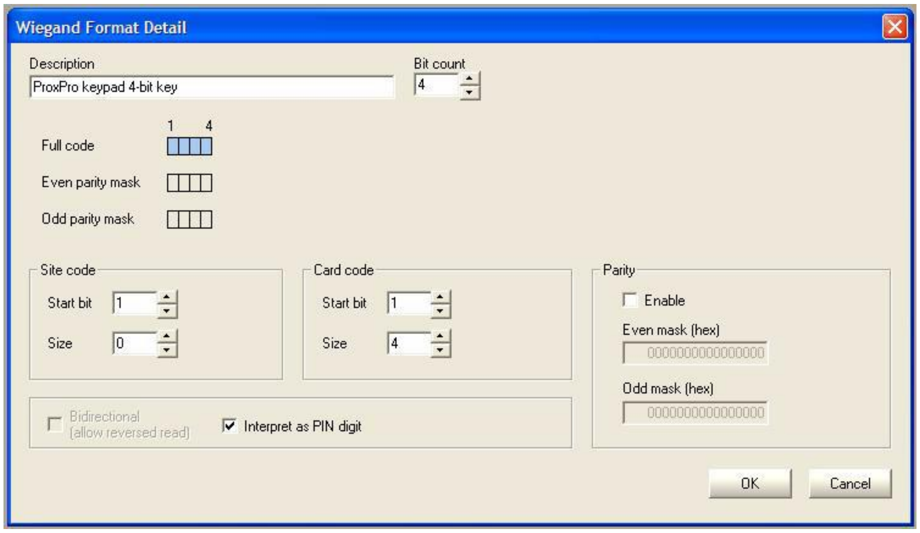
Parity: ☑ Enable

Even mask (hex): 0000000003FFE000

Odd mask (hex): 0000000000001FFF

☑ Bidirectional (allow reversed read)

☐ Interpret as PIN digit



Wiegand Format Detail

Description: ProxPro keypad 4-bit key

Bit count: 4

Full code, Even parity mask, Odd parity mask: bits 1 to 4

Site code: Start bit 1, Size 0

Card code: Start bit 1, Size 4

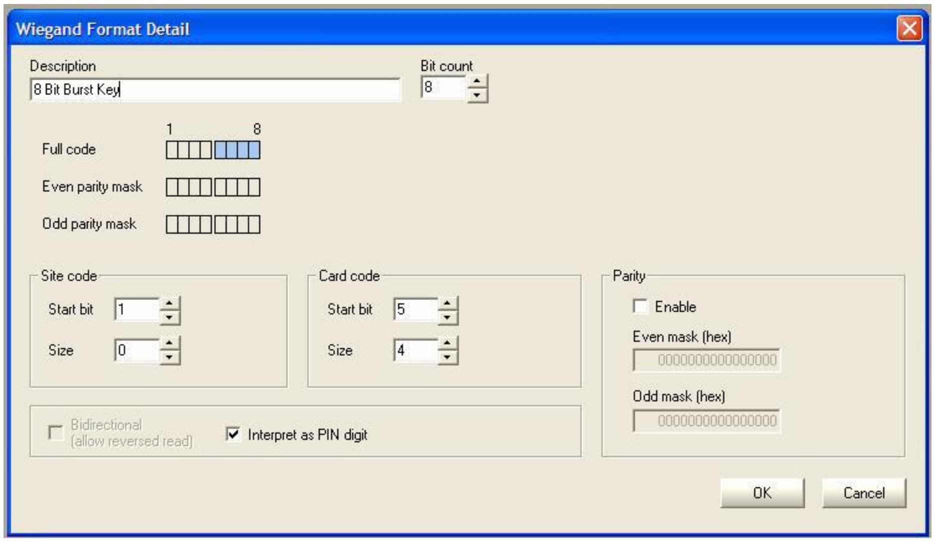
Parity: ☐ Enable

Even mask (hex): 0000000000000000

Odd mask (hex): 0000000000000000

☐ Bidirectional (allow reversed read)

☑ Interpret as PIN digit



Wiegand Format Detail

Description: 8 Bit Burst Key

Bit count: 8

Full code 1 – 8

Even parity mask

Odd parity mask

Site code

Start bit: 1

Size: 0

Card code

Start bit: 5

Size: 4

Parity

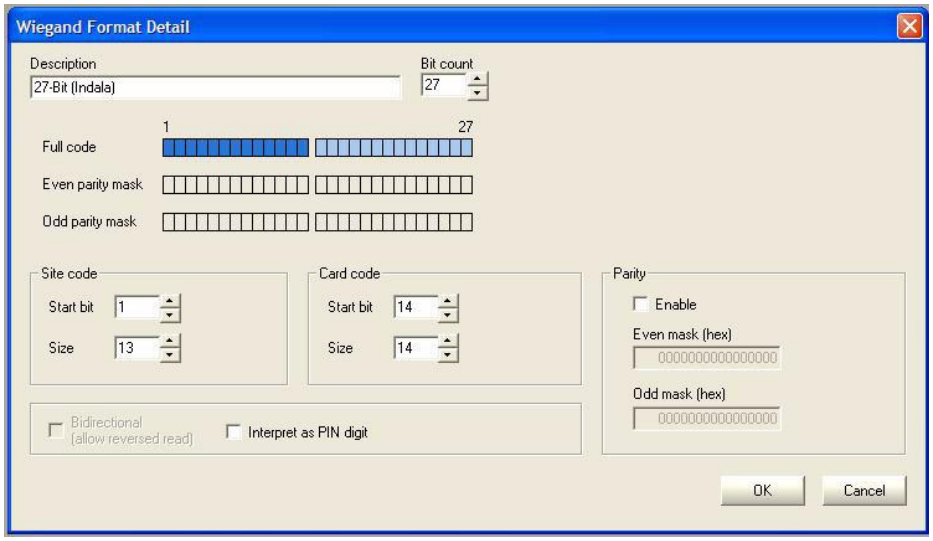
□ Enable

Even mask (hex): 0000000000000000

Odd mask (hex): 0000000000000000

□ Bidirectional (allow reversed read)

☑ Interpret as PIN digit



Wiegand Format Detail

Description: 27-Bit (Indala)

Bit count: 27

Full code 1 – 27

Even parity mask

Odd parity mask

Site code

Start bit: 1

Size: 13

Card code

Start bit: 14

Size: 14

Parity

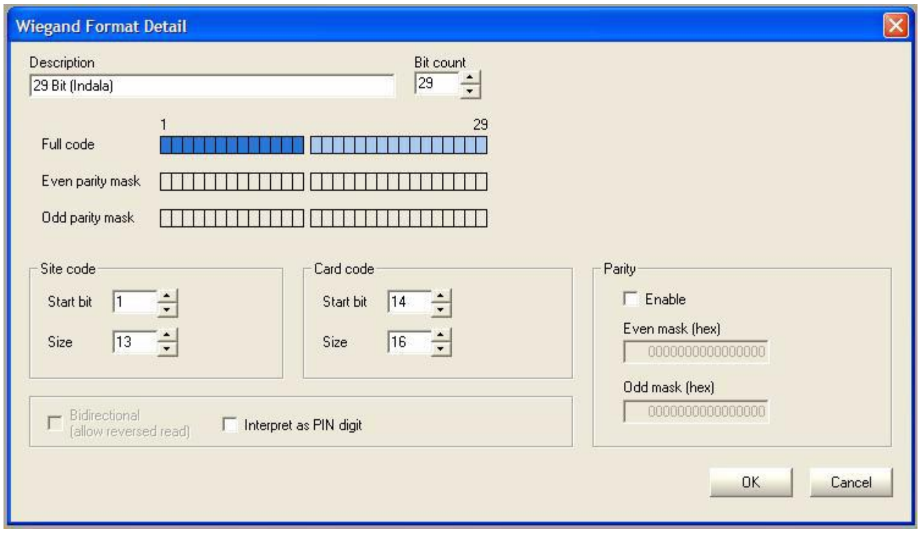
□ Enable

Even mask (hex): 0000000000000000

Odd mask (hex): 0000000000000000

□ Bidirectional (allow reversed read)

□ Interpret as PIN digit



Wiegand Format Detail

Description: 29 Bit (Indala)

Bit count: 29

Full code 1 – 29

Even parity mask

Odd parity mask

Site code

Start bit: 1

Size: 13

Card code

Start bit: 14

Size: 16

Parity

□ Enable

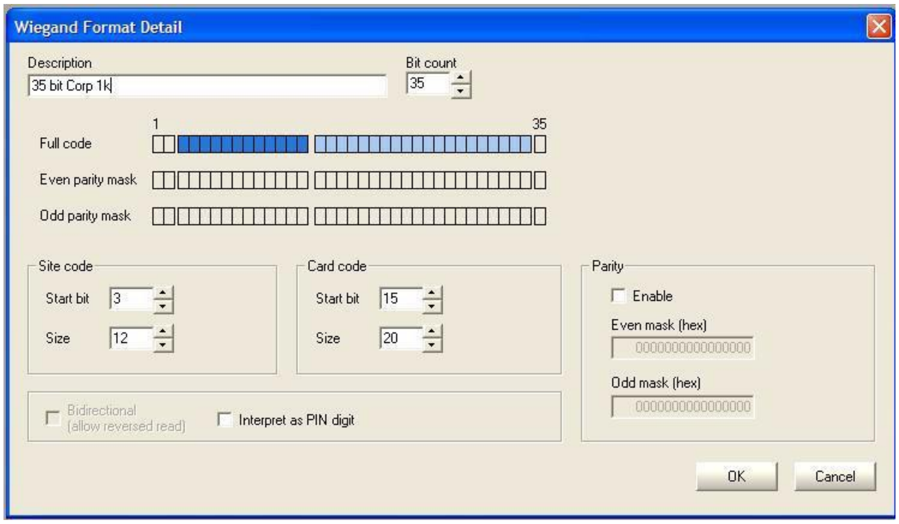
Even mask (hex): 0000000000000000

Odd mask (hex): 0000000000000000

□ Bidirectional (allow reversed read)

□ Interpret as PIN digit

Standard 35-bit Corporate 1K (for eIDC Only)



Wiegand Format Detail

Description: 35 bit Corp 1k

Bit count: 35

Full code / Even parity mask / Odd parity mask (bits 1 to 35)

Site code — Start bit: 3, Size: 12

Card code — Start bit: 15, Size: 20

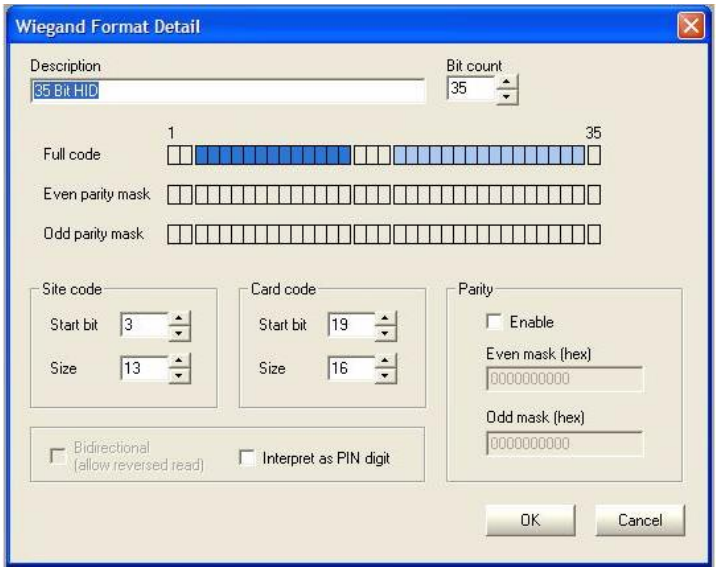
Parity — □ Enable; Even mask (hex): 0000000000000000; Odd mask (hex): 0000000000000000

□ Bidirectional (allow reversed read)

□ Interpret as PIN digit

The standard 35-bit Corporate 1k card format (shown above) that is listed as a default format within Supervisor Plus can be customized to work with an IDC controller. Customizing that will allow the format to work (with limitations) for both eIDC and IDC controllers within Supervisor Plus is as follows:

Non-standard 35-bit Corporate 1K (for IDC and possibly eIDC)



Wiegand Format Detail

Description: 35 Bit HID

Bit count: 35

Full code / Even parity mask / Odd parity mask (bits 1 to 35)

Site code — Start bit: 3, Size: 13

Card code — Start bit: 19, Size: 16

Parity — □ Enable; Even mask (hex): 0000000000; Odd mask (hex): 0000000000

□ Bidirectional (allow reversed read)

□ Interpret as PIN digit

With the non-standard 35-bit Corporate 1K format for IDC and eIDC controllers, the card site code is limited to between 0 to 8191. The card number is limited to between 0 to 65535. This is fine for an IDC controller, since the IDC is limited to card numbers no greater than 65535. (Refer to Table 3-1 above.) This format becomes a problem though for cards used on an eIDC or IDC controller with a card number greater than 65535. *Currently, cards in this format with a card number greater than 65535 are not read properly by the eIDC or IDC; that is, the card number printed on the card will not match what is read by either controller within Supervisor Plus.*

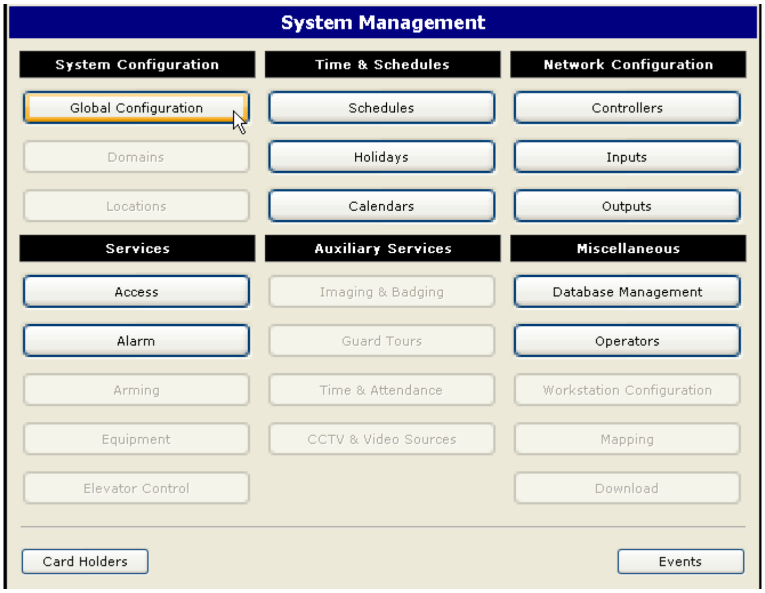
Important: Consider using the non-standard 35-bit Corporate 1K format only with IDC controllers.

Instructions for creating custom Wiegand formats are provided in the section below.

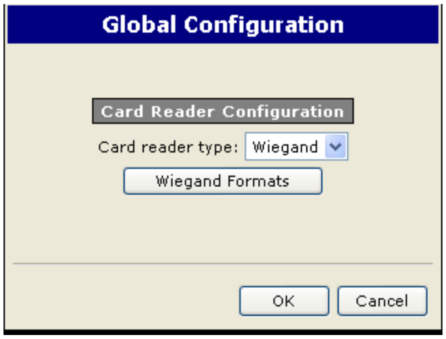
Creating A Custom Wiegand Format

Perform the following steps to custom create an access card with Wiegand formatting:

1. Select “Global Configuration” from the Intelli-M Web Interface “System Management” screen.

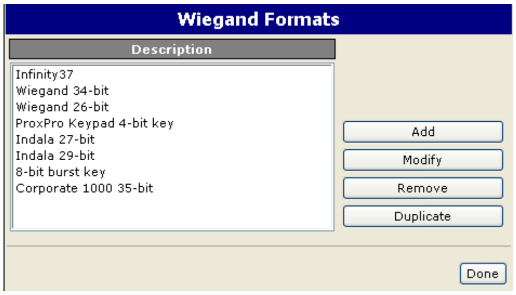


When the **Global Configuration** button is pressed, the following screen will be displayed:



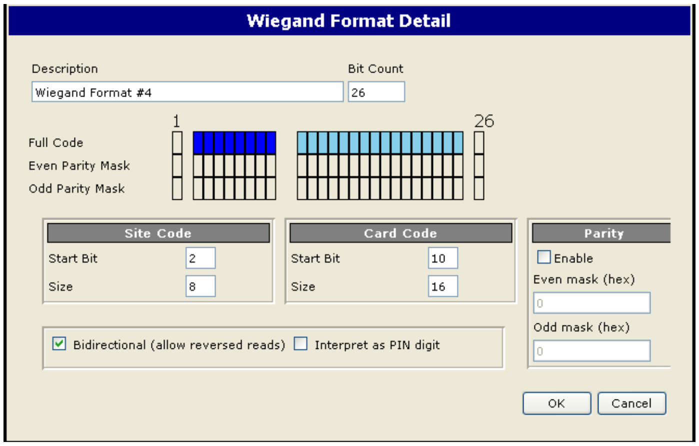
Card reader type: Wiegand

2. Wiegand is the only card reader type that can be used with the Intelli-M Web Interface. Click the “Wiegand Formats...” button.



Infinity37
Wiegand 34-bit
Wiegand 26-bit
ProxPro Keypad 4-bit key
Indala 27-bit
Indala 29-bit
8-bit burst key
Corporate 1000 35-bit

3. Click on the “ADD” button.



Wiegand Format Detail

Description: Wiegand Format #4

Bit Count: 26

Site Code

Start Bit: 2

Size: 8

Card Code

Start Bit: 10

Size: 16

Parity

☐ Enable

Even mask (hex): 0

Odd mask (hex): 0

☑ Bidirectional (allow reversed reads) ☐ Interpret as PIN digit

4. Enter a description name for the new format, and then set the "Bit Count" (bit size) for the new format. The bits are in numerical order from left to right, always starting with "1" as shown by the "Full Code" section.

    -- The "Site Code" is represented as dark blue boxes. The "Start Bit" is the bit number from which the site code will start. "Size" within the "Site Code" area is the total number of bits designated to the site code.

    Note: Zero (0) is allowed as a site code. A site code of 0 will cause the eIDC to ignore the site code and only compare the card codes.

    -- The "Card Code" is represented as light blue boxes. "Start Bit" within the "Card Code" area must be assigned. The total number of bits allotted to "Size" for "Card Code" must also be assigned.

    -- If "Parity" masking is to be utilized, then some conversion is required from binary to hexadecimal. The default 26-bit "Even mask (hex)" is 3FFE000 which when converted to binary is thirteen ones followed by thirteen zeros. The "Odd Mask (hex)" is thirteen ones.

    Note: Parity masking is an option. When trying to conform to a particular manufacturer's standard, that manufacturer may need to be consulted for accurate formatting information.

    -- "Bidirectional" is available for certain types of supported readers. The "Wiegand Swipe" and "Wiegand Insertion" are two styles of readers that would use this feature.

    -- "Interpret as PIN digit" is available for keypad formats associated as Pin digits. The HID Prox Pro K combination Prox / Keypad reader is an example of a keypad format that is associated as Pin digits.

5. Set up the "Wiegand Format Detail" screen to fit your need. When finished click "OK" to save the format.
6. Click "Done" to leave the Wiegand Formats menu.
7. Click "Done" in the Global Configuration menu.
8. Present a finished card to a reader to make sure that it works. This will verify the format on the card.

Chapter 4: Schedules, Holidays, Calendars

Contents

This Chapter provides instructions on how to set up time and schedules within the Intelli-M® Web Interface. Times and Schedules are set up from within the System Management screen of the Intelli-M Web Interface.

The following topics can be found within this Chapter:

- Schedules
- Holidays
- Calendars

Schedules

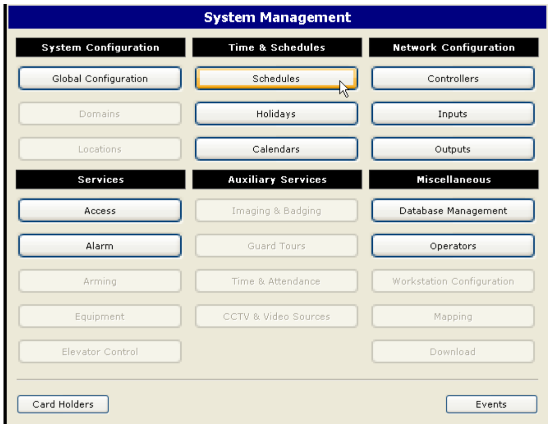
A schedule is a determined number of hours and days. Each schedule is assigned a name by the operator. The schedules are used to tell the system when certain actions are allowed in the system, such as when a door is to be locked or when employees can gain access to an area by presenting their credentials (such as a card or key tag).

Two system schedules are included in the Intelli-M Web Interface: **Never**, which denies access all day, every day; and **Always**, which grants access all day, every day. Following are examples of typical schedules in an access control system:

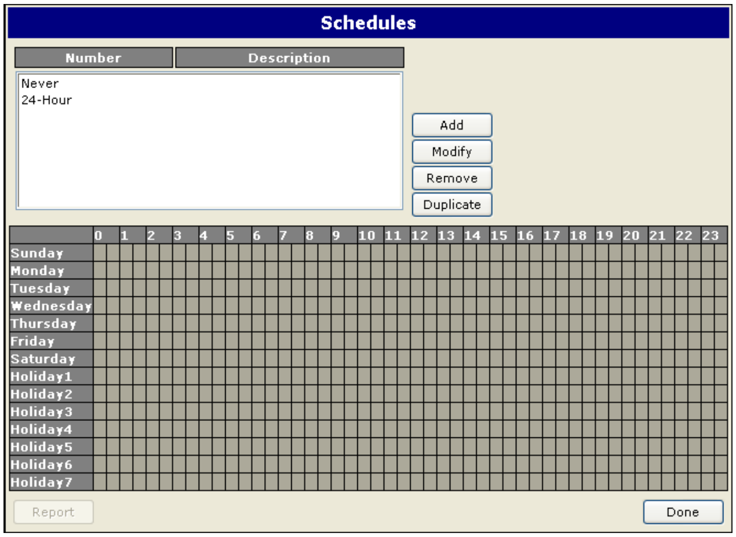
- **Employee --** allows access from 8:00 through 17:00 (24-hour clock), Monday through Friday.
- **Janitorial --** allows access from 17:00 through 23:00, Monday through Friday, to accommodate cleaning crews.

To define a schedule, complete the following steps:

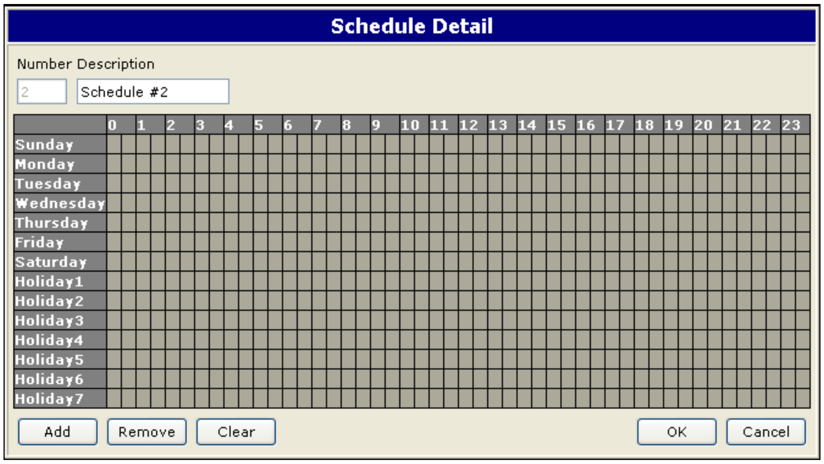
1. Click “**Schedules**” on the **System Configuration** screen.



When the “**Schedules**” button is pressed, the following screen will be displayed:



2. Click “**Add**” on the **Schedules** screen. The **Schedules Detail** screen will be displayed.



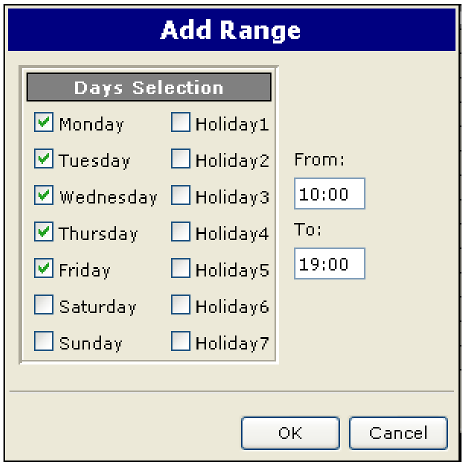
Schedule Detail

Number Description

2 | Schedule #2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Monday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Tuesday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Wednesday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Thursday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Friday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Saturday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday2	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday3	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday4	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday5	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday6	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Holiday7	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

3. Enter a name for the new schedule in the **Description** field.
4. Click “**Add**” and enter start and end times. Select the days and holidays to which these times apply.



Add Range

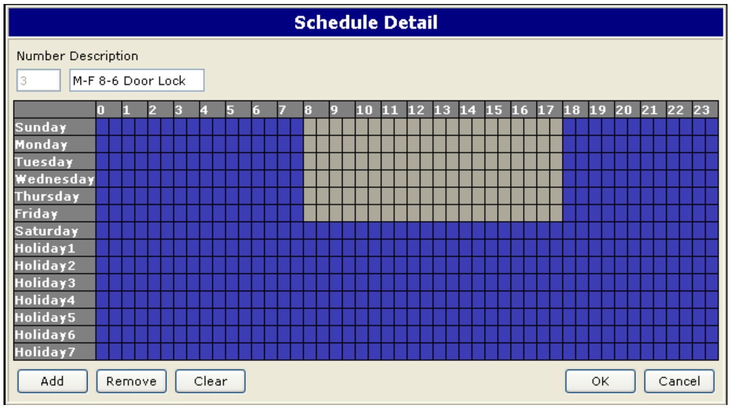
Days Selection

☑ Monday	□ Holiday1
☑ Tuesday	□ Holiday2
☑ Wednesday	□ Holiday3
☑ Thursday	□ Holiday4
☑ Friday	□ Holiday5
□ Saturday	□ Holiday6
□ Sunday	□ Holiday7

From: 10:00

To: 19:00

When applying schedules to doors, the door is locked at times colored blue and unlocked at times colored grey.



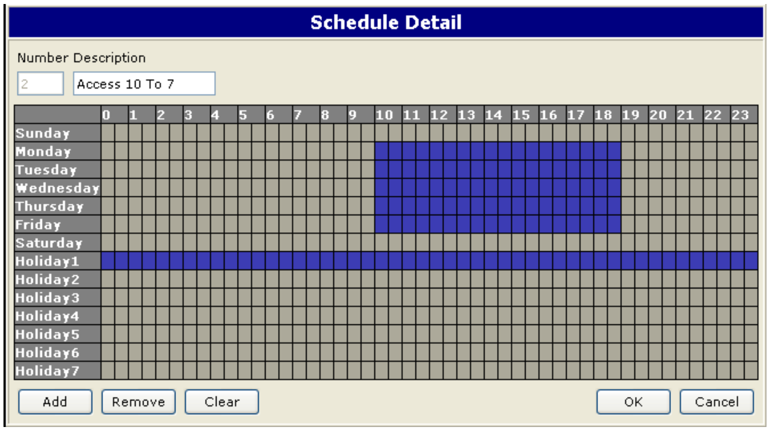
Schedule Detail

Number Description

3 | M-F 8-6 Door Lock

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Monday	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Tuesday	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Wednesday	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Thursday	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Friday	■	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Saturday	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday1	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday2	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday3	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday4	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday5	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday6	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Holiday7	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

When applying schedules to card holders, access is allowed at times colored blue and access is denied at times colored grey.



Number Description

2 Access 10 To 7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday																								
Monday											🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦					
Tuesday											🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦					
Wednesday											🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦					
Thursday											🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦					
Friday											🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦					
Saturday																								
Holiday1	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Holiday2																								
Holiday3																								
Holiday4																								
Holiday5																								
Holiday6																								
Holiday7																								

Times can be divided, such as activating a lock between 0:00 and 7:00, unlocking the door from 7:00 through 17:00, and then locking the door again until 24:00.

Times can also be added or modified by selecting a block on the schedule and clicking "**Add**" or "**Remove**."

To eliminate all information on the schedule, click "**Clear**."

When finished, click "**OK**" to return to **Schedules**.

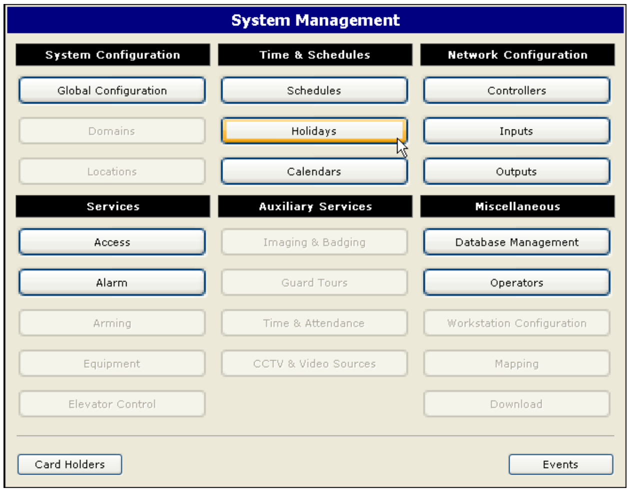
Continue creating new schedules by repeating these steps. When finished, click "**Done**" to return to the **System Management** screen

Holidays

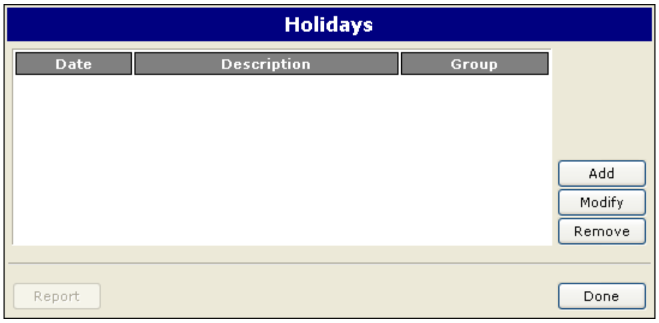
Holidays allow you to treat certain days differently than other days of the week. Holidays are assigned to up to seven groups; holidays that are grouped together allow you to select the entire group of holidays for access purposes. For more information on associating a holiday with a schedule, see the previous section.

To define a holiday, complete the following steps:

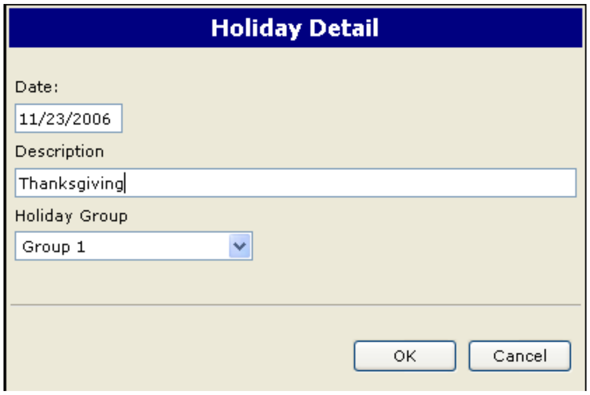
1. Click "**Holidays**" on the **System Configuration** screen.



When the "**Holidays**" button is pressed, the following screen will be displayed:



2. To add a new holiday, click "**Add**." To edit an existing holiday, click on the holiday in the list and then click "**Modify**."
3. Enter the **Date** you want to designate as a holiday.
4. Enter a **Description** for this holiday.



Date: 11/23/2006

Description: Thanksgiving

Holiday Group: Group 1

5. Select a **Holiday Group** from the drop-down menu. A maximum of seven holiday groups can be programmed in the system.
6. Click "**OK**" to return to the **Holidays** screen.

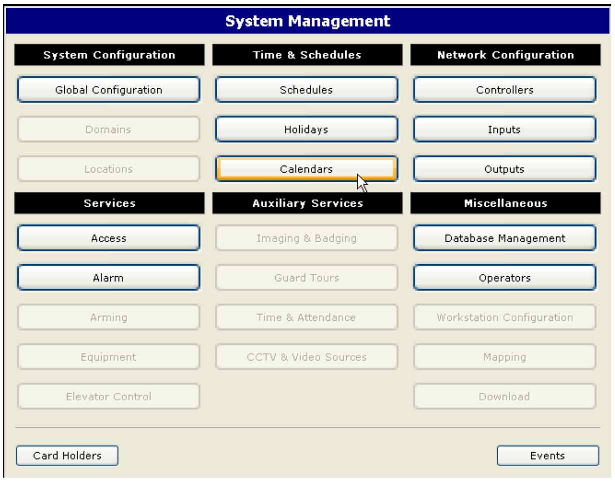
To continue adding new holidays, repeat steps 2 through 6. When finished, click "**Done**."

Calendars

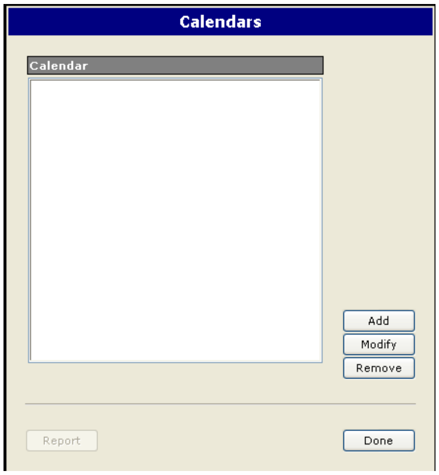
Yearly calendars allow you to assign a different schedule to each week of the year. Each weekly schedule change is automatically downloaded, by default, at the beginning of each week. The calendar schedule can only be assigned to card holders by way of their privilege group.

To create a calendar schedule, complete the following steps:

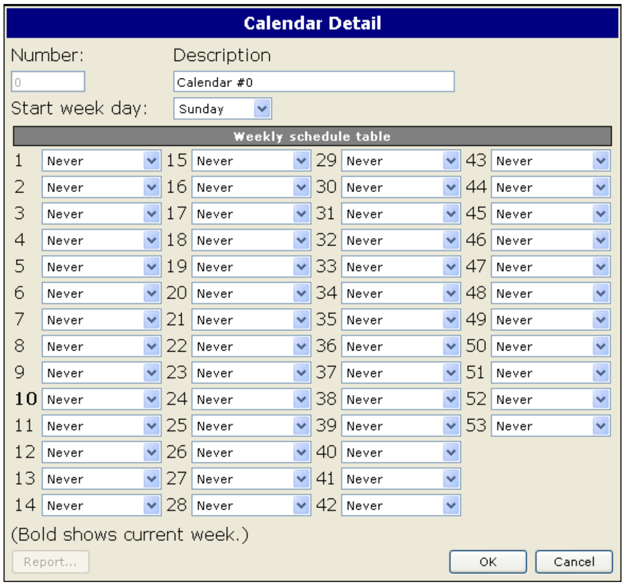
1. Click "**Calendars**" on the **System Configuration** screen.



When the "**Calendars**" button is pressed, the following screen will be displayed:



2. To add a new calendar schedule, click "**Add.**" To edit an existing calendar schedule, click to highlight the calendar schedule in the list and then click "**Modify**."



Calendar Detail

Number: 0

Description: Calendar #0

Start week day: Sunday

Weekly schedule table

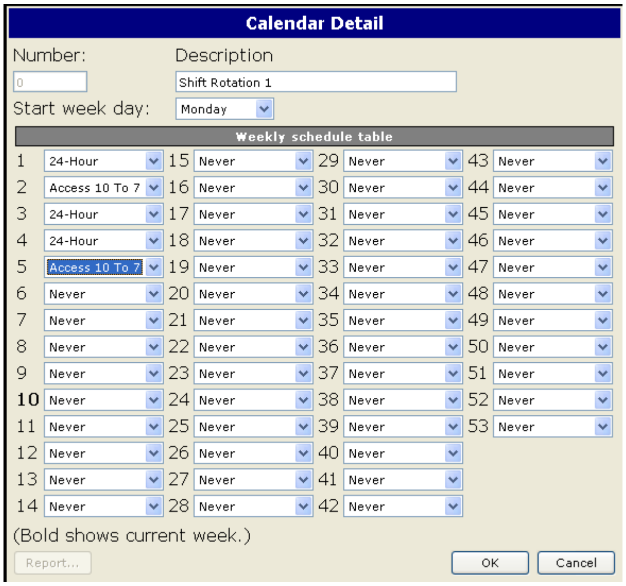
1	Never	15	Never	29	Never	43	Never
2	Never	16	Never	30	Never	44	Never
3	Never	17	Never	31	Never	45	Never
4	Never	18	Never	32	Never	46	Never
5	Never	19	Never	33	Never	47	Never
6	Never	20	Never	34	Never	48	Never
7	Never	21	Never	35	Never	49	Never
8	Never	22	Never	36	Never	50	Never
9	Never	23	Never	37	Never	51	Never
10	Never	24	Never	38	Never	52	Never
11	Never	25	Never	39	Never	53	Never
12	Never	26	Never	40	Never		
13	Never	27	Never	41	Never		
14	Never	28	Never	42	Never		

(Bold shows current week.)

3. Enter the **Description** for this calendar schedule

4. From the **Start Week Day** drop-down, select the day of the week that the schedules will be downloaded to the controllers. This occurs at midnight of the day selected each week.

5. For each week of the year (1-53), a drop-down is available and the current week is highlighted with bold text. Click the drop-down for a specific week, select a schedule, and click "**Select**." When finished, click "**OK**." If a new schedule is required, you must create it from the **Schedules** menu.



Calendar Detail

Number: 0

Description: Shift Rotation 1

Start week day: Monday

Weekly schedule table

1	24-Hour	15	Never	29	Never	43	Never
2	Access 10 To 7	16	Never	30	Never	44	Never
3	24-Hour	17	Never	31	Never	45	Never
4	24-Hour	18	Never	32	Never	46	Never
5	Access 10 To 7	19	Never	33	Never	47	Never
6	Never	20	Never	34	Never	48	Never
7	Never	21	Never	35	Never	49	Never
8	Never	22	Never	36	Never	50	Never
9	Never	23	Never	37	Never	51	Never
10	Never	24	Never	38	Never	52	Never
11	Never	25	Never	39	Never	53	Never
12	Never	26	Never	40	Never		
13	Never	27	Never	41	Never		
14	Never	28	Never	42	Never		

(Bold shows current week.)

The calendar schedule is now given a **Number** that is displayed with all available schedules when configuring **Privilege Groups**.

To add additional calendar schedules, repeat steps 2-5. When finished, click "**Done**."

Chapter 5: Programming Access Control Devices

Contents

This Chapter provides instructions on how to set up the network configuration within the Intelli-M® Web Interface by programming various access control devices. Access control devices for the Intelli-M Web Interface are the eIDC controller, and the input and output devices connected to the eIDC controller. The devices to be set up within the network configuration can be accessed from within the System Management screen of the Intelli-M Web Interface.

The following topics can be found within this Chapter:

Access Control Devices Overview

Access control systems typically control three basic types of devices: inputs, outputs, and readers. Each access control panel and the devices it controls must be defined.

Inputs typically consist of**:**

- Door contacts
- Motion detectors
- Temperature sensors
- Emergency pull stations
- Any other supervisory equipment that can report a status change

Outputs typically include**:**

- Electromagnetic locks
- Door strikes
- Turnstiles
- Motorized barrier gates
- Sounders or alarms
- Any electric equipment that operates to perform a specific function

Readers include**:**

- Proximity card readers (Wiegand, smart, and so on)
- Magnetic stripe readers
- Biometric readers (fingerprint, hand geometry, and so on)
- Any other device that identifies, records, and validates the authorized access level of the user in the system

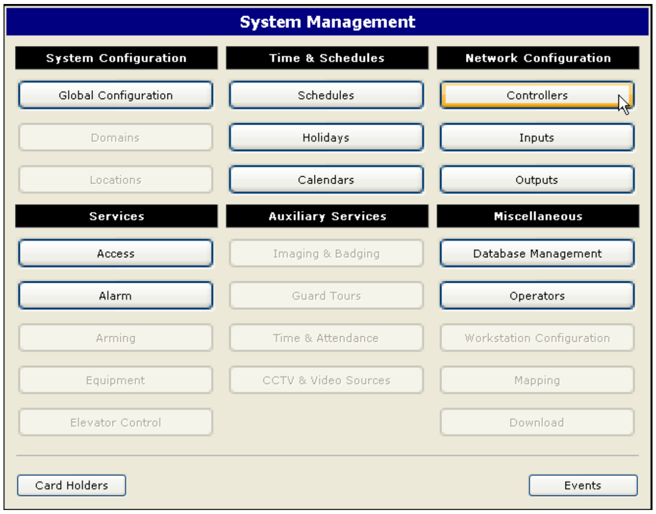
These devices are connected to the controllers through the following input and output ports:

- OC -- Output (2 open collector, shared between OC1 & OC2), provides power for locks
- NC/NO -- Output (1 Form C SPDT), configurable initial status (NO/NC)
- IN -- Input (4), configurable NO/NC with optional EOLR supervision
- CR -- Card Reader (2 located on the IDC controller), CR-IN & CR-OUT

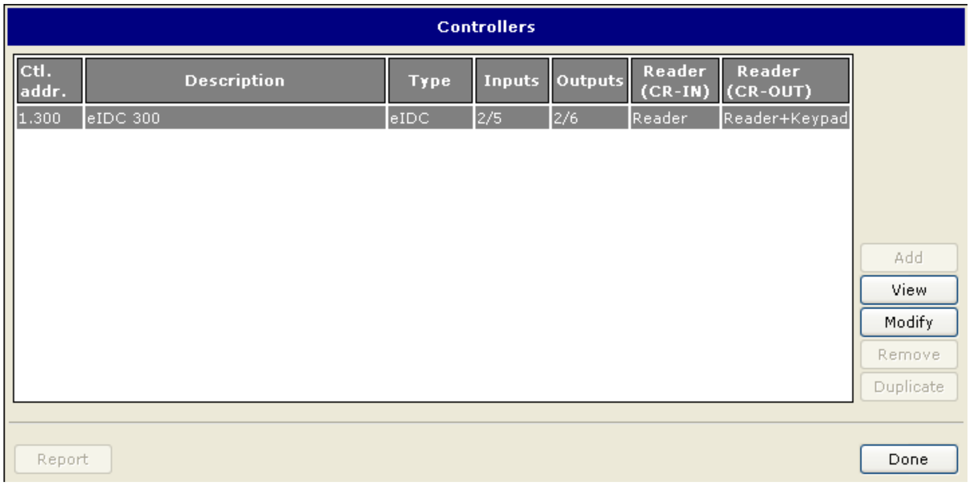
Defining The Controller

To define the eIDC controller for your network, complete the following steps:

1. Click “**Controllers**” on the **System Management** screen.

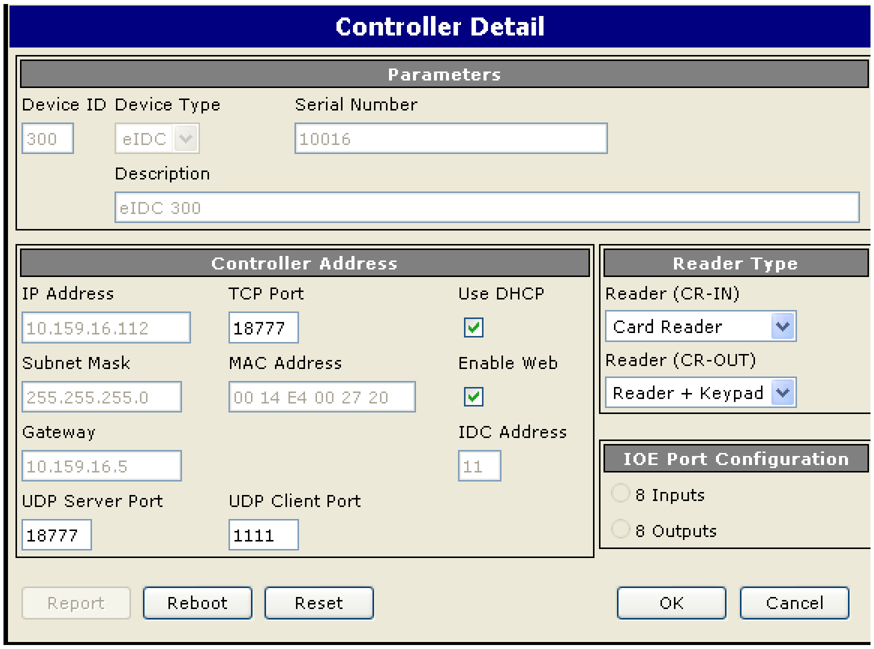


2. Most of the information for the fields are already done if the eIDC was correctly installed, and if the default configuration was loaded as described in Chapter 1. Click to highlight the eIDC information, and then click “**Modify**” to edit the controller.



Ctl. addr.	Description	Type	Inputs	Outputs	Reader (CR-IN)	Reader (CR-OUT)
1.300	eIDC 300	eIDC	2/5	2/6	Reader	Reader+Keypad

When “**Modify**” is clicked, a Controller Detail screen similar to what is shown below will be displayed.



Controller Detail

Parameters

Device ID: 300

Device Type: eIDC

Serial Number: 10016

Description: eIDC 300

Controller Address

IP Address: 10.159.16.112

TCP Port: 18777

Use DHCP: ☑

Subnet Mask: 255.255.255.0

MAC Address: 00 14 E4 00 27 20

Enable Web: ☑

Gateway: 10.159.16.5

IDC Address: 11

UDP Server Port: 18777

UDP Client Port: 1111

Reader Type

Reader (CR-IN): Card Reader

Reader (CR-OUT): Reader + Keypad

IOE Port Configuration

○ 8 Inputs

○ 8 Outputs

- **Reboot --** This button when clicked causes a power cycle to occur at the eIDC.
- **Reset --** This button when clicked causes the eIDC to revert to its factory default settings.

3. The **TCP Port** and **UDP Server Port** are set to 18777 by default in the Web Interface. The UDP Client Port is set to 1111 by default as well. If any of the port defaults cannot be used on the network for your eIDC, then change the port information as appropriate for the network used by your eIDC.

   Note: The selected ports must be opened by the network administrator.

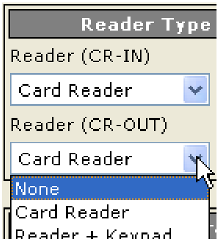
4. To enable DHCP, the **Use DHCP** checkbox should be checked. For static, make sure DHCP is deselected.

   Important: For static, make sure DHCP is deselected, and enter the correct **IP Address**, **Subnet Mask**, and **Gateway**.

5. **Enable Web** must be checked if you want to be able to access the eIDC by way of a web browser. This box should only be unchecked if you have the “Intelli-M Supervisor Plus” software and no longer want web access to the eIDC.

   Caution: Only uncheck the Enable Web feature if you no longer want to be able to access the eIDC by way of the web. Once this feature is disabled, the only way to enable web access again without the “Intelli-M Supervisor Plus” software is to physically reset the eIDC. Information on resetting an eIDC can be found in the “Intelli-M Hardware Installation and Reference” manual. A PDF of this manual can be downloaded from the infinias Web site at: http://www.infinias.com/.

6. Enter the **Reader Types** for both the ***CR-IN*** (in reader), and ***CR-OUT*** (out reader).



Reader Type

Reader (CR-IN)

Card Reader

Reader (CR-OUT)

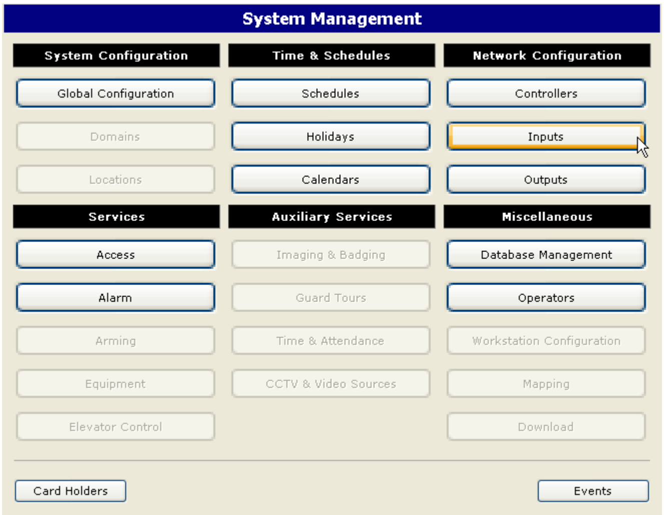
Card Reader

7. Click "**OK**" to save the controller settings or "**Cancel**" to exit without saving. Then click "**Done**" to return to the System Management screen.

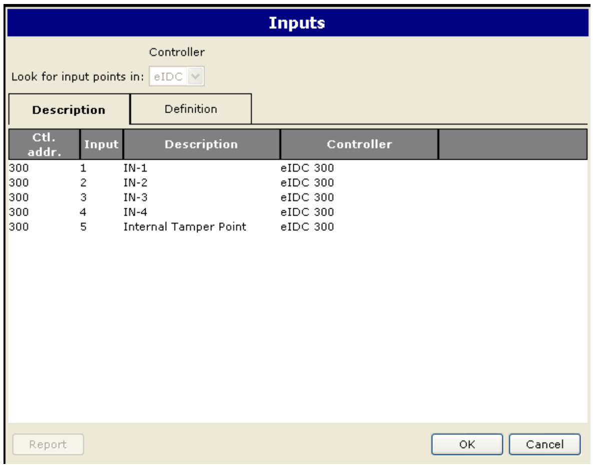
Defining Inputs

To define inputs, complete the following steps:

1. Click "**Inputs**" on the **System Management** screen.



The **Inputs** screen will appear similar to what is shown below:

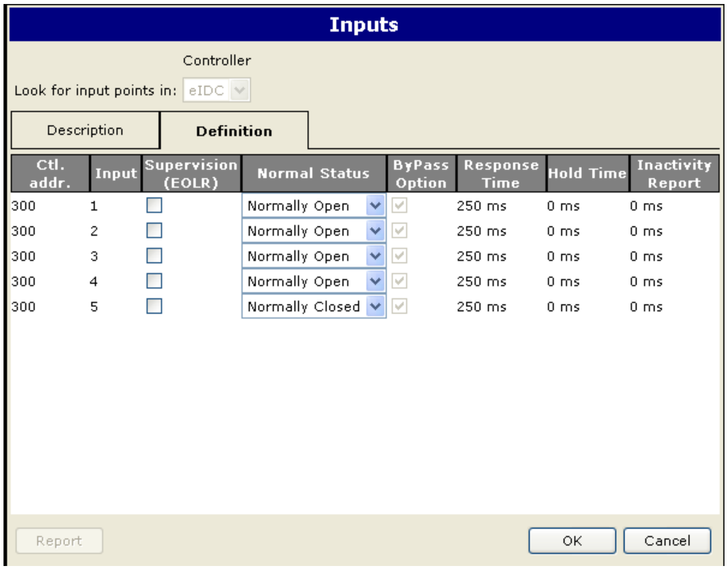


Look for input points in: eIDC

Ctl. addr.	Input	Description	Controller
300	1	IN-1	eIDC 300
300	2	IN-2	eIDC 300
300	3	IN-3	eIDC 300
300	4	IN-4	eIDC 300
300	5	Internal Tamper Point	eIDC 300

The **Inputs** screen first appears with the **Description** tab being the active view. The **Description** tab view provides a description of each input used on the eIDC. The **Description** tab is only for viewing purposes, no edits or changes can be made form this view.

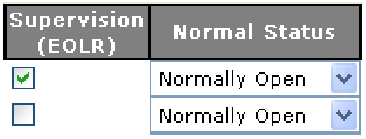
2. Select the **Definition** tab to continue programming the controller.



Look for input points in: eIDC

Ctl. addr.	Input	Supervision (EOLR)	Normal Status	ByPass Option	Response Time	Hold Time	Inactivity Report
300	1	□	Normally Open	☑	250 ms	0 ms	0 ms
300	2	□	Normally Open	☑	250 ms	0 ms	0 ms
300	3	□	Normally Open	☑	250 ms	0 ms	0 ms
300	4	□	Normally Open	☑	250 ms	0 ms	0 ms
300	5	□	Normally Closed	☑	250 ms	0 ms	0 ms

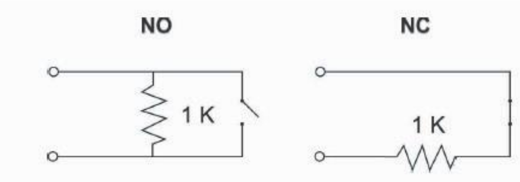
3. For each input, select (i.e., check mark) **Supervision EOLR** (End Of Line Resistance) if a 1K-ohm resistor is connected. Supervision EOLR failures cause input trouble alarm events to be reported.



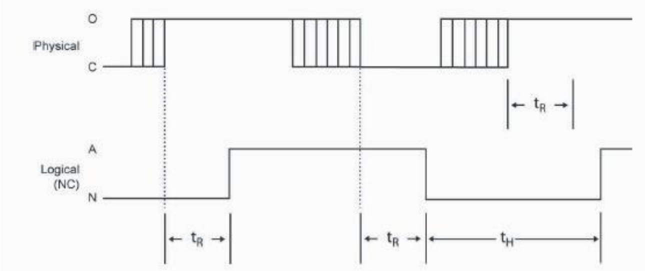
Supervision (EOLR)	Normal Status
☑	Normally Open
□	Normally Open

4. Select the **Normal Status** position from the pull down for each input. The **Normal Status** position can be either **Normally Open** (the input status is considered normal when the cir-

cuit is open) or **Normally Closed** (the input status is considered normal when the circuit is closed). The normal logical state corresponds with no activity. For example, an input triggers an alarm only in the abnormal state. Standard electrical connections of End-Of-Line Resistors are shown as follows:



5. The **Bypass Option** is set by default to allow operators to bypass and un-bypass the input manually on the **Network Status** screen.
6. The **Response Time** is set by default to 250 milliseconds. This is to help prevent false alarms. The response time is the delay during which the incoming signal must remain electrically steadily active (depending on the normal status) before the input is considered active as seen by the system. Any transition shorter than this delay is ignored.
7. The **Hold Time** is set by default to 0 milliseconds. A hold time is the minimal time after being deactivated during which the input will be held logically inactive before becoming active again, even if it is electrically activated. The hold time is subject to the response time.



Physical state either C (closed) or O (open)
Logical state either N (normal) or A (abnormal), normally closed configuration

Note: Response time applies symmetrically (that is, both to rising and falling transitions). Hold time, however, applies only to rising transitions.

8. The **Inactivity Report** is set by default to 0 milliseconds. An inactivity report time is useful in a situation where supervision of movement in a room is necessary, such as in an elderly care facility. If no activity is reported within the inactivity report time, an event is reported in the system.

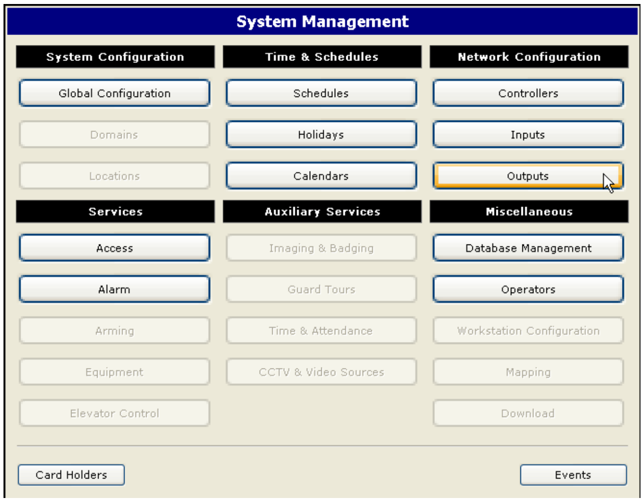
Note: To change the time default setting, click on the timing default to alternate between milliseconds, seconds, and minutes.

9. Click “**OK**” to save the input settings or “**Cancel**” to exit without saving. The System Management screen will be displayed.

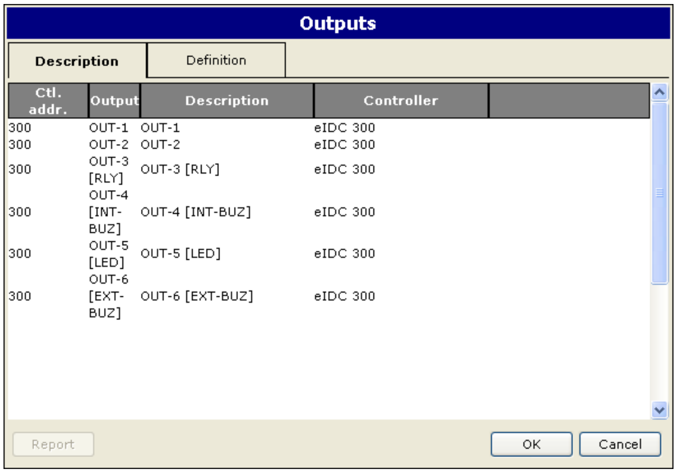
Defining Outputs

To define an output, complete the following steps:

1. Click "**Outputs**" on the **System Management** screen.



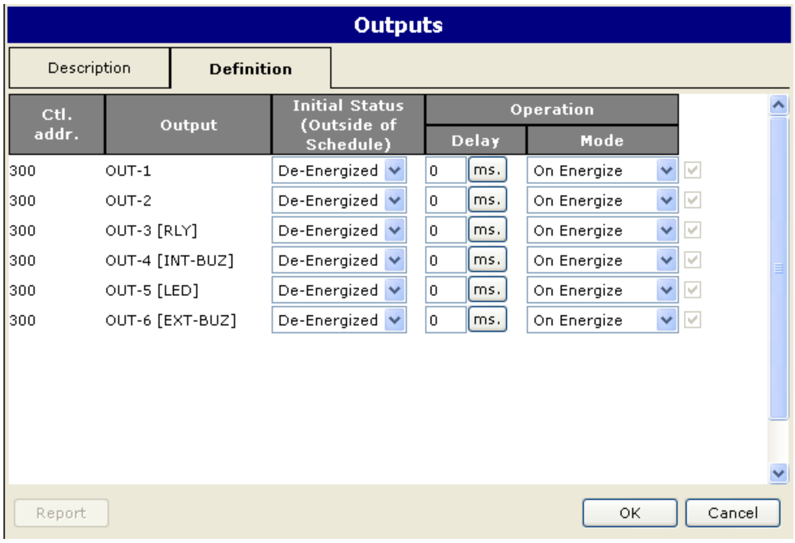
The **Outputs** screen will appear similar to what is shown below:



Ctl. addr.	Output	Description	Controller
300	OUT-1	OUT-1	eIDC 300
300	OUT-2	OUT-2	eIDC 300
300	OUT-3 [RLY]	OUT-3 [RLY]	eIDC 300
300	OUT-4 [INT-BUZ]	OUT-4 [INT-BUZ]	eIDC 300
300	OUT-5 [LED]	OUT-5 [LED]	eIDC 300
300	OUT-6 [EXT-BUZ]	OUT-6 [EXT-BUZ]	eIDC 300

The **Outputs** screen first appears with the **Description** tab being the active view. The **Description** tab view provides a description of each output used on the eIDC. The **Description** tab is only for viewing purposes, no edits or changes can be made form this view.

2. To continue programming the controller, select the **Definition** tab.



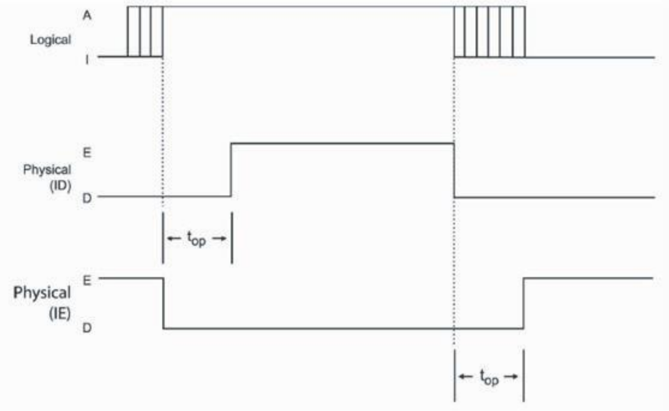
Outputs

Ctl. addr.	Output	Initial Status (Outside of Schedule)	Operation		
			Delay	Mode	
300	OUT-1	De-Energized	0 ms.	On Energize	☑
300	OUT-2	De-Energized	0 ms.	On Energize	☑
300	OUT-3 [RLY]	De-Energized	0 ms.	On Energize	☑
300	OUT-4 [INT-BUZ]	De-Energized	0 ms.	On Energize	☑
300	OUT-5 [LED]	De-Energized	0 ms.	On Energize	☑
300	OUT-6 [EXT-BUZ]	De-Energized	0 ms.	On Energize	☑

3. Select the **Initial Status (Outside of Schedule)** for each output "**De-Energized**" or "**Energized**." For example, if you want to program a door strike as fail secure, which means that the door should be locked (i.e., de-energized) if the power fails, then the initial status should be set as energize.

4. Enter an **Operation Delay** time (default is in milliseconds) for each output. The **Operation Delay** time delays the output before it is triggered. You can change the time value by clicking to highlight the value shown and then typing in the value needed.

5. Select an **Operation Mode** from the pull down for each output. The **Operation Mode** determines whether the delay happens before the output becomes energized or before it becomes de-energized. The following figure shows typical timing on energizing. Depending on the output's initial status, the delay is inserted either at the beginning or at the end of the cycle.



Logical state either I (inactive) or A (active -- driven by a service). Physical state either D (de-energized) or E (energized) based on initial state either Initially De-energized (ID) or Initially Energized (IE).

6. Click "**OK**" to save the output settings or "**Cancel**" to exit without saving. The System Management screen will be displayed.

Chapter 6: Services

Contents

The Intelli-M® Web Interface has simplified access control programming by developing services. A service is defined as a series of inputs, outputs, or triggers that interact with each other to perform a specific event. This Chapter provides instructions on how to program Access Services and Alarm Services within the Intelli-M Web Interface.

The following topics can be found within this Chapter:

Overview

Intelli-M Web Interface services have been broken down into the following two groups to make programming easier:

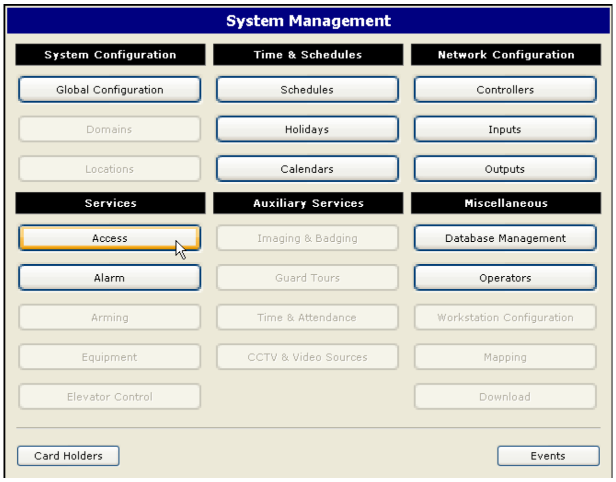
- **Access services --** provide the parameters for how access is programmed for doors. Only one access service can be programmed per eIDC.
- **Alarm services --** provide the relationship between inputs and outputs that need to be triggered according to a specific schedule, such as alarm supervision.

Programming Access Services

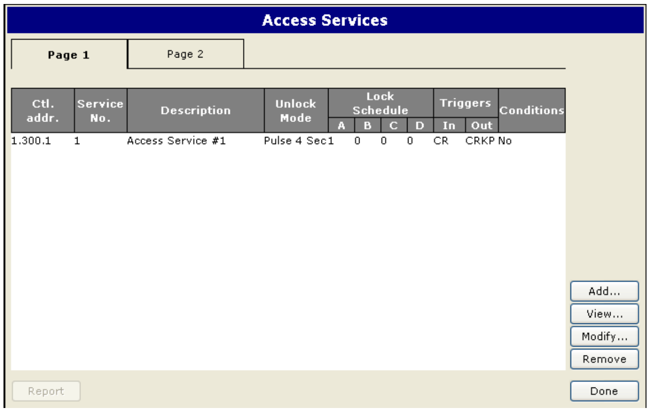
Access services provide the parameters for controlling specific doors. Only one access service can be programmed per eIDC.

To initiate an access service, complete the following steps:

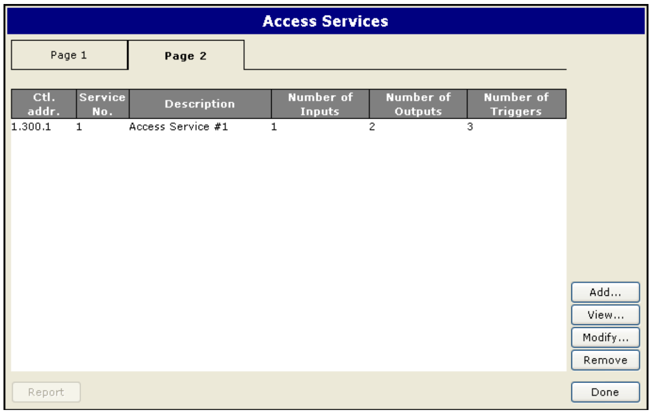
1. Click "**Access"** on the **System Management** screen.



The **Access Services** screen will appear. An eIDC can have one access service configured to it. The **Page 1** tab and **Page 2** tab provide a view of access data currently programmed into the eIDC controller. The initial viewing of these two tabs will show the default configuration if the eIDC controller was set up as described in Chapter 2.



Ctl. addr.	Service No.	Description	Unlock Mode	Lock Schedule				Triggers		Conditions
				A	B	C	D	In	Out	
1.300.1	1	Access Service #1	Pulse 4 Sec	1	0	0	0	CR	CRKP	No



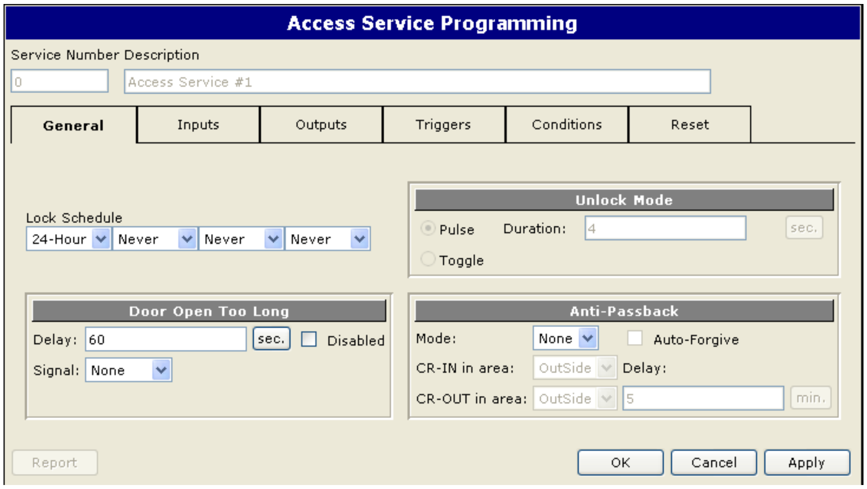
Ctl. addr.	Service No.	Description	Number of Inputs	Number of Outputs	Number of Triggers
1.300.1	1	Access Service #1	1	2	3

2. To create a new access service if the eIDC controller has not been programmed, click “**Add**.” To edit an existing access service (including default configuration data), click to highlight the service on either tab page and then click “**Modify**.”

Access Services—General Tab

To associate general information to this access service:

1. You can assign up to four **Lock Schedules** by using the appropriate pull down. Each drop-down menu displays the previously determined schedules. A Lock Schedule of “24-Hour” overrides all other schedules. For more information on schedules, see “Chapter 4: Schedules, Holidays, and Calendars.”



Service Number: 0 Description: Access Service #1

Lock Schedule: 24-Hour, Never, Never, Never

● Pulse Duration: 4 sec.

○ Toggle

Delay: 60 sec. □ Disabled

Signal: None

Mode: None □ Auto-Forgive

CR-IN in area: OutSide Delay: 5 min.

CR-OUT in area: OutSide

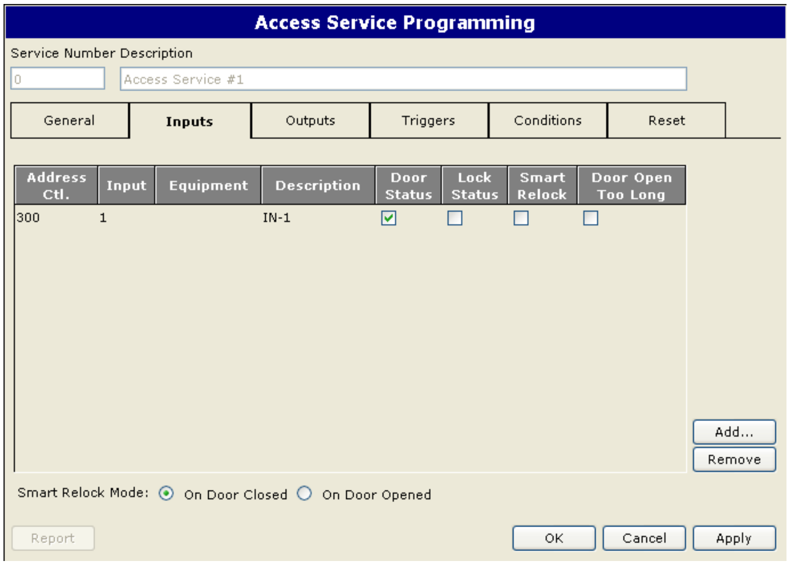
2. The **Unlock Mode** is automatically set to **Pulse**. Pulse activates a service for a determined duration, and the Duration is automatically set at 4 seconds.
3. In the **Door Open Too Long** (DOTL) section, enter a delay time or select the **Disabled** check box. The DOTL **Delay** time can be entered by clicking to highlight the number already there and then typing in a new number. To change the time interval, click to toggle the time interval button between seconds and minutes.
4. From the **Signal** drop down for DOTL, select whether a warning should be sent or no when a DOTL event occurs. Refer to "Access Services—Outputs Tab" in this Chapter for more information on selecting warning outputs.
5. To enable Anti-Passback, select either "**Soft**" or "**Hard**" from the **Mode** drop down list.
   - **Hard** -- With hard anti-passback, card holders are required to present their cards at the In Reader upon entering, and the Out Reader upon exiting. If a card holder enters behind another without presenting a card, the card holder is unable to use the card to enter or exit through any other doors until the **Auto-Forgive** (if enabled) **Delay** time has elapsed.
   - **Soft --** With soft anti-passback, card holders are allowed to re-enter or exit an area where they have not previously presented their cards; however, an alarm is reported on the **Event Monitoring** screen.
   - **Auto-Forgive --** If soft or hard anti-passback has been selected, Auto-Forgive can be enabled by clicking to check the Auto-Forgive check box, and then entering a **Delay** time (default is in minutes). The Auto-Forgive **Delay** time can be entered by clicking to highlight the number already there and then typing in a new number. To change the time interval, click to toggle the time button between minutes, hours, days and weeks.
6. After all the selections have been made, click the **Apply** button.

To continue programming the access service, click on the **Inputs** tab.

Access Services—Inputs Tab

To associate inputs with this access service:

1. Click on the **Inputs** tab on the **Access Service Programming** screen.



Access Service Programming

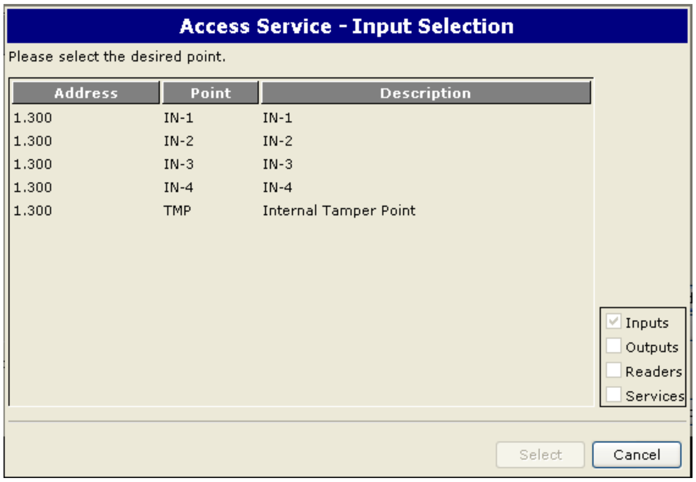
Service Number: 0

Description: Access Service #1

Address Ctl.	Input	Equipment	Description	Door Status	Lock Status	Smart Relock	Door Open Too Long
300	1		IN-1	☑	□	□	□

Smart Relock Mode: ● On Door Closed ○ On Door Opened

2. To program a new input, click the “**Add...**” button.



Access Service - Input Selection

Please select the desired point.

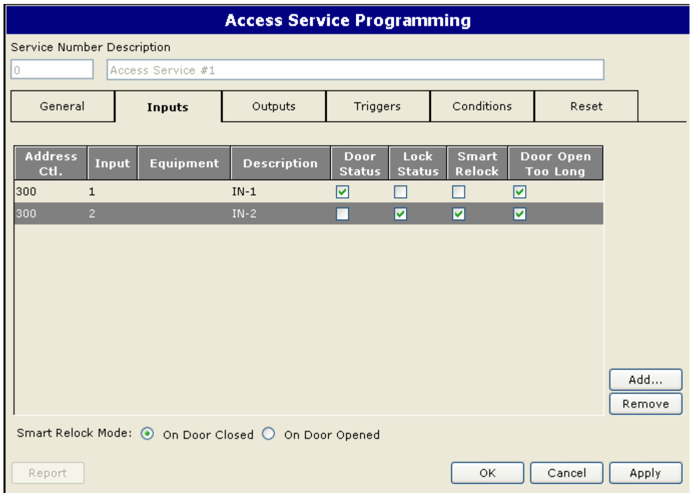
Address	Point	Description
1.300	IN-1	IN-1
1.300	IN-2	IN-2
1.300	IN-3	IN-3
1.300	IN-4	IN-4
1.300	TMP	Internal Tamper Point

☑ Inputs
□ Outputs
□ Readers
□ Services

3. Select the desired input and click the “**Select**” button. The door and lock status inputs are automatically bypassed when the door is unlocked.

4. In the **Inputs** tab, select by clicking to check the appropriate box or boxes of what the input will monitor. The choices of what the input can monitor are:

   - **Door Status** or **Lock Status**
   - **Smart Relock**
   - **Door Open Too Long**



Service Number: 0
Description: Access Service #1

Address Ctl.	Input	Equipment	Description	Door Status	Lock Status	Smart Relock	Door Open Too Long
300	1		IN-1	☑	□	□	☑
300	2		IN-2	□	☑	☑	☑

Smart Relock Mode: ● On Door Closed ○ On Door Opened

Smart Relock is a specialized function that gives greater control over when the door is actually relocked after legitimate access. It is independent of the unlock duration when the pulse mode is selected. If the door does not physically move during the pulse (as monitored by the inputs selected above for smart relock), the access service simply relocks at the end of the pulse. If the door physically opens and closes, the smart relock function takes over in one of the following ways which you can select:

- **On Door Closed** -- The access service locks again only when the door is closed.
- **On Door Opened** -- The access service locks as soon as the door is opened.

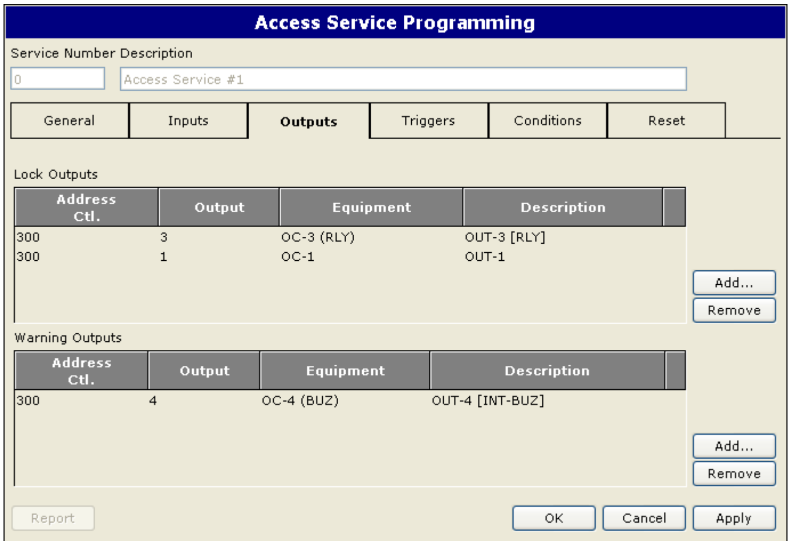
5. Add other inputs to the access service as required.
6. After all selections have been made, click the “**Apply**” button.

To continue programming the access service, click on the “**Outputs**” tab.

Access Services—Outputs Tab

To associate outputs with the access service:

1. Click on the **Outputs Tab** tab in the **Access Service Programming** screen.



Access Service Programming

Service Number Description

0 | Access Service #1

Lock Outputs

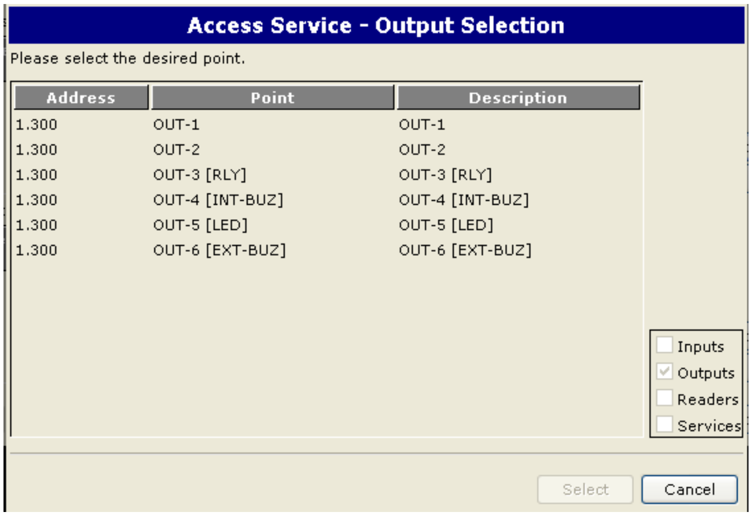
Address Ctl.	Output	Equipment	Description
300	3	OC-3 (RLY)	OUT-3 [RLY]
300	1	OC-1	OUT-1

Warning Outputs

Address Ctl.	Output	Equipment	Description
300	4	OC-4 (BUZ)	OUT-4 [INT-BUZ]

2. Outputs can be designated as **Lock Outputs** or **Warning Outputs**. Click the appropriate **Add** button for the type of output needed.

3. Choose an output from the list and click “**Select**.”



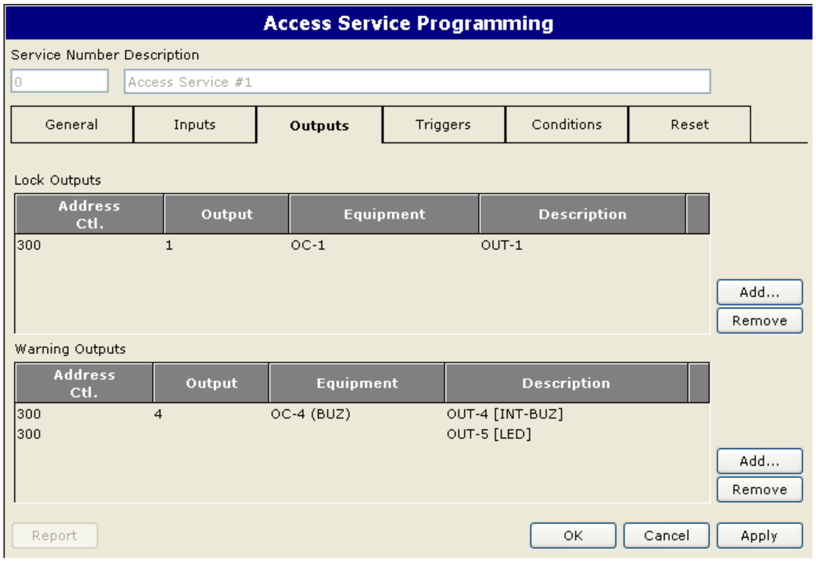
Access Service - Output Selection

Please select the desired point.

Address	Point	Description
1.300	OUT-1	OUT-1
1.300	OUT-2	OUT-2
1.300	OUT-3 [RLY]	OUT-3 [RLY]
1.300	OUT-4 [INT-BUZ]	OUT-4 [INT-BUZ]
1.300	OUT-5 [LED]	OUT-5 [LED]
1.300	OUT-6 [EXT-BUZ]	OUT-6 [EXT-BUZ]

□ Inputs
☑ Outputs
□ Readers
□ Services

4. When all **Lock Output** and/or **Warning Output** selections have been made, click the “**Apply**” button to validate the changes.



Service Number Description

0 Access Service #1

Lock Outputs

Address Ctl.	Output	Equipment	Description
300	1	OC-1	OUT-1

Warning Outputs

Address Ctl.	Output	Equipment	Description
300	4	OC-4 (BUZ)	OUT-4 [INT-BUZ]
300			OUT-5 [LED]

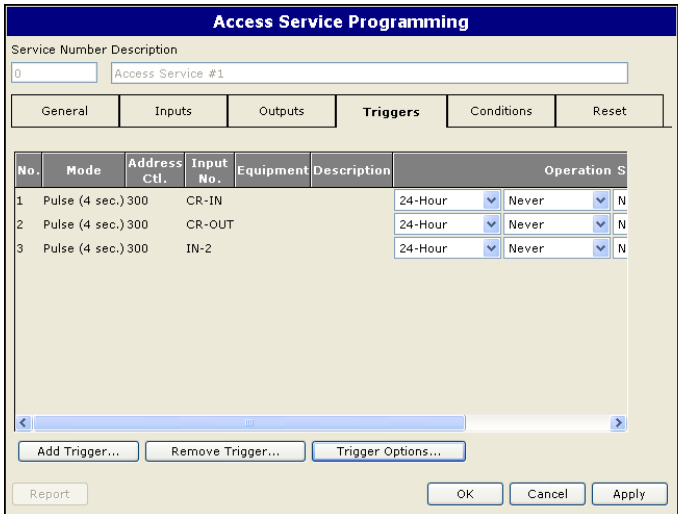
Note: In this example, both the warning buzzer and the LED are activated if the door is held open.

To continue programming the access service, click on the "**Triggers**" tab.

Access Services—Triggers Tab

The triggers associated with this access service are the readers or inputs, such as a remote button, for the door. To associate triggers with the access service, complete the following steps:

1. Click on the "**Triggers**" tab on the **Access Services Programming** screen.

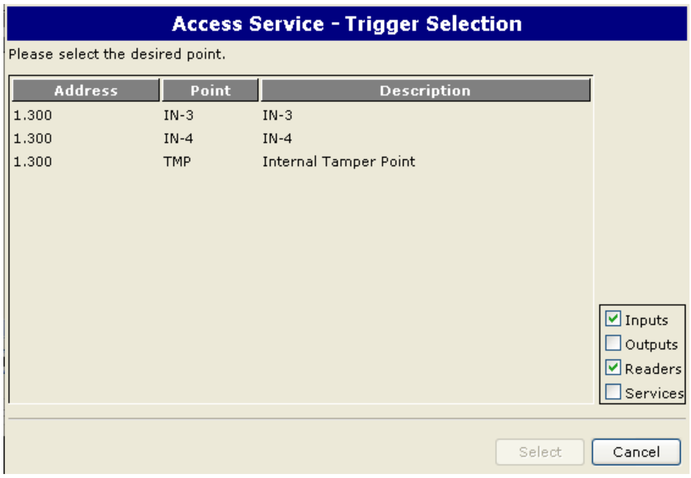


Service Number Description

0 Access Service #1

No.	Mode	Address Ctl.	Input No.	Equipment	Description	Operation S		
1	Pulse (4 sec.)	300	CR-IN			24-Hour	Never	N
2	Pulse (4 sec.)	300	CR-OUT			24-Hour	Never	N
3	Pulse (4 sec.)	300	IN-2			24-Hour	Never	N

2. To select a trigger device, click "**Add Trigger**." These triggers activate the outputs (unlock the door) and bypass the inputs.



Access Service - Trigger Selection

Please select the desired point.

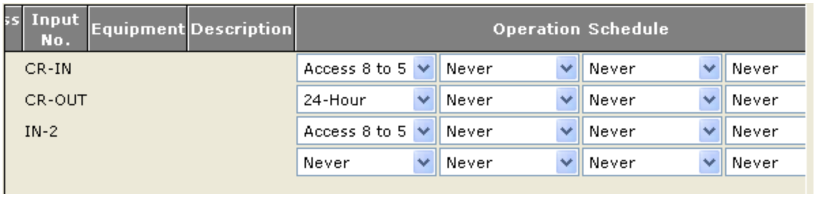
Address	Point	Description
1.300	IN-3	IN-3
1.300	IN-4	IN-4
1.300	TMP	Internal Tamper Point

☑ Inputs
☐ Outputs
☑ Readers
☐ Services

3. Choose a new trigger by clicking to highlight the desired trigger, and then click the "**Select**" button.

   Note: To display the available **Inputs**, **Outputs**, **Readers**, and/or **Services**, click to check the appropriate check box (lower right-hand side of screen).

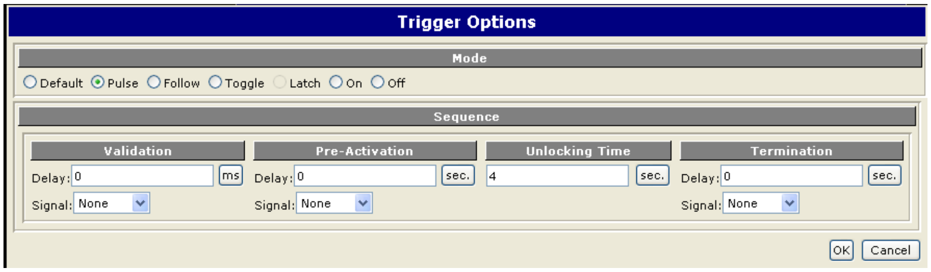
4. For each trigger you have, you can select up to four Operation Schedules which are used to determine when the trigger is considered for service activation. Outside this schedule, the trigger has no effect on the service. A pull down is available for each **Operation Schedule**.



ss	Input No.	Equipment	Description	Operation Schedule			
	CR-IN			Access 8 to 5	Never	Never	Never
	CR-OUT			24-Hour	Never	Never	Never
	IN-2			Access 8 to 5	Never	Never	Never
				Never	Never	Never	Never

Advanced Trigger Options

For advanced applications, it might be appropriate to program trigger options. If advanced trigger options are not needed, skip the following procedures and move ahead to the section on Access Services—Conditions Tab. For advanced programming options, select the appropriate trigger and click "**Trigger Options**" from the **Triggers** tab, and then complete the following steps:



Trigger Options

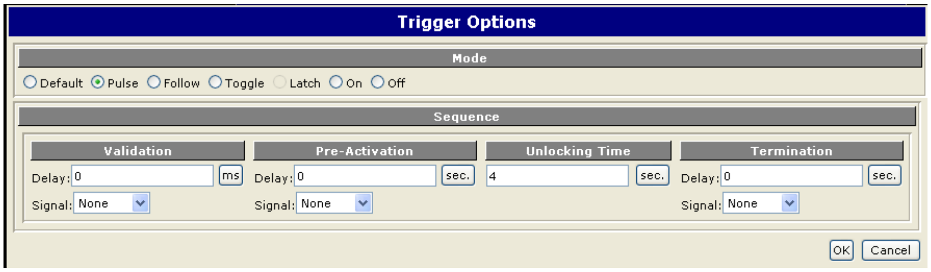
Mode

○ Default ● Pulse ○ Follow ○ Toggle ○ Latch ○ On ○ Off

Sequence

Validation	Pre-Activation	Unlocking Time	Termination
Delay: 0 ms	Delay: 0 sec.	4 sec.	Delay: 0 sec.
Signal: None	Signal: None		Signal: None

1. Select the trigger **Mode**. The basic execution sequence has the same form in all services with slight variations depending on the selected **Mode** activation, which specifies how the service reacts to status changes of the trigger point. The **Sequence** is determined by a series of timing parameters that affect how service activation unfolds through time.



Trigger Options

Mode

○ Default ● Pulse ○ Follow ○ Toggle ○ Latch ○ On ○ Off

Sequence

Validation	Pre-Activation	Unlocking Time	Termination
Delay: 0 ms	Delay: 0 sec.	4 sec.	Delay: 0 sec.
Signal: None	Signal: None		Signal: None

The default **Mode** varies based on the mode selected in the **General** tab. Mode options include the following:

- **Pulse** -- This activates the service for a determined duration.
- **Follow** -- The service remains active as long as the trigger remains active. For example, when interlocking two points, the second point takes on the same state as the triggering point.
- **Toggle** -- The trigger inverts the current state of the service, and the service is alternately activated and deactivated by the trigger.
- **Latch** -- The service is activated and remains activated indefinitely until it is reset.
- **On** -- The trigger activates the service until it is superseded by another trigger (see the Trigger Simultaneously section).
- **Off** -- The trigger deactivates the service until it is superseded by another trigger (see the Trigger Simultaneously section).

Note: TOGGLE and **OFF** modes can deactivate a service, contrary to all other activation modes that activate the service. The activation sequence described here applies symmetrically in these cases, with the terms "**Activation**" and "**De-activation**" exchanging positions.

2. Enter a "**Validation Delay**" time and select if a "**Signal**" (i.e., warning) is needed. Validation is a specified delay during which the trigger must remain active in order to engage the remainder of the sequence. If the trigger is released before the delay has elapsed, the entire sequence is aborted. An optional signal can be generated during this step by using the warning outputs. For example, there might be a **Validation Delay** time of three seconds for a push bar on an emergency door. If the push bar is held down for two seconds and then released, the service does not continue through the remainder of the activation sequence. However, if the push bar is held down for the entire three seconds, the execution sequence enters the **Pre-Activation** stage.

3. Enter a **Pre-Activation** time, and select if a "**Signal**" (i.e., warning) is needed. **Pre-Activation** is an additional delay before the service is actually activated. The difference between pre-activation and validation is that after the pre-activation stage has been reached, the sequence is not aborted even if the trigger is released. An optional signal can be generated during this stage by using the warning outputse.

4. Enter an **Unlocking** time. This option is automatically selected with a preset unlocking time if the **Pulse** mode is selected. In **Pulse** mode, the unlocking time parameter determines the exact time duration of this stage. To enter an alternative unlocking time, select the pulse mode (instead of using the default) and enter the unlocking time (the default time unit for unlocking is in seconds). Click on the current time unit to alternate between seconds and minutes.

5. Enter a **Termination Delay** and select if a "**Signal**" (i.e., warning) is needed. Termination delay is available only in pulse or default mode (if the default is set to pulse). Termination enables the production of an optional warning signal for a certain amount of time before the end of the sequence is reached.
6. When finished, click "**OK**" to return to the **Triggers** tab.
7. Click "**Apply**" to validate the changes.

To continue programming the access service, click on the "**Conditions**" tab.

Access Services—Conditions Tab

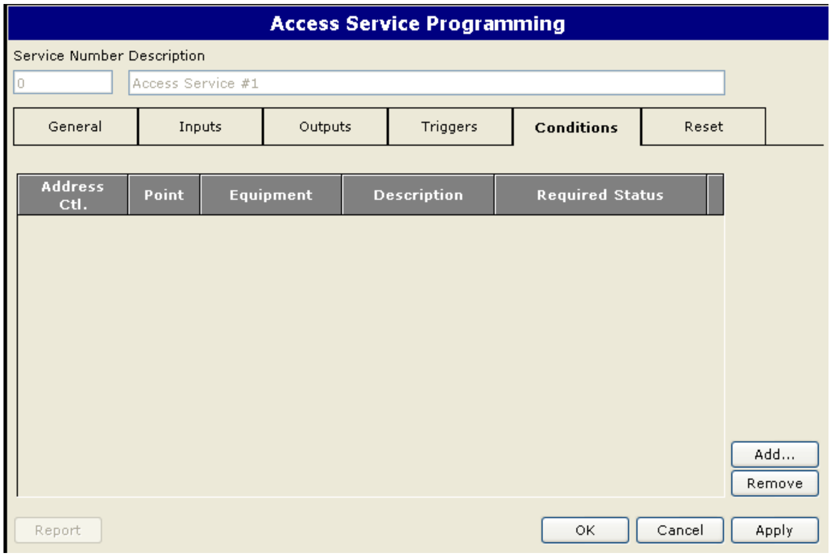
Conditions are used to enable triggers in specific situations. Service activation can be programmed in such a way to require that specific circumstances in the system occur in order to run the service. If those conditions do not occur, the condition completely prevents the service from running.

Conditions are usually based on input points, but the Intelli-M Web Interface also allows you to select outputs as condition points. For example, a simple mantrap could be implemented by defining two access services, each of which includes the other in its condition list with required status as **LOCKED**. This would prevent unlocking any one access service when the other is already unlocked.

> **Note:** An unassertive condition does not prevent service deactivation. An example of this would be from a trigger with mode **OFF**.

To associate a condition with this access service, complete the following steps:

1. Click the "**Conditions**" tab on the **Access Services Programming** screen.

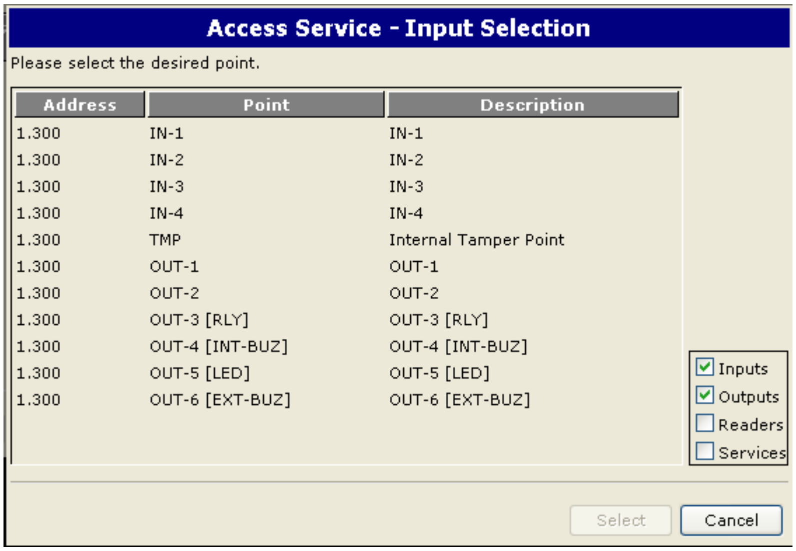


Access Service Programming

Service Number: 0
Description: Access Service #1

Address Ctl.	Point	Equipment	Description	Required Status

2. To program a new condition, click the "**ADD**" button.



Access Service - Input Selection

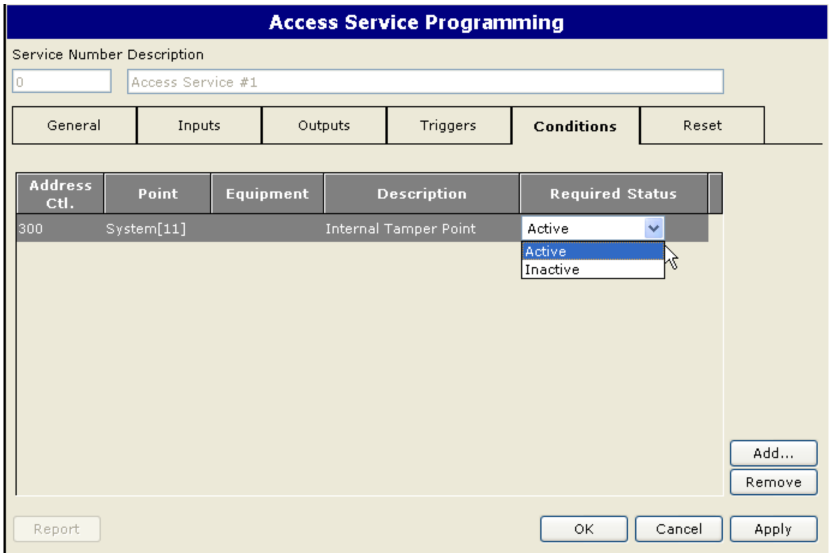
Please select the desired point.

Address	Point	Description
1.300	IN-1	IN-1
1.300	IN-2	IN-2
1.300	IN-3	IN-3
1.300	IN-4	IN-4
1.300	TMP	Internal Tamper Point
1.300	OUT-1	OUT-1
1.300	OUT-2	OUT-2
1.300	OUT-3 [RLY]	OUT-3 [RLY]
1.300	OUT-4 [INT-BUZ]	OUT-4 [INT-BUZ]
1.300	OUT-5 [LED]	OUT-5 [LED]
1.300	OUT-6 [EXT-BUZ]	OUT-6 [EXT-BUZ]

☑ Inputs
☑ Outputs
☐ Readers
☐ Services

3. To display the available **Inputs**, **Outputs**, **Readers**, and/or **Services**, click to check the appropriate check box (lower right-hand side of screen). Then choose the input, output, reader or service that you want to create the condition for and click the "**Select**" button.

4. In order for the condition to be asserted and thereby permit service activation, all the listed points must be in their required status as selected next to each point. To select the **Required Status**, click the pull-down arrow in the column next to the desired point and select the desired status (either Active or Inactive). Available selections depend on the type of point selected.



Access Service Programming

Service Number Description

0 | Access Service #1

Address Ctl.	Point	Equipment	Description	Required Status
300	System[11]		Internal Tamper Point	Active

5. After all selections have been made, click the "**Apply**" button to validate the changes.

To continue programming the access service, click on the "**Reset**" tab.

Access Services—Reset Tab

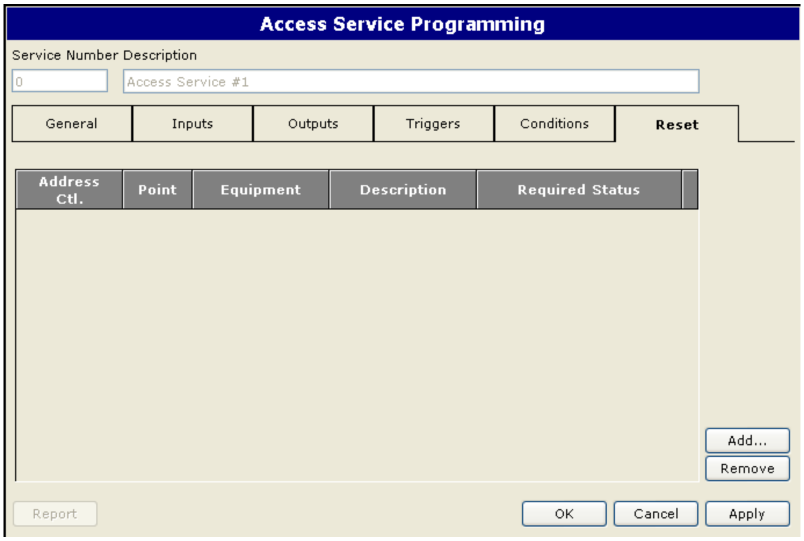
When a service is executed in **Latch** mode (see “Advance Trigger Options” which was previously discussed in this Chapter), it must be reset in order to return the service to an idle state. This can be done in the appropriate service control panel, or by programming a set of reset points into the service regarding when the service should be reset externally. This section lists the selected reset points for the service. A reset can also be programmed to stop the execution of a service at any point during its activation sequence, regardless of the activation mode.

The following should also be noted about the reset function:

- When a service is reset anywhere in the sequence (with the exception of the validation step), the remainder of the sequence is aborted and the service immediately deactivates.
- During validation, reset applies to all validation timers in progress. Instead of canceling the sequence, it merely restarts the sequence at the beginning if the triggers are still active.
- When the current trigger uses the **Follow** mode and a service reset occurs, the service is momentarily deactivated; if the trigger is still active though, it is immediately re-engaged.
- Resetting a service does not necessarily deactivate it; resetting brings the service back to its scheduled state. That is, it resets the service to where it should be according to its activation schedule (or lock schedule, with regard to access) as defined in service programming. This is also the case when particular activation sequences end. For example, activating a trigger in **Pulse** mode while the service is already within its activation schedule has no effect on the service.

To program a reset function for the access service, complete the following steps:

1. Click the “**Reset**” tab on the **Access Services Programming** screen.



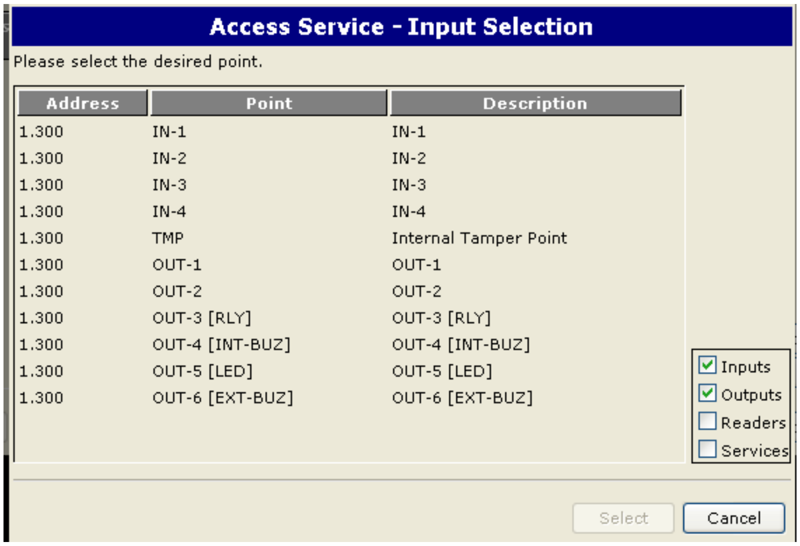
Access Service Programming

Service Number Description

0 | Access Service #1

Address Ctl.	Point	Equipment	Description	Required Status

2. To program a new **Reset** function, click the “**ADD**” button.



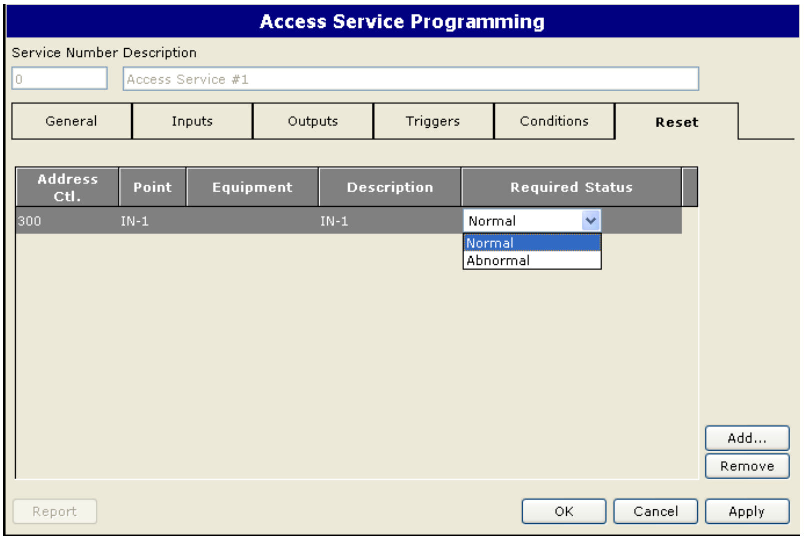
Access Service - Input Selection

Please select the desired point.

Address	Point	Description
1.300	IN-1	IN-1
1.300	IN-2	IN-2
1.300	IN-3	IN-3
1.300	IN-4	IN-4
1.300	TMP	Internal Tamper Point
1.300	OUT-1	OUT-1
1.300	OUT-2	OUT-2
1.300	OUT-3 [RLY]	OUT-3 [RLY]
1.300	OUT-4 [INT-BUZ]	OUT-4 [INT-BUZ]
1.300	OUT-5 [LED]	OUT-5 [LED]
1.300	OUT-6 [EXT-BUZ]	OUT-6 [EXT-BUZ]

☑ Inputs
☑ Outputs
☐ Readers
☐ Services

3. To display the available **Inputs**, **Outputs**, **Readers**, and/or **Services**, click to check the appropriate check box (lower right-hand side of screen). Then choose the input, output, reader or service that you want to create the reset for and click the "**Select**" button.
4. The service is reset when any of the listed reset points are in the required status as selected next to each point. To select the **Required Status**, click the pull-down arrow in the column next to the desired point and select the desired status (either Normal or Abnormal). Available selections vary depending on the type of point selected.



Access Service Programming

Service Number: 0
Description: Access Service #1

Address Ctl.	Point	Equipment	Description	Required Status
300	IN-1		IN-1	Normal

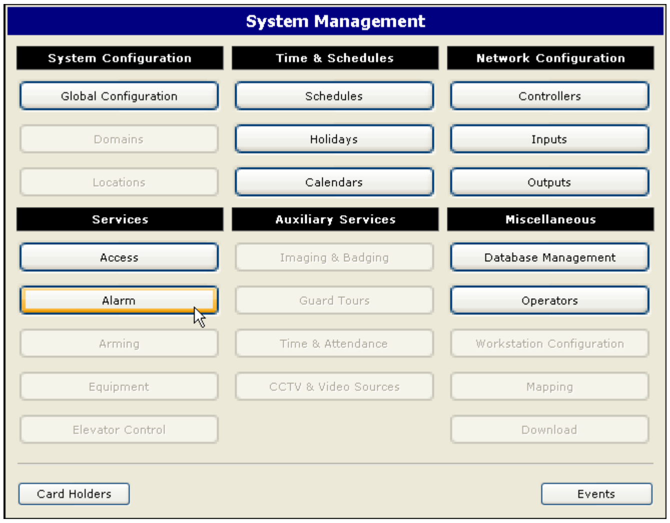
5. After all selections have been made, click the "**Apply**" button to validate the changes.

Programming Alarm Services

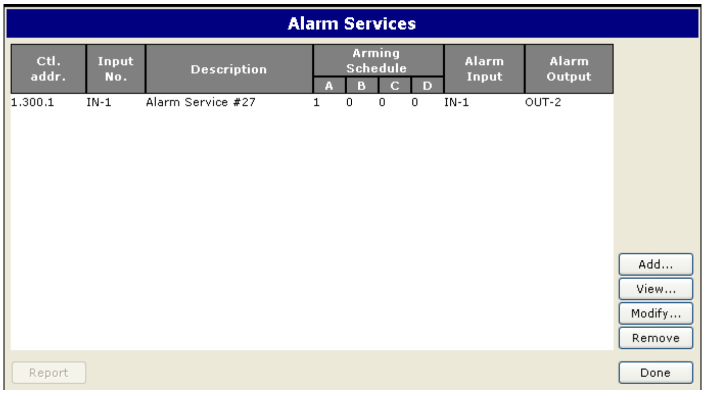
Alarm services create the link between inputs and the outputs that are triggered according to specific schedules. When access services are programmed, the Intelli-M Web Interface automatically creates an alarm service associated with the inputs in the access service.

To initiate an alarm service, complete the following steps:

1. Click “**Alarms”** on the **System Management** screen.

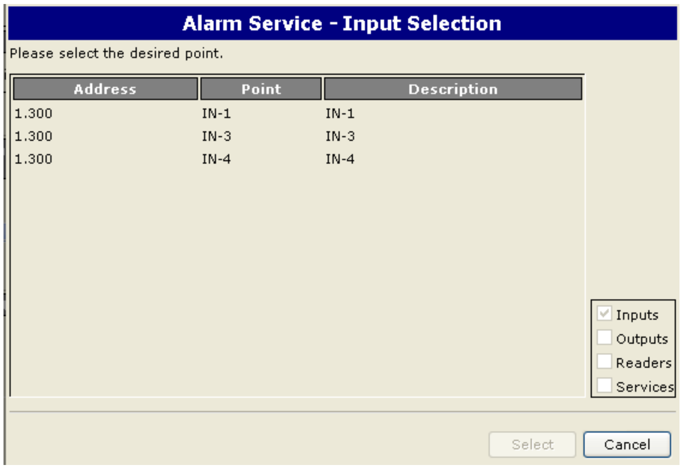


The **Alarm Services** screen will be displayed.



Ctl. addr.	Input No.	Description	Arming Schedule				Alarm Input	Alarm Output
			A	B	C	D		
1.300.1	IN-1	Alarm Service #27	1	0	0	0	IN-1	OUT-2

2. If you want to create a new alarm service, click the “**ADD**” button. The “**Alarm Service-Input Selection**” screen will appear.



Alarm Service - Input Selection

Please select the desired point.

Address	Point	Description
1.300	IN-1	IN-1
1.300	IN-3	IN-3
1.300	IN-4	IN-4

☑ Inputs
☐ Outputs
☐ Readers
☐ Services

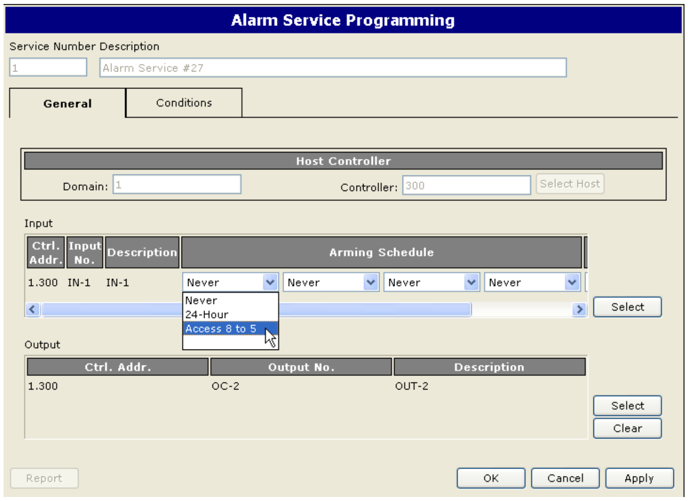
From the “**Alarm Service-Input Selection**” screen, select the desired input the alarm is to be associated with and then click the “**Select**” button. The **Alarm Services Programming** screen will be displayed. To continue defining the alarm service, refer to the “**General”** tab section below.

3. If you want to edit an existing input service, select the service and click the “**Modify**” button. The **Alarm Services Programming** screen will be displayed. To continue defining the alarm service, refer to the “**General”** tab section below.

Alarm Services—General Tab

To associate general information to an alarm service:

1. In the **Arming Schedule** section of the **Alarm Services Programming** screen, select up to four schedules from the pull downs. The schedules are used to determine when the alarm service is armed. Outside the schedules, the alarm is not triggered, even when its input becomes abnormal. Click the down arrow button to choose the schedule you want.



Alarm Service Programming

Service Number Description

1 | Alarm Service #27

Host Controller

Domain: 1 Controller: 300

Input

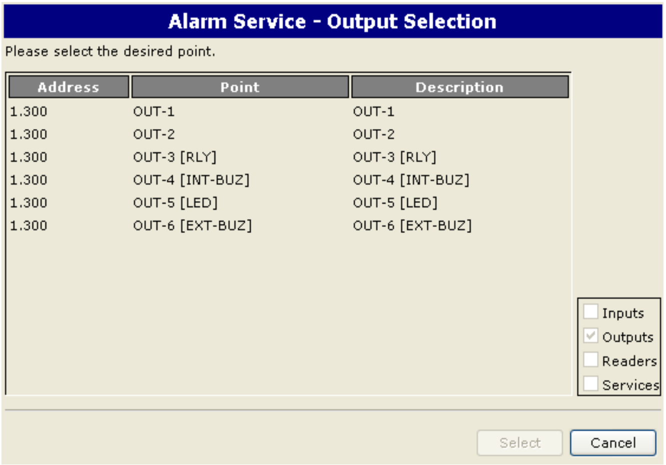
Ctrl. Addr.	Input No.	Description	Arming Schedule			
1.300	IN-1	IN-1	Never	Never	Never	Never

Output

Ctrl. Addr.	Output No.	Description
1.300	OC-2	OUT-2

You can click the “**Select**” button for the **Arming Schedule** section to display the “**Alarm Service-Input Selection**” screen again if you want to choose a different input.

2. Click on the "**Select**" button for the **Output** section. The "**Alarm Service-Output Selection**" screen will be displayed.



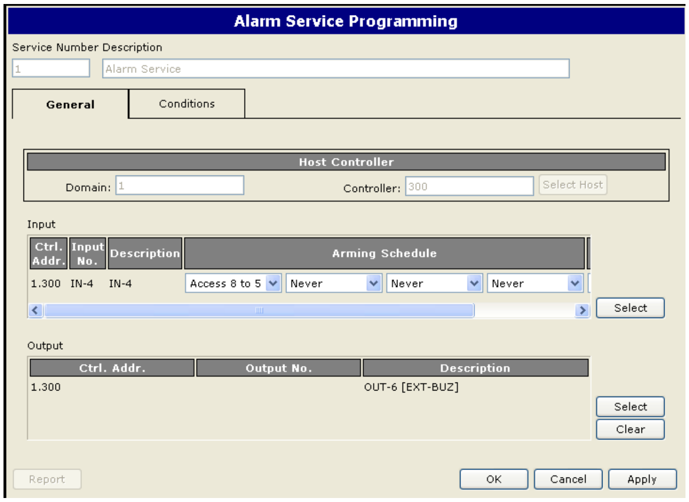
Alarm Service - Output Selection

Please select the desired point.

Address	Point	Description
1.300	OUT-1	OUT-1
1.300	OUT-2	OUT-2
1.300	OUT-3 [RLY]	OUT-3 [RLY]
1.300	OUT-4 [INT-BUZ]	OUT-4 [INT-BUZ]
1.300	OUT-5 [LED]	OUT-5 [LED]
1.300	OUT-6 [EXT-BUZ]	OUT-6 [EXT-BUZ]

□ Inputs
☑ Outputs
□ Readers
□ Services

3. Choose the desired output from the list of outputs and click the "**Select**" button. The **Alarm Services Programming** screen will display listing the output you selected.



Alarm Service Programming

Service Number Description
1 Alarm Service

Host Controller

Domain: 1 Controller: 300

Input

Ctrl. Addr.	Input No.	Description	Arming Schedule			
1.300	IN-4	IN-4	Access 8 to 5	Never	Never	Never

Output

Ctrl. Addr.	Output No.	Description
1.300		OUT-6 [EXT-BUZ]

4. Click the "**Apply**" button to validate the changes.

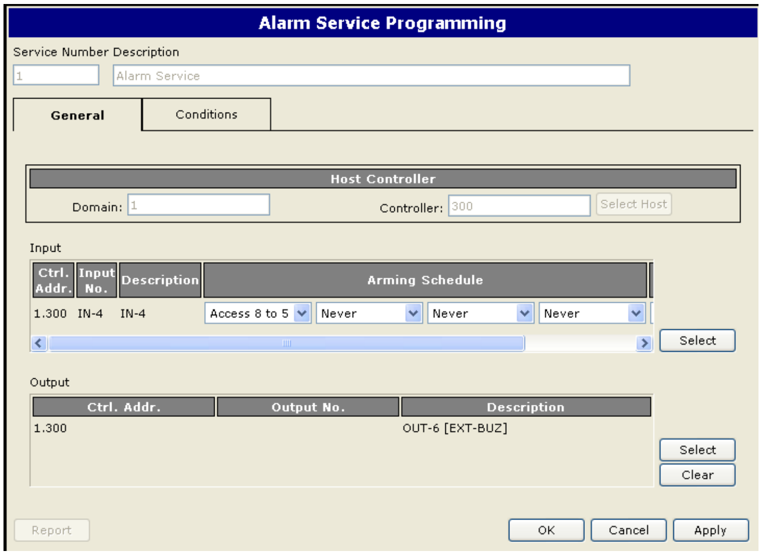
To enable the alarm service only in specific situations, you must program a condition. Click the "**Conditions**" tab to continue.

Alarm Services—Conditions Tab

To program a new condition, perform the following steps:

1. If you want to choose a different input for the condition, then from the **Alarm Services** screen click the "**Add**" button. The "**Alarm Service-Input Selection**" screen will be displayed. Click to highlight the input you want, and then click the "**Select**" button so that the **Alarm Services Programming** screen is displayed.

   If you want to modify an existing input on the **Alarm Services** screen so that it has a condition, then click to highlight the input you want. Then click the "**Modify**" button so that the **Alarm Services Programming** screen is displayed.



Alarm Service Programming

Service Number: 1
Description: Alarm Service

Host Controller

Domain: 1
Controller: 300

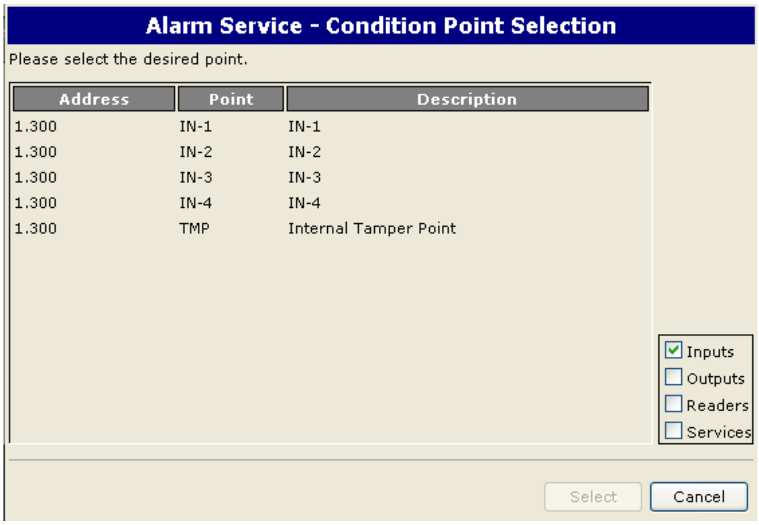
Input

Ctrl. Addr.	Input No.	Description	Arming Schedule			
1.300	IN-4	IN-4	Access 8 to 5	Never	Never	Never

Output

Ctrl. Addr.	Output No.	Description
1.300		OUT-6 [EXT-BUZ]

2. Click the **Conditions** tab.
3. Click "**ADD**" button. The **Alarm Service - Condition Point Selection**" screen will be displayed.



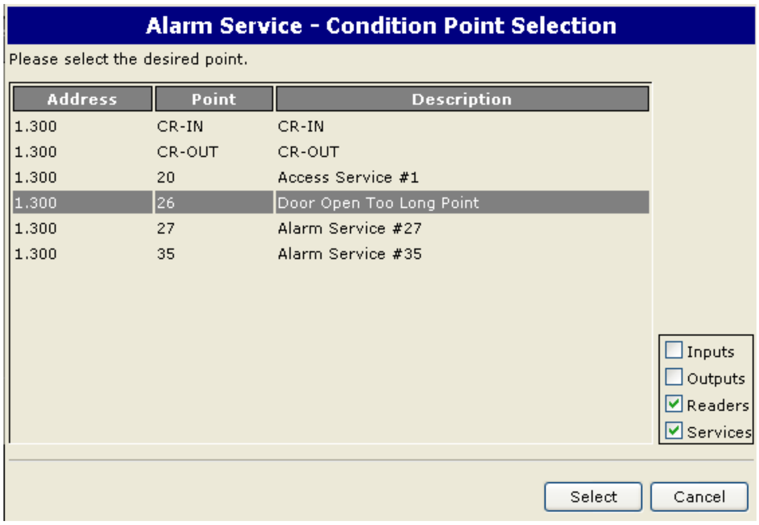
Alarm Service - Condition Point Selection

Please select the desired point.

Address	Point	Description
1.300	IN-1	IN-1
1.300	IN-2	IN-2
1.300	IN-3	IN-3
1.300	IN-4	IN-4
1.300	TMP	Internal Tamper Point

☑ Inputs
☐ Outputs
☐ Readers
☐ Services

4. To display the available **Inputs**, **Outputs**, **Readers**, and/or **Services**, click to check the appropriate check box (lower right-hand side of screen). Then choose the input, output, reader or service that you want to create the condition for and click the "**Select**" button.



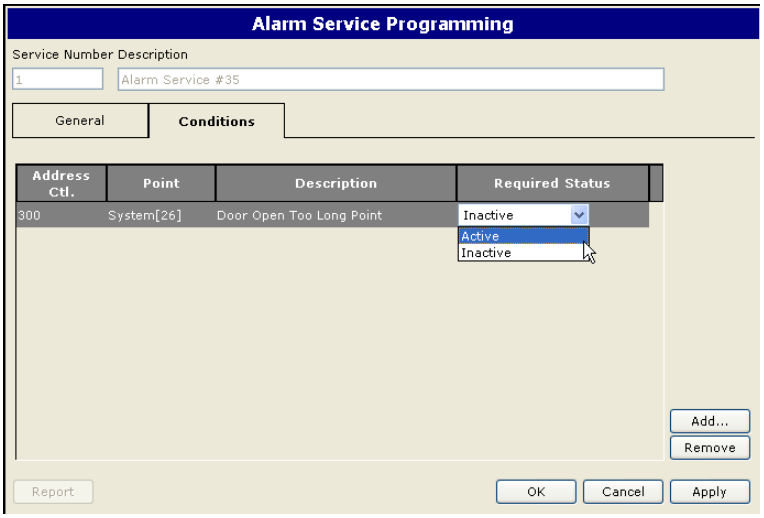
Alarm Service - Condition Point Selection

Please select the desired point.

Address	Point	Description
1.300	CR-IN	CR-IN
1.300	CR-OUT	CR-OUT
1.300	20	Access Service #1
1.300	26	Door Open Too Long Point
1.300	27	Alarm Service #27
1.300	35	Alarm Service #35

□ Inputs
□ Outputs
☑ Readers
☑ Services

5. For the condition to be asserted -- and thereby to permit service activation -- all listed points must be in their **Required Status**, as selected in the list next to each point. To select the **Required Status**, click the down arrow button in the column next to the desired point and choose from the **Required Status** drop-down list. Available selections depend on the type of point selected.



Alarm Service Programming

Service Number: 1
Description: Alarm Service #35

Address Ctl.	Point	Description	Required Status
300	System[26]	Door Open Too Long Point	Inactive

6. The **Add...** button can be used to add other conditions. After all selections have been made, click the "**Apply**" button to validate the changes.

Chapter 7: Card Holders And Badging

Contents

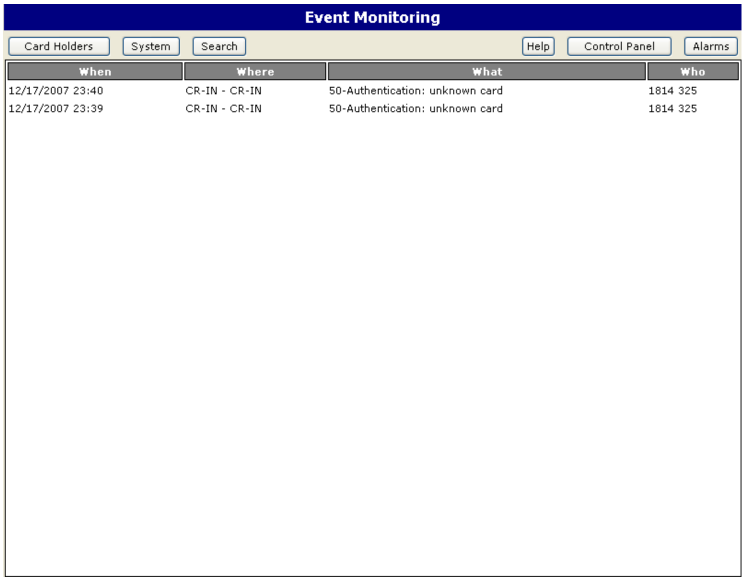
In the Intelli-M® Web Interface, administrators grant permissions for certain individuals to access certain areas at certain times. These permissions are granted via cards or keytags. Options for the cards can be defined in the system, and then each card holder can be added to the system within a Card Holder Record.

The following topics can be found within this Chapter:

Accessing The Card Holders Screen

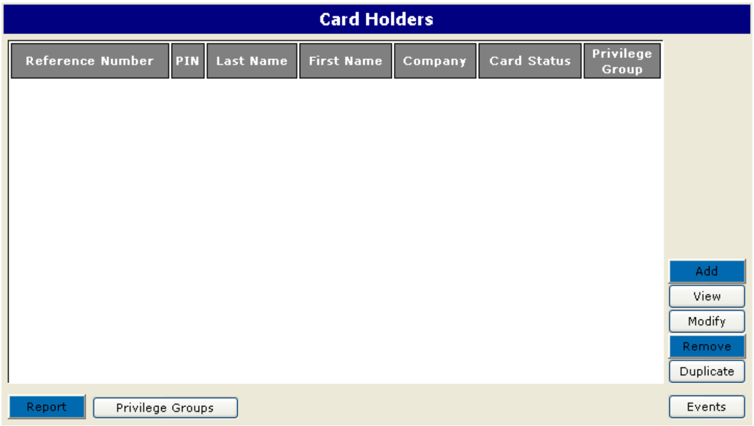
The **Card Holders** screen defines the association between the card holder (a person), a credential (card or key tag), and the privileges granted to the person. To access the **Card Holders** screen, do the following:

-- Click on “**Card Holders**” on the **Event Monitoring** screen.



When	Where	What	Who
12/17/2007 23:40	CR-IN - CR-IN	50-Authentication: unknown card	1814 325
12/17/2007 23:39	CR-IN - CR-IN	50-Authentication: unknown card	1814 325

The **Card Holders** screen will be displayed.



Reference Number	PIN	Last Name	First Name	Company	Card Status	Privilege Group

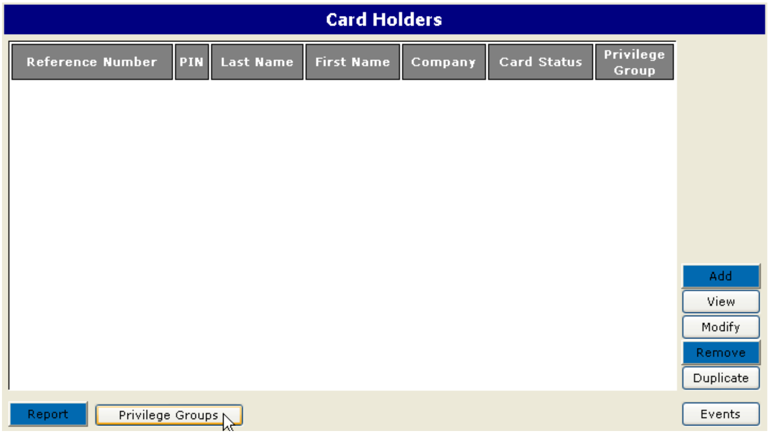
Privilege Groups

It is likely that certain groups of people require identical access privileges in a typical organization. Instead of programming access privileges separately to each individual, you can create privilege groups and then assign each individual to a group. For example, you might create a privilege group for managers, another for hourly employees, and another for a cleaning crew.

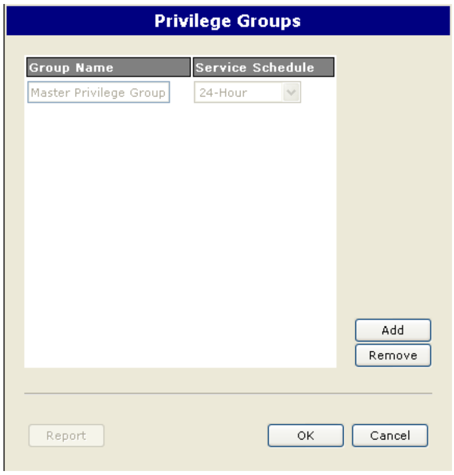
> **Note:** Access privileges can also be assigned individually.

To create a new privilege group, complete the following steps:

1. Click "**Privilege Groups**" on the **Card Holders** screen.



The **Privilege Groups** screen will be displayed.

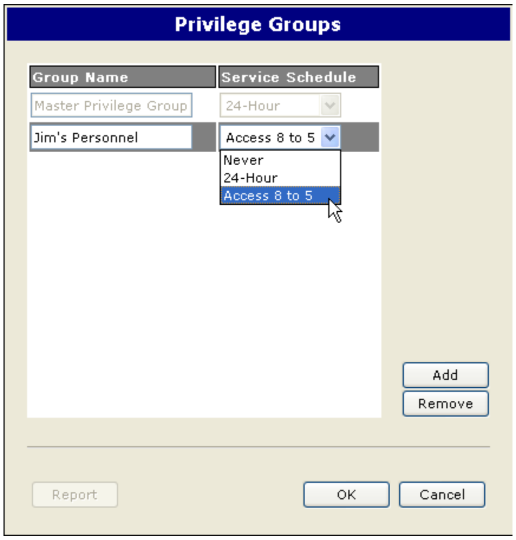


Group Name	Service Schedule
Master Privilege Group	24-Hour

2. To create a new privilege group, click the "**Add**" button. "Privilege Group #0"will show as the default Group Name. You can enter a group name of your choice by highlighting "Privilege Group #" and typing in the name that you want.

   To remove an existing privilege group, click to highlight the group name and then click "**Remove**" button.

3. Select a service schedule for the privilege group by choosing a schedule from the drop-down list. If a new schedule is required, refer to “Chapter 4: Schedules, Holidays, Calendars” for information on how to create a schedule.



Privilege Groups

Group Name	Service Schedule
Master Privilege Group	24-Hour
Jim's Personnel	Access 8 to 5

4. If more Privilege Groups (i.e., Group Name with Service Schedule) need to be created, click the “**Add**” button and repeat the naming and service scheduling procedures.

5. When finished, click the “**OK**” button to return to the **Card Holders** screen.

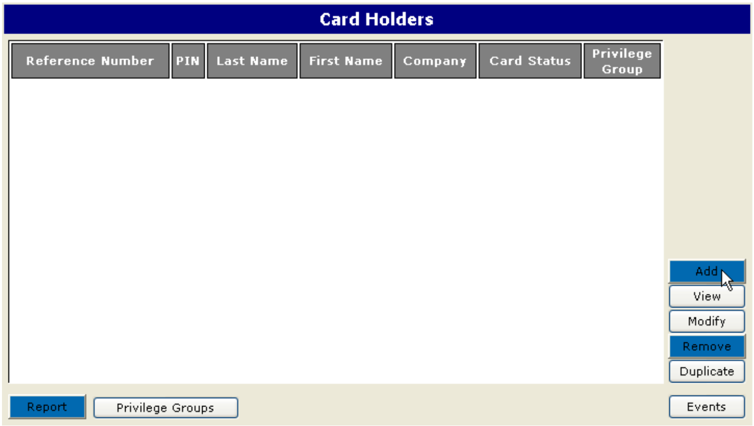
Adding Card Holders Into The System

Now that the system has been programmed for card holder privilege group(s), you are ready to start adding card holders to the system. The card information you provide about each card holder will become part of the card holder record.

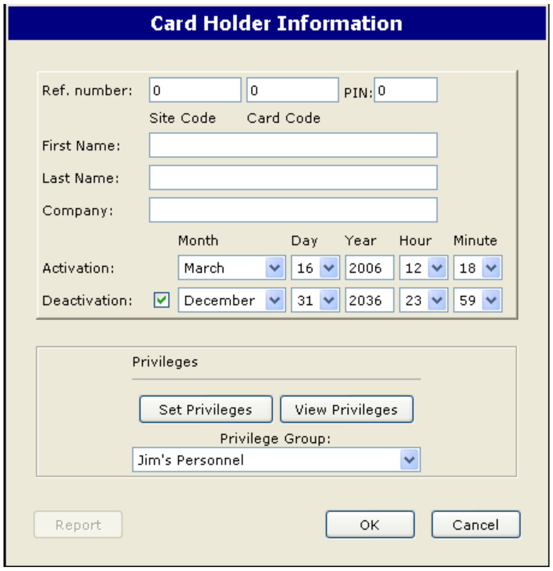
To program a card holder record, complete the following steps:

1. To create a new card holder record, click "**Add**" on the **Card Holders** screen.

   For already existing card holder records that need to be edited, click to highlight the record and then click the "**Modify**" button. To create a new card holder record that has the same privileges of an existing card, select the existing card and click "**Duplicate**."



   The "**Card Holder Information**" screen will be displayed.



Ref. number: 0 0 PIN: 0
Site Code Card Code
First Name:
Last Name:
Company:

		Month	Day	Year	Hour	Minute
Activation:		March	16	2006	12	18
Deactivation:	☑	December	31	2036	23	59

Privilege Group: Jim's Personnel

2. Assign a **Site Code** and **Card Code** since the Web Interface only allows cards that use the Weigand format at this time.

3. Enter a PIN (personal identification number) number that can be used for more secure identity checks when a card reader/keypad is available. PINs can be up to four digits.

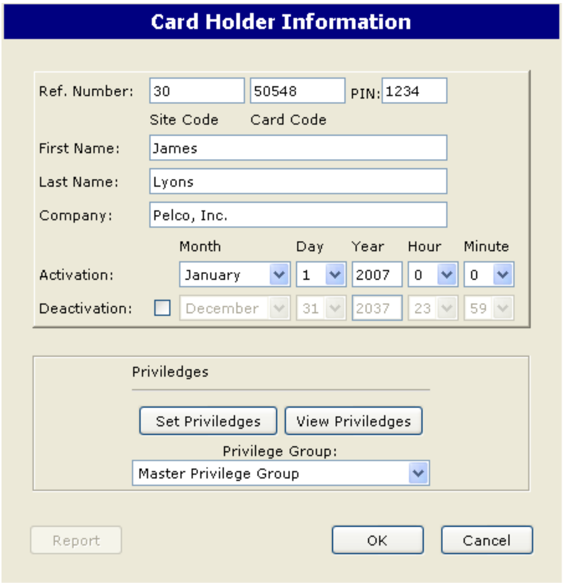
4. Enter the card holder’s **First Name** and **Last Name**. The “First Name” field is limited to 30 characters. The “Last Name” field is limited to 60 characters.

5. Enter the company name (or a branch or department name) in the **Company** field. The “Company” field is limited to 40 characters.

6. Use the pull downs to enter an **Activation** date and time. The default activation date and time is set to the current day at approximately midnight.

   Note: Every card must be programmed with a specific **Activation** date. The card cannot be accepted as valid by the system until the activation time is reached.

7. You have the option of having a **Deactivation** date and time via the check box. When the check box is checked, the **Deactivation** fields become active. If a deactivation date and time is entered, the system automatically rejects the card starting at that date and time. Leave the deactivation field empty if the card should not expire.



Card Holder Information

Ref. Number: 30 (Site Code) 50548 (Card Code) PIN: 1234

First Name: James

Last Name: Lyons

Company: Pelco, Inc.

	Month	Day	Year	Hour	Minute
Activation:	January	1	2007	0	0
Deactivation: □	December	31	2037	23	59

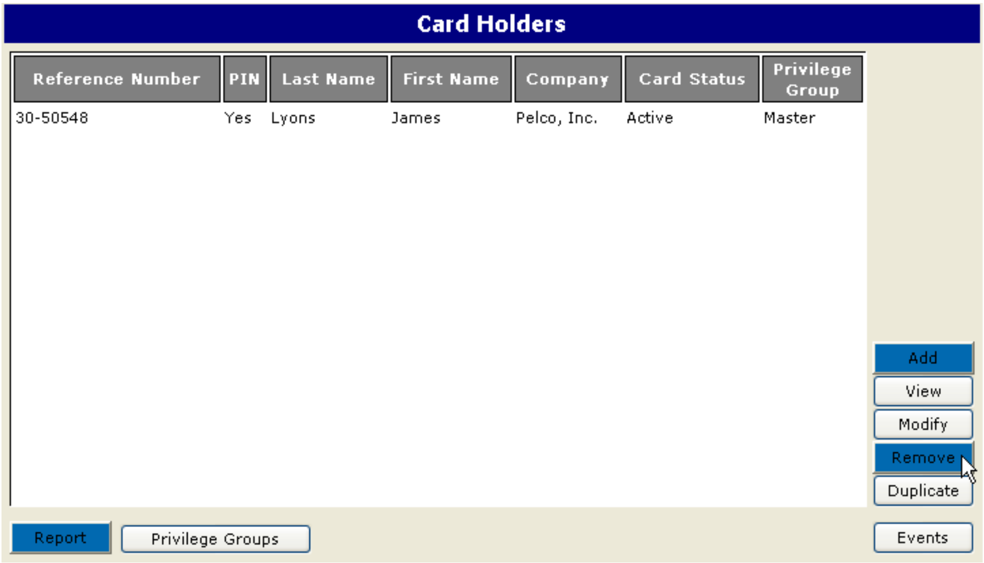
Priviledges

Privilege Group: Master Privilege Group

8. Select a **Privilege Group**. In the drop-down **Privilege Group** list, you can select a previously created privilege groups or **Master Privilege Group**. If a previously created privilege group is selected, click on the “**Set Privileges**” button and assign access privileges in the same way the privilege group access is assigned. If **Master Privilege Group** is chosen, the card holder will have unrestricted access (when properly identified with their card and PIN) to all services in the system.

   Note: The **Master Privilege Group** should be granted only to those card holders with sufficient authority. If a previously created privilege group is selected, the card holder will have the same access assigned to that group. To view the access that will be granted for a particular privilege group, click the “**View Privileges**” button.

9. After all the card holder record information has been completed, click the “**OK**” button to return to the **Card Holders** screen.



Card Holders

Reference Number	PIN	Last Name	First Name	Company	Card Status	Privilege Group
30-50548	Yes	Lyons	James	Pelco, Inc.	Active	Master

Deleting Card Holder Records

NOTE: Before deleting a cardholder, make sure you have deactivated the cardholder first by editing the user, setting the deactivation date and making sure the deactivation date checkbox is checked.

To delete a card holder record on the **Card Holders** screen, click to highlight the record and then click the “**Remove**” button.

> **Note:** If a card holder record is deleted from the system, all information related to that card holder is deleted from the main and history databases.

For security reasons, the system automatically keeps track of removed card holders with previously assigned valid (non-zero) reference numbers. Up to a maximum of 10,000 cards with distinct reference numbers are tracked in order to be able to exclude those cards until they can be physically invalidated by re-writing. Provided that your system contains fewer than 10,000 active card holders, you can still create new card holders in one of the following ways:

- By reassigning a previously used reference number. You must have recovered the card with that number, and it must be in good condition, so that you can attribute it to someone else's use.

Chapter 8: Monitoring The System

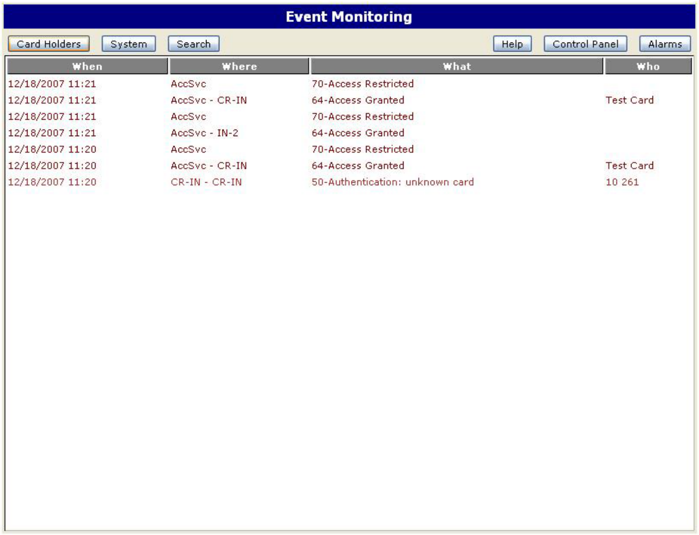
Contents

This Chapter discusses how to monitor the system by way of the Intelli-M® Web Interface. An operator can monitor the system for events such as access being granted or restricted at the door. Also discussed is how to view an alarm that may be trigger within the system, and appropriate responses to alarm types. Monitoring also includes using the control panel to override the services, inputs, and outputs that have been programmed into the system, and how to check the status of devices that make up the network.

The following topics can be found within this Chapter:

Event Monitoring

The first window that appears after logging into the system is the **Event Monitoring** screen, which is initially set up to display all events that occur in the Intelli-M Web Interface.



When	Where	What	Who
12/18/2007 11:21	AccSvc	70-Access Restricted	
12/18/2007 11:21	AccSvc - CR-IN	64-Access Granted	Test Card
12/18/2007 11:21	AccSvc	70-Access Restricted	
12/18/2007 11:21	AccSvc - IN-2	64-Access Granted	
12/18/2007 11:20	AccSvc	70-Access Restricted	
12/18/2007 11:20	AccSvc - CR-IN	64-Access Granted	Test Card
12/18/2007 11:20	CR-IN - CR-IN	50-Authentication: unknown card	10 261

Events are color-coded so that you can quickly identify what type of event has occurred, as shown in the following list:

Maroon Events -- signifying success (usually on unattended operations):

- Controller tamper restored
- Access granted/restricted
- Alarm service armed/disarmed

Black -- status change from controller:

- Input bypassed/un-bypassed
- Output overridden/override reversed
- Input/output trouble

Brown -- events requiring special attention or reflecting failed operation:

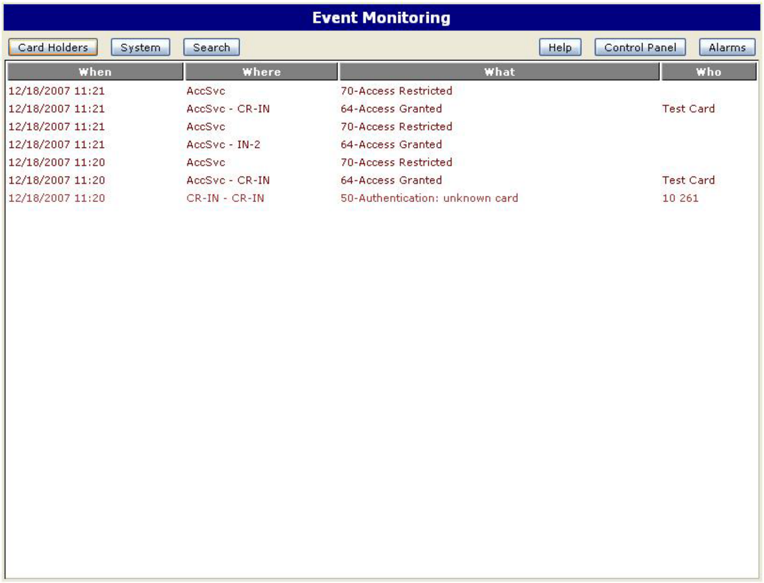
- Card update failed
- Card holder authentication failure (such as wrong PIN or invalid card)
- Access denied
- Anti-passback violation
- Card holder authentication failure

Red -- alarms

- Local alarm
- Door open too long alarm
- Card holder authentication failure

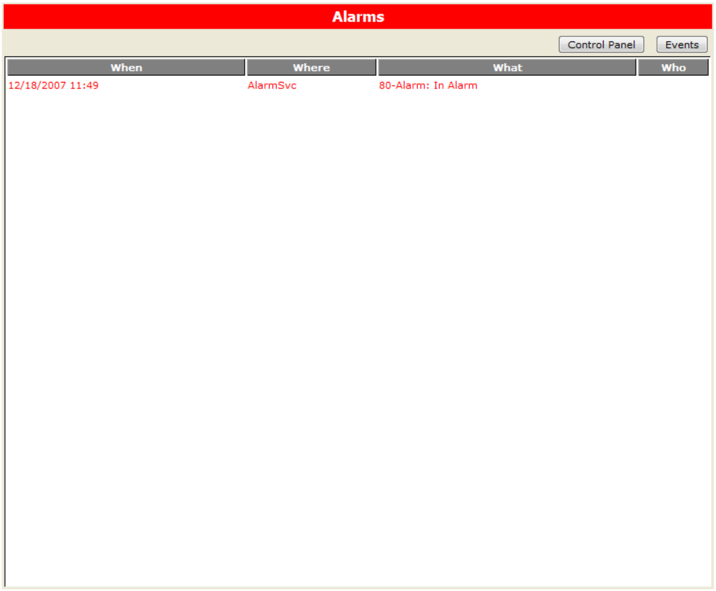
Viewing and Responding to Alarms

Alarm events that occur in the system must be handled cautiously to ensure a quick and appropriate response from surveillance personnel. Every alarm event appears simultaneously on the **Event Monitoring** and **Alarms** screens. The **Event Monitoring** screen provides a view of events (including alarms) in chronological order. The Intelli-M Web Interface can detect when the condition that caused the alarm returns to normal. When the condition returns to normal, the alarm is automatically restored. An alarm is considered resolved when it is restored.



When	Where	What	Who
12/18/2007 11:21	AccSvc	70-Access Restricted	
12/18/2007 11:21	AccSvc - CR-IN	64-Access Granted	Test Card
12/18/2007 11:21	AccSvc	70-Access Restricted	
12/18/2007 11:21	AccSvc - IN-2	64-Access Granted	
12/18/2007 11:20	AccSvc	70-Access Restricted	
12/18/2007 11:20	AccSvc - CR-IN	64-Access Granted	Test Card
12/18/2007 11:20	CR-IN - CR-IN	50-Authentication: unknown card	10 261

The **Alarms** screen restricts its content exclusively to alarm events. Also, an alarm event on the **Alarms** screen only stays displayed until the alarm is resolved; once resolved the screen automatically clears. To view the **Alarms** screen, click “**Alarms**” on the **Event Monitoring** screen.



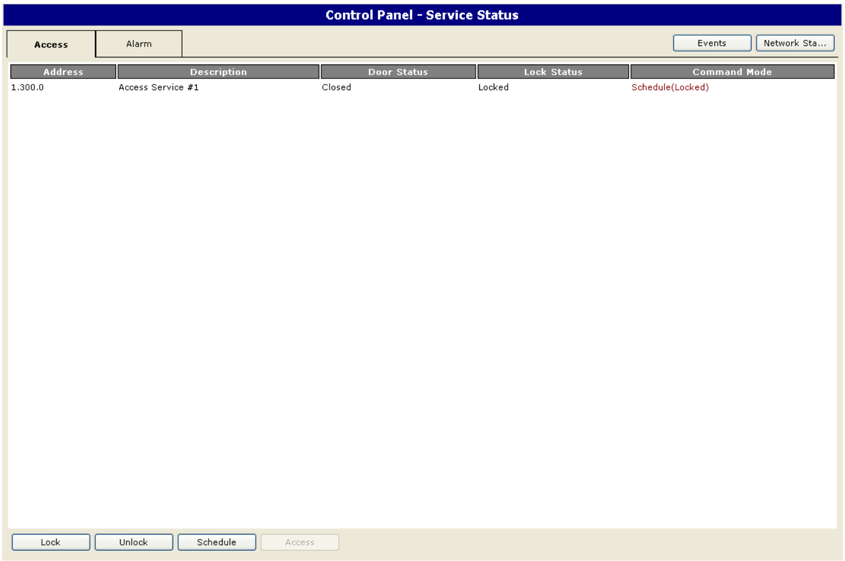
When	Where	What	Who
12/18/2007 11:49	AlarmSvc	80-Alarm: In Alarm	

Control Panel Service Status

The Control Panel screen allows you to monitor and manually override the services, inputs and outputs that have been programmed into the system. For example, suppose a warehouse door is scheduled to be locked—but after the lock time has occurred, a delivery person arrives. In this case, an operator can unlock the warehouse door right from the Intelli-M Web Interface. This can be done for the following services: access and alarm.

Service Status Access Tab

The **Access** tab allow you to quickly see if the controller is indicating the door as open or closed. The following information can be accessed: Address, Description, Door Status, Command Mode, Lock Status.



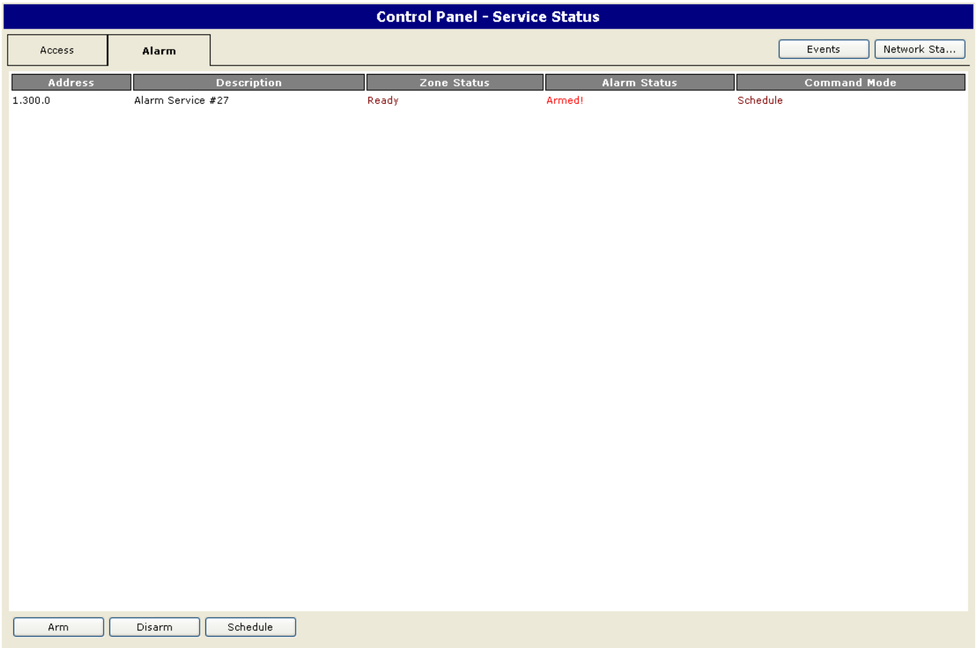
Address	Description	Door Status	Lock Status	Command Mode
1.300.0	Access Service #1	Closed	Locked	Schedule(Locked)

The information about each column is as follows:

- Address -- The identification address of the service point. The abbreviated device type (eIDC) is also displayed.
- Description -- The description of the access service.
- Door status -- The current door status reported by the service, either Open or Closed
- Command Mode -- The mode under which the service is working, either Locked or Unlocked.
- Lock -- The current lock status reported by the Controller for the access service, either Schedule or Manual. Schedule means the service is in its scheduled state (determined by its lock schedule). Manual means the service was put in its current state by way of a manual command issued from the Control Panel (i.e., the service was overridden). The three buttons on the lower right-hand side of the Control Panel are used for manual overrides:
    - Lock -- Manually lock the door controlled by the selected service. (Authorized accesses through normal trigger activation are still allowed.)
    - Unlock -- Manually unlock the door controlled by the selected service.
    - Schedule -- Revert the service to its scheduled state. This will reverse the effects of a manual Lock or Unlock command.

Service Status Alarm Tab

On the **ALARM** tab, services can be armed or disarmed. The following information can be accessed: Address, Description, Zone Status, Alarm Status, and Command Mode. To return alarms to their programmed state, highlight the service and click the “**Schedule**” button.



Address	Description	Zone Status	Alarm Status	Command Mode
1.300.0	Alarm Service #27	Ready	Armed!	Schedule

The information about each column is as follows:

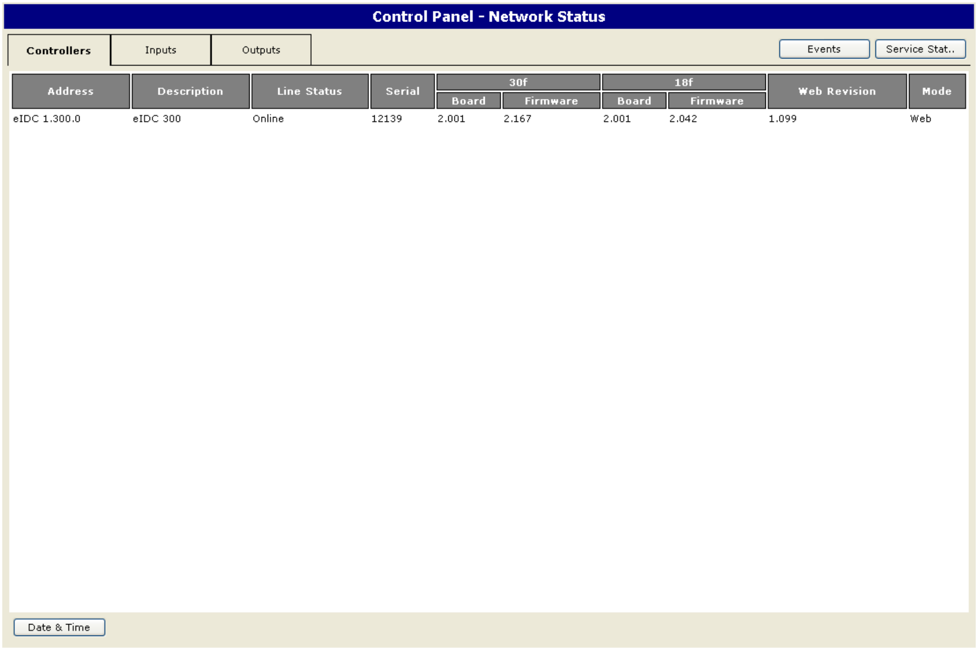
- Address -- The identification address of the service point. The abbreviated device type (eIDC) is also displayed.
- Description -- The description of the alarm service.
- Zone status -- The current zone status reported by the service (which is in fact equivalent to the status of the programmed alarm input) which will be either “Ready” (input normal) or “Not ready” (input abnormal).
- Alarm Status -- The current status (Armed or Disarmed) reported by the service.
- Command Mode -- The mode under which the service is currently working, either in a scheduled state or a manual state. The three buttons on the lower right-hand side of the Control Panel are used for manual overrides of the command mode:
  - Arm -- Manually arm the selected service.
  - Disarm -- Manually disarm the selected service.
  - Schedule -- Revert the service to its scheduled arming state. This will reverse the effects of a manual arm or disarm command.

Control Panel Network Status

The network status screens allow operators to check the status of Controllers, Inputs, and Outputs. The tabs (i.e., pages) within the network status correspond to physical network elements and their current status. This mode is particularly useful when used to diagnose installation or communication problems.

Network Status Controllers Tab

The **Controllers** tab is used to monitor the line status of the eIDC controller, and to display the serial number and firmware version of the eIDC controller.



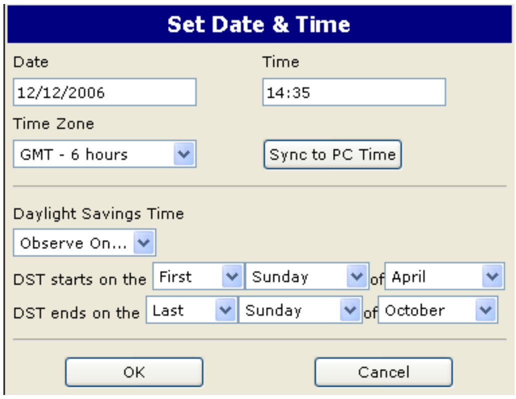
Address	Description	Line Status	Serial	30f		18f		Web Revision	Mode
				Board	Firmware	Board	Firmware		
eIDC 1.300.0	eIDC 300	Online	12139	2.001	2.167	2.001	2.042	1.099	Web

The information about each column is as follows:

- Address -- The identification of the controller. The abbreviated device type (eIDC) is also displayed.
- Description -- The description of the controller.
- Line status -- The current communication status with the controller, either Online or Offline.
- Serial -- The device serial number.
- Board -- The the device board(s) revision number.
- Firmware -- The firmware version number.
- Web Revision -- The version of Intelli-M Web Interface being used.
- Mode -- The mode under which the Intelli-M Web Interface is being used.

Date & Time

The “**Date & Time**” button allows you to update the eIDC controller with the date and time for its location once the “OK” button is clicked. When the “**Date & Time**” button is clicked, a dialog screen similar to that shown below is displayed:



Set Date & Time

Date: 12/12/2006

Time: 14:35

Time Zone: GMT - 6 hours

Daylight Savings Time: Observe On...

DST starts on the First Sunday of April

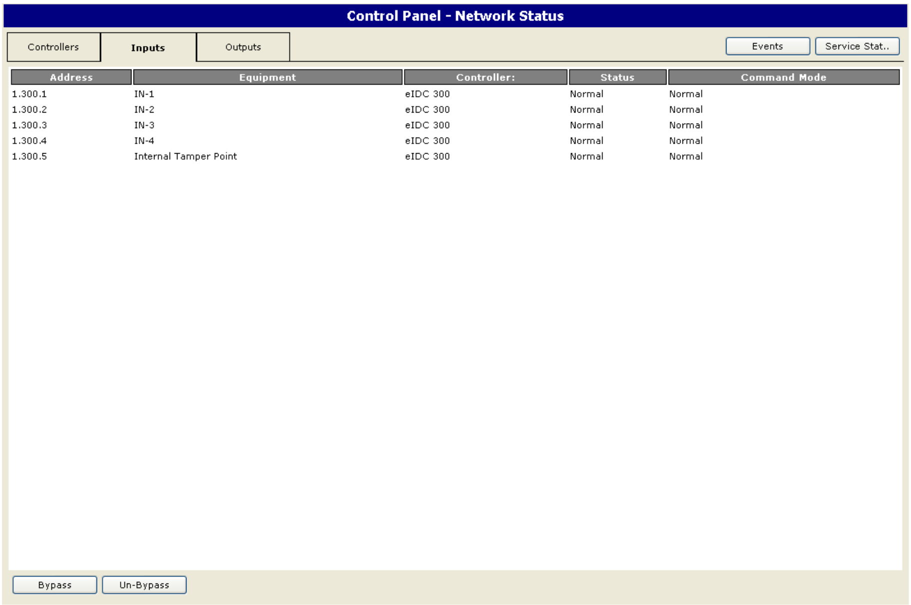
DST ends on the Last Sunday of October

The date and time initially displayed is read from the device. The date is in the format mm/dd/yyyy. The time is always expressed in 24-hour cycle (military) format, regardless of regional settings. The Date and the Time fields can be changed simply by typing over what is initially displayed. Pull downs are available for the Time Zone and Daylight Savings Time. The choices for Daylight Savings Time are: Ignore, Observe on..., and Always. If “Observe On...” is selected, then the “DST starts on the” and the “DST ends on the” fields become active. Once active, the start and end dates of DST can be selected. Once “OK” is clicked, the date and time information is downloaded to the controller.

> **Important:** “Sync to PC Time” will populate only the “Time” and “Time Zone” fields with the time and time zone of the connecting PC. The DST fields are not effected by the “Sync to PC Time” button.

Network Status Inputs Tab

The **Inputs** tab displays the real-time status of every input defined in the system, and to some extent enables you to see and manipulate their status in real-time. Inputs are configured in the Inputs screen (refer to “Chapter 5: Programming System Devices”), but their presence in the system depends on how the eIDC is configured.



Control Panel - Network Status

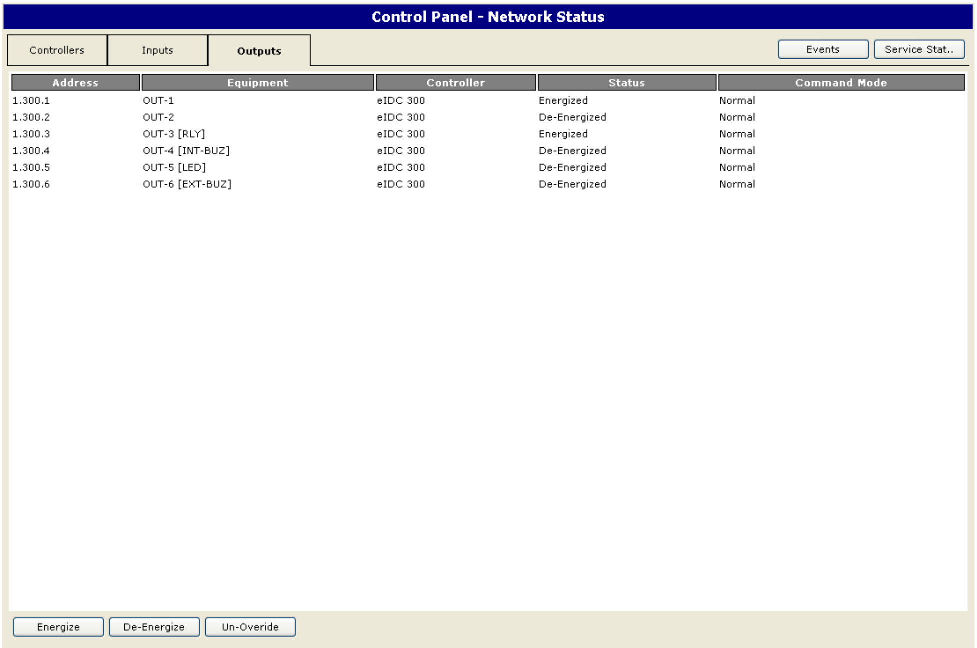
Address	Equipment	Controller:	Status	Command Mode
1.300.1	IN-1	eIDC 300	Normal	Normal
1.300.2	IN-2	eIDC 300	Normal	Normal
1.300.3	IN-3	eIDC 300	Normal	Normal
1.300.4	IN-4	eIDC 300	Normal	Normal
1.300.5	Internal Tamper Point	eIDC 300	Normal	Normal

The information about each column is as follows:

- Address -- The identification address of the input point. The abbreviated device type (eIDC) is also displayed.
- Equipment -- The abbreviation of the equipment connected to the input.
- Controllers -- The description of the controller where the input is located.
- Status -- The current state of the input, either Normal or Abnormal.
- Command Mode -- The mode under which the input is currently working, either in a Normal state or a Bypass state. The two buttons on the lower right-hand side of the Control Panel are used for manual overrides of the command mode:
  - Bypass -- Puts the selected input into a muted state. The input will no longer react to electrical transitions on the corresponding port.
  - Un-Bypass -- Removes a previous Bypass.

Network Status Outputs Tab

The **Outputs** tab displays the real-time status of every output defined in the system, and to some extent enables you to see and manipulate their status in real-time. Outputs are configured in the Outputs screen (refer to "Chapter 5: Programming System Devices"), but their presence in the system depends on how the eIDC is configured.



Address	Equipment	Controller	Status	Command Mode
1.300.1	OUT-1	eIDC 300	Energized	Normal
1.300.2	OUT-2	eIDC 300	De-Energized	Normal
1.300.3	OUT-3 [RLY]	eIDC 300	Energized	Normal
1.300.4	OUT-4 [INT-BUZ]	eIDC 300	De-Energized	Normal
1.300.5	OUT-5 [LED]	eIDC 300	De-Energized	Normal
1.300.6	OUT-6 [EXT-BUZ]	eIDC 300	De-Energized	Normal

The information about each column is as follows:

- Address -- The identification address of the output point. The abbreviated device type (eIDC) is also displayed.
- Equipment -- The abbreviation of the equipment connected to the output.
- Controllers -- The description of the controller where the output is located.

- Status -- The current state of the output, either Energized or De-Energized.
- Command Mode -- The mode under which the output is currently working, either in a Normal state or an Override state. The three buttons on the lower right-hand side of the Control Panel are used for manual overrides of the status condition:
  - Energized -- This will force the selected output into an Energized state. For example, a buzzer normally de-energized (no buzz sound) would become energized (and start buzzing). The output will no longer react to electrical transitions on the corresponding port, which means that the buzzing would continue until either the de-energized or un-override button is clicked.
  - De-Energized -- This will force the selected output into an De-Energized state. That is, an output that is energized would be placed into a de-energized state.
  - Un-Override -- This button cancels the effect of a previous override (Energized or De-Energized) command.

Chapter 9: History Searches And Reports

Contents

A history of every event that occurs in the system is stored by the Intelli-M® Web Interface. This Chapter discusses how to perform a search of all the stored events for a specific event or events. A history search covers the question of when, where, who, or what in regards to the security system that has been set up. A report can then be generated of the information found by the search.

The following topics can be found within this Chapter:

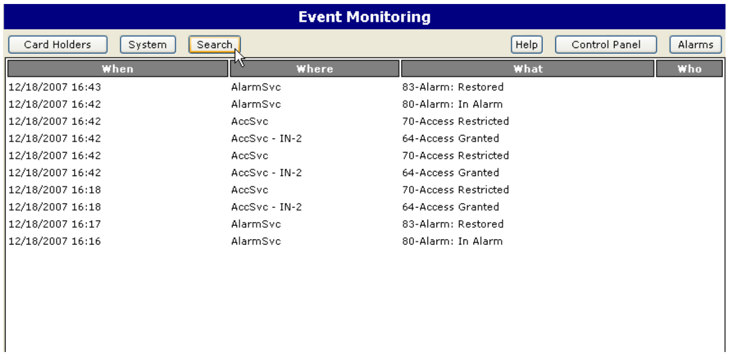
- History Search And Report Generating
- Card Holder Report

History Search and Report Generating

The Intelli-M Web Interface stores history for every event that occurs in the system, and a search can be performed for specific events within this history. The outcome of the search can then be printed as a report. To search the history log, at least one of the following four event information fields must be completed: **When**, **Where**, **Who** and **What**. The search results are displayed on the **History** screen in the same format as **Event Monitoring** screen.

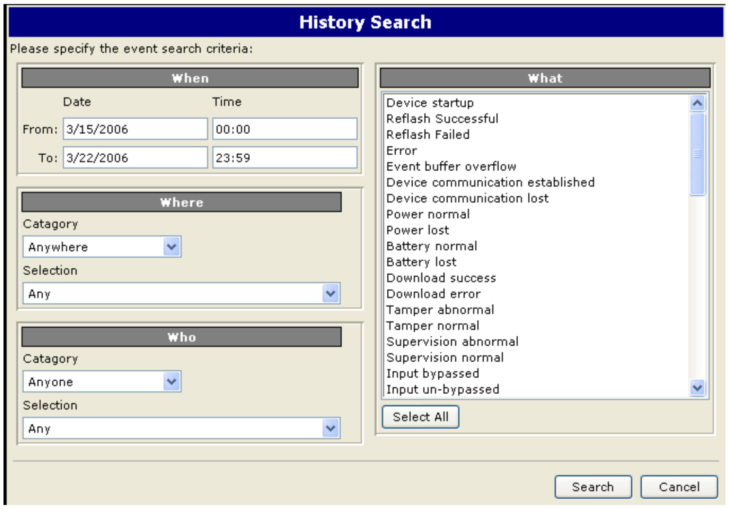
To perform a history search, do the following:

1. Click "**Search"** on the **Event Monitoring** screen.



When	Where	What	Who
12/18/2007 16:43	AlarmSvc	83-Alarm: Restored	
12/18/2007 16:42	AlarmSvc	80-Alarm: In Alarm	
12/18/2007 16:42	AccSvc	70-Access Restricted	
12/18/2007 16:42	AccSvc - IN-2	64-Access Granted	
12/18/2007 16:42	AccSvc	70-Access Restricted	
12/18/2007 16:42	AccSvc - IN-2	64-Access Granted	
12/18/2007 16:18	AccSvc	70-Access Restricted	
12/18/2007 16:18	AccSvc - IN-2	64-Access Granted	
12/18/2007 16:17	AlarmSvc	83-Alarm: Restored	
12/18/2007 16:16	AlarmSvc	80-Alarm: In Alarm	

The **History Search** screen will appear.



Please specify the event search criteria:

When

	Date	Time
From:	3/15/2006	00:00
To:	3/22/2006	23:59

Where

Catagory: Anywhere

Selection: Any

Who

Catagory: Anyone

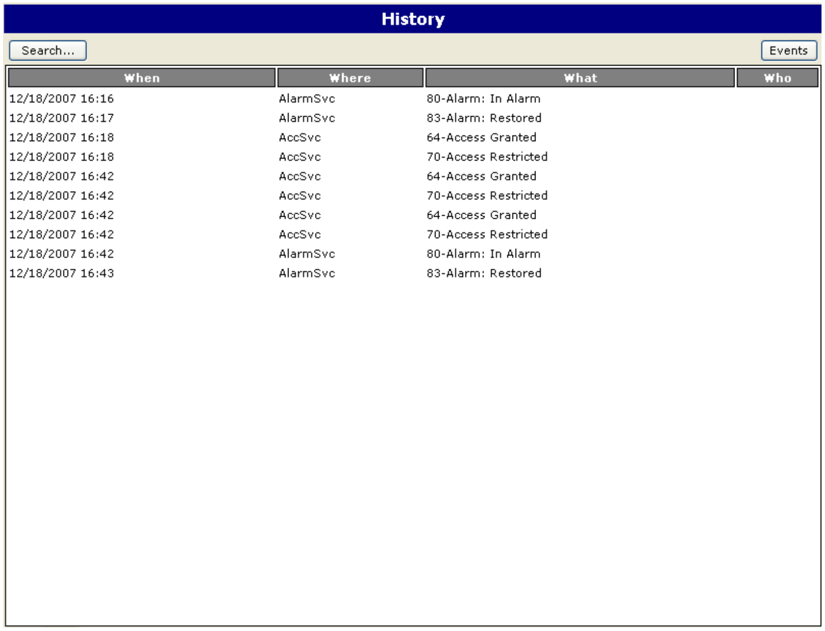
Selection: Any

What

Device startup
Reflash Successful
Reflash Failed
Error
Event buffer overflow
Device communication established
Device communication lost
Power normal
Power lost
Battery normal
Battery lost
Download success
Download error
Tamper abnormal
Tamper normal
Supervision abnormal
Supervision normal
Input bypassed
Input un-bypassed

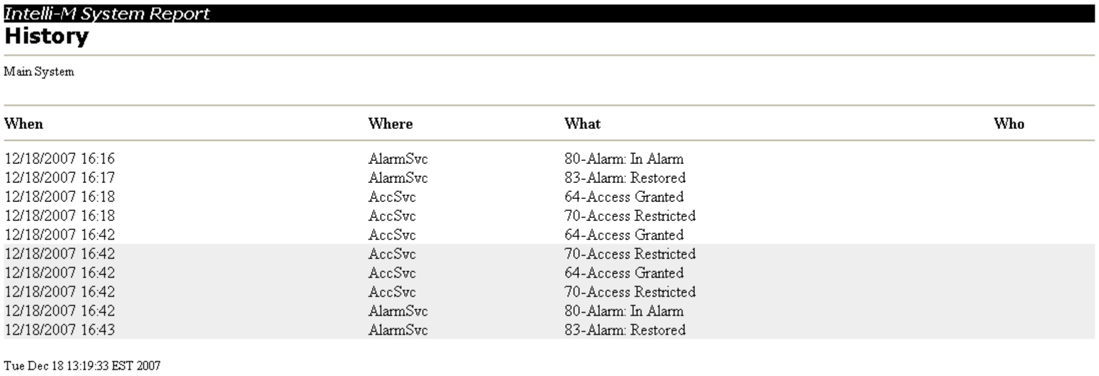
2. Establish the **When** search parameters for the report by entering the beginning date and time in the "**From**" field and the ending date and time in the "**To**" field.
3. For the **Where** parameters, select a "**Category**" and "**Selection**" from the drop-down lists. What is shown in the "**Selection**" drop-down list is dependent on what is chosen for "**Category**." For instance, if "Reader" is selected in "**Category**," then you "**Selection**" choices will be "Any," "CR-IN," or "CR-OUT."
4. For the **Who** parameters, select a "**Category**" and "**Selection**" from the drop-down lists. The "**Category**" drop-down choices will always be "Anyone," "Cardholder," or "Company." The "**Selection**" drop-down choices will always be "Any."

5. In the **What** area, select the types of history events that should appear in the report. Multiple history events can be selected at the same time by using one of the following methods:
   - To select a group of events that are listed together: click on the first event you want to select, hold the <Shift> key on your keyboard, and then select the last event. All the events between are selected.
   - To select multiple events that are not listed together: click on the first event, hold the <Ctrl> key on your keyboard, and then select all the desired events. Release the <Ctrl> key when finished.
   - To select all events in the list, click the "**Select All**" button.
6. When the report criteria is complete, click the "**Search**" button. The **History** screen will be displayed.



When	Where	What	Who
12/18/2007 16:16	AlarmSvc	80-Alarm: In Alarm	
12/18/2007 16:17	AlarmSvc	83-Alarm: Restored	
12/18/2007 16:18	AccSvc	64-Access Granted	
12/18/2007 16:18	AccSvc	70-Access Restricted	
12/18/2007 16:42	AccSvc	64-Access Granted	
12/18/2007 16:42	AccSvc	70-Access Restricted	
12/18/2007 16:42	AccSvc	64-Access Granted	
12/18/2007 16:42	AccSvc	70-Access Restricted	
12/18/2007 16:42	AlarmSvc	80-Alarm: In Alarm	
12/18/2007 16:43	AlarmSvc	83-Alarm: Restored	

7. The report listing is displayed on the **History** screen. To redefine the search, click the "**Search**" button and change the parameters within the **History Search** screen.
8. To generate a report, click the "**Report**" button.



Intelli-M System Report

History

Main System

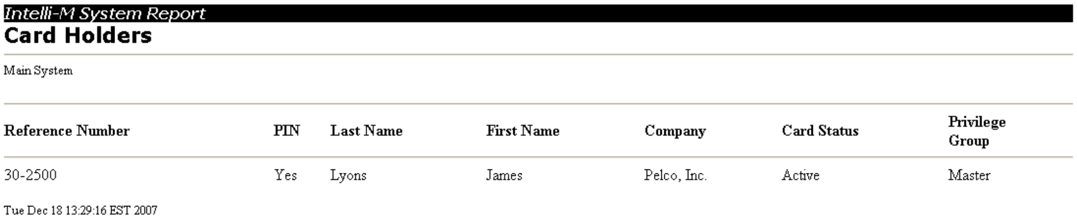
When	Where	What	Who
12/18/2007 16:16	AlarmSvc	80-Alarm: In Alarm	
12/18/2007 16:17	AlarmSvc	83-Alarm: Restored	
12/18/2007 16:18	AccSvc	64-Access Granted	
12/18/2007 16:18	AccSvc	70-Access Restricted	
12/18/2007 16:42	AccSvc	64-Access Granted	
12/18/2007 16:42	AccSvc	70-Access Restricted	
12/18/2007 16:42	AccSvc	64-Access Granted	
12/18/2007 16:42	AccSvc	70-Access Restricted	
12/18/2007 16:42	AlarmSvc	80-Alarm: In Alarm	
12/18/2007 16:43	AlarmSvc	83-Alarm: Restored	

Tue Dec 18 13:19:33 EST 2007

Card Holder Report

A list of all the card holders can be generated by doing the following:

1. Click on “**Card Holders**” on the **Event Monitoring** screen.
2. Click the “**Report**” button on the **Card Holders** screen. A report listing of all the card holders will be generated.



Intelli-M System Report

Card Holders

Main System

Reference Number	PIN	Last Name	First Name	Company	Card Status	Privilege Group
30-2500	Yes	Lyons	James	Pelco, Inc.	Active	Master

Tue Dec 18 13:29:16 EST 2007

Appendix A: eFamily Update Utility (Backup, Upgrade, And Restore eFamily Device Software)

Contents

The eFamily Update Utility provides the ability to update the firmware, backup the device configuration (including card holders, schedules, and services) and event history log, and/or restore a backup configuration to an eFamily device.

The following topics can be found within this Appendix:

Installing The eFamily Update Utility

Installation of the eFamily Update Utility is dependent on Intelli-M® Supervisor Plus or the Intelli-M® Web Interface.

Supervisor Plus Users

The eFamily Update Utility can be found on the Intelli-M Supervisor Plus installation CD. Once the CD is placed into the CD-ROM drive, right-click on the CD-ROM drive icon within “My Computer” and select “Open.” Navigate to the eFamily Update Utility folder, and then follow the installation procedure steps below.

Web Interface Users

The eFamily Update Utility file can be downloaded from the infinias Web site at: www.infinias.com.

Installation Procedure

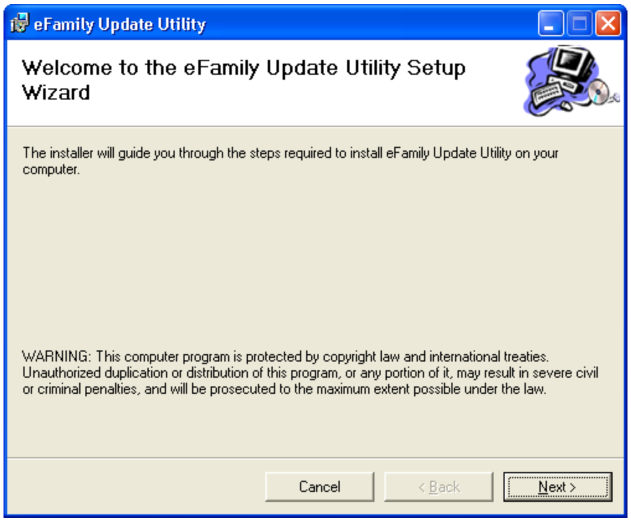
The procedure for installing the eFamily Update Utility is as follows:

1. **If the file was downloaded from the Web site, unzip the downloaded file.**

   Important: Make a note of where you unzip the file contents, as you will need the unzipped files during the update procedure.

2. **Launch (double click) the “setup.exe” file.**

   The welcome screen for the install wizard screen similar to that shown in Figure A-1 will be displayed.


eFamily Update Utility

Welcome to the eFamily Update Utility Setup Wizard

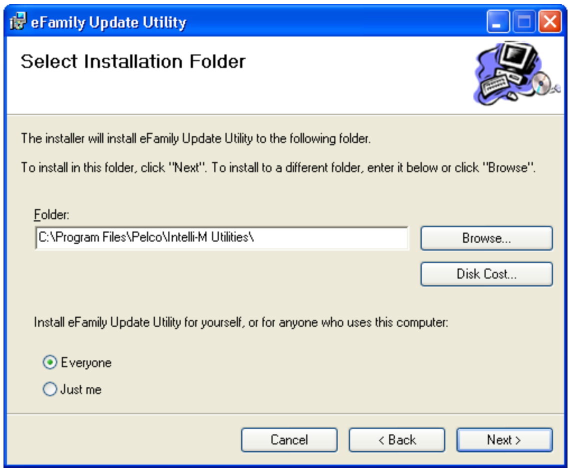
The installer will guide you through the steps required to install eFamily Update Utility on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure A-1: Setup Welcome Screen

3. **Click the “Next” button.**

   The installer select installation folder screen similar to that shown in Figure A-2 will be displayed.



Select Installation Folder

The installer will install eFamily Update Utility to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Pelco\Intelli-M Utilities\

Install eFamily Update Utility for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

Figure A-2: Select Installation Folder Screen

Be sure to indicate if the utility will be used by only you, or if it will be used by anyone who has access to the computer.

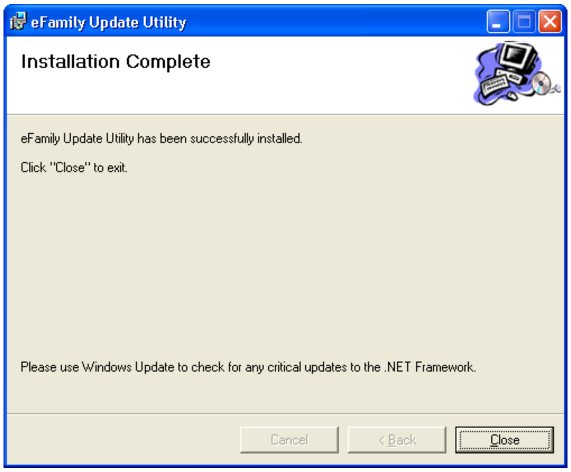
The "Disk Cost" button can be used to determine how much room is on each of the computer's drives, and how much disk space (cost) will be used after the program is installed.

The "Browse" button can be used to install the utility at some location on the computer other than the default location.

4. **Click the "Next" button so that the "Confirm Installation" screen is displayed.**

   This will prepare the installer to install the eFamily Update Utility onto the computer.

5. **Click the "Next" button. A screen displaying the progress of the installation process will be displayed. Then, an "Installation Compete" screen similar to that shown in Figure A-3 will be displayed.**



Installation Complete

eFamily Update Utility has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Figure A-3: Installation Complete Screen

6. **Click the "Close" button.**

   This completes installation of the "eFamily Update Utility".

Before Updating Your eFamily Device

To update an eFamily device, you must first gather the following information for the procedure:

- IP Address of the device you want to update
- Port number configured for communication
- FTP Username and Password for that device
  (The default Username and Password is the word “admin” without the quotes.)
- Location of the update file

If you are unsure of the IP address for the eFamily device you plan to update, power cycle the device. As the device boots, the IP address will be signalled by the LEDs. Refer to the “Determining The eIDC IP Address” section within Chapter 1 of this manual for details on reading the IP address from an eFamily device.

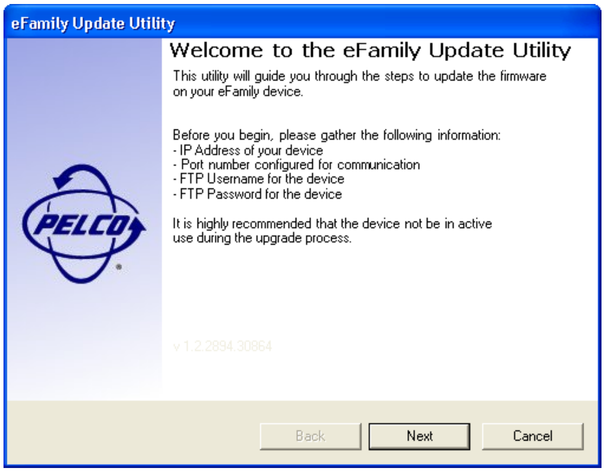
eFamily Update Procedure

Perform the following steps to update an eFamily device:

1. **Launch the eFamily Update Utility** (Start >> All Programs >.> infinias >> Intelli-M Utilities >> eFamily Update Utility).

   The following screen will be displayed.

   Note: If your computer needs to be updated to .NET Framework 2.0, then installation screens for NET Framework will be displayed before the screen shown in Figure A-4 is displayed.



Welcome to the eFamily Update Utility

This utility will guide you through the steps to update the firmware on your eFamily device.

Before you begin, please gather the following information:
- IP Address of your device
- Port number configured for communication
- FTP Username for the device
- FTP Password for the device

It is highly recommended that the device not be in active use during the upgrade process.

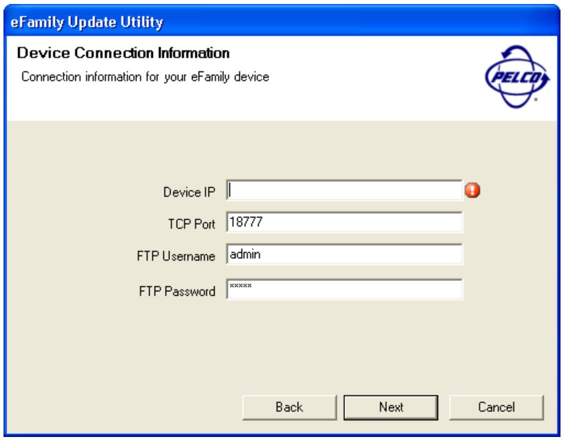
v 1.2.2894.30864

Figure A-4: eFamily Update Utility Screen

   Click the “Next” button.

2. **Type in the connection information used by the eFamily device to be updated.**

   A screen similar to that shown in Figure A-5 will be displayed requesting the path to the upgrade file. Type in the IP address. The TCP port number, FTP user name, and FTP password are system defaults. If you are unsure of the port number, user name, or password for your system, then use the default information provided. In most instances, the default information will be correct. If you know that your TCP port number and/or name and password are different, then type in the correct information for your system.



eFamily Update Utility

Device Connection Information

Connection information for your eFamily device

Device IP:

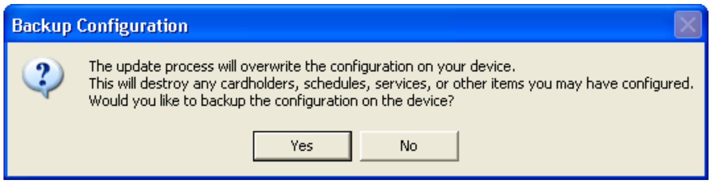
TCP Port: 18777

FTP Username: admin

FTP Password: *****

Figure A-5: Connection Information Screen

Click the "Next" button which will display the "Backup File" screen. Since updating an eFamily device erases any configuration data coded into it, a dialog is displayed that gives the opportunity to back up the device. Refer to Figure A-6.



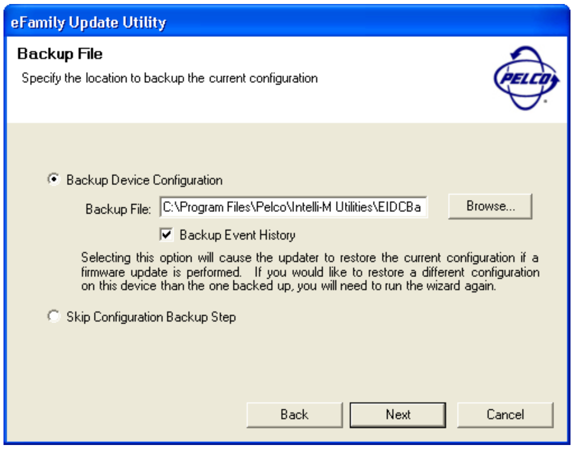
Backup Configuration

The update process will overwrite the configuration on your device.
This will destroy any cardholders, schedules, services, or other items you may have configured.
Would you like to backup the configuration on the device?

Figure A-6: Choice To Backup Screen

If "Yes" is selected, "Backup Device Configuration" is enabled on the Backup File screen. Refer to Figure A-7. An additional option is also given to backup up the Event Log on the eFamily device.

If "No" is selected, a verify skip backup dialog is displayed, then "Skip Configuration Backup Step" is enabled.



eFamily Update Utility

Backup File

Specify the location to backup the current configuration

● Backup Device Configuration

Backup File: C:\Program Files\Pelco\Intelli-M Utilities\EIDCBa

☑ Backup Event History

Selecting this option will cause the updater to restore the current configuration if a firmware update is performed. If you would like to restore a different configuration on this device than the one backed up, you will need to run the wizard again.

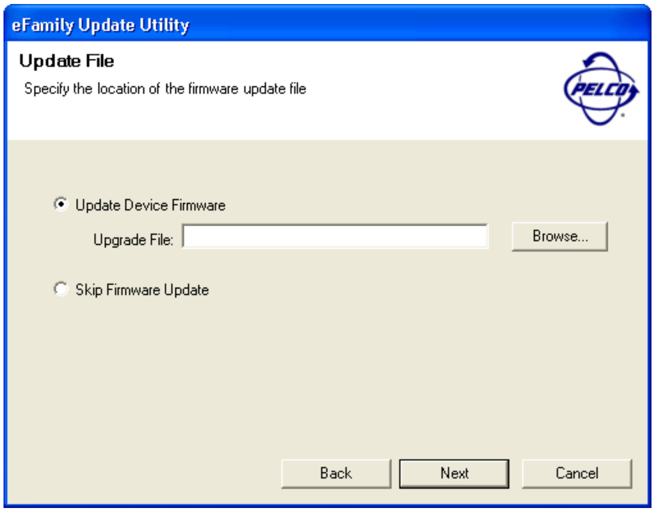
○ Skip Configuration Backup Step

Figure A-7: Connection Information Screen

The “Browse” button can be used to change the default name of the backup file (which is the year, month, and date per the computer’s clock in yyyymmdd format), and can also be used to change the default location (eFamily Update folder) to which the device’s current configuration is saved.

Click the “Next” button which will display the “Update File” screen.

3. **The eFamily Update Utility file will have an .iti or .xml extension. Use the “Browse...” button to navigate to the file and open it. Refer to Figures A-8 and A-9.**



eFamily Update Utility

Update File

Specify the location of the firmware update file

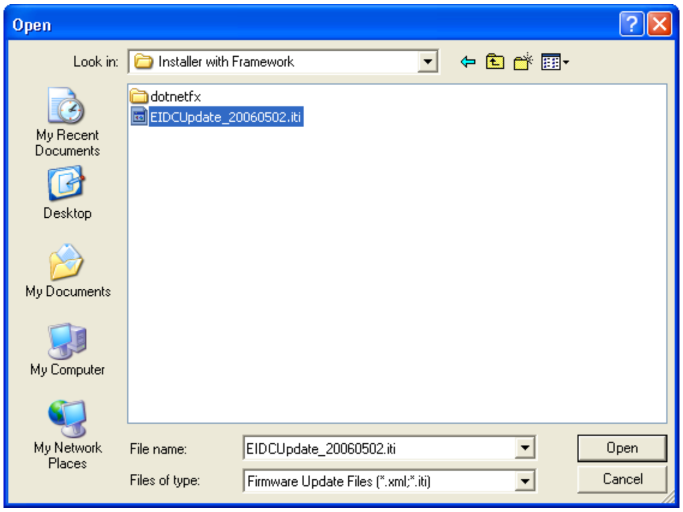
● Update Device Firmware

Upgrade File:

○ Skip Firmware Update

Figure A-8: Example Use Of Path To Upgrade File Screen

If “Skip Firmware Update” is enabled (checked), go to Step 4.



Open

Look in: Installer with Framework

dotnetfx

EIDCUpdate_20060502.iti

File name: EIDCUpdate_20060502.iti

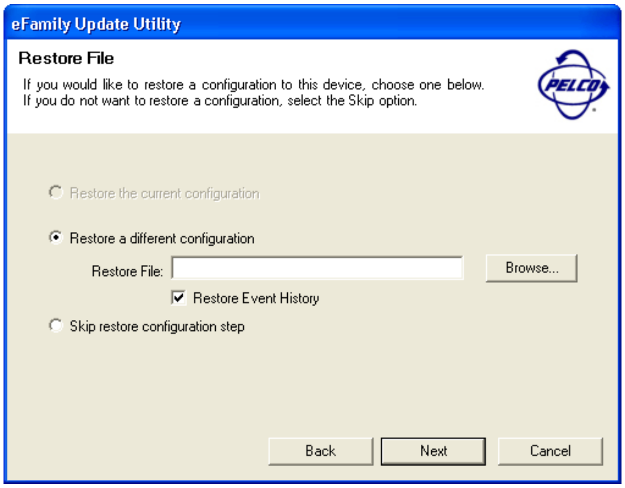
Files of type: Firmware Update Files (*.xml;*.iti)

Figure A-9: Example Of Browse Button Being Used Screen

If “Skip Firmware Update” is disabled (unchecked), click the “Next” button and go to Step 5.

4. **The "Restore File" screen is used to load a configuration onto the device that is different from the one currently on the device. (An example of this would be a previously backed up configuration.) Refer to Figure A-10. Use the "Browse..." button to navigate to the file, and then click the "Next" button.**

   Note: The backed up eFamily configuration file must have an .iti or .xml extension.



Restore File

If you would like to restore a configuration to this device, choose one below.
If you do not want to restore a configuration, select the Skip option.

○ Restore the current configuration

● Restore a different configuration

Restore File:

☑ Restore Event History

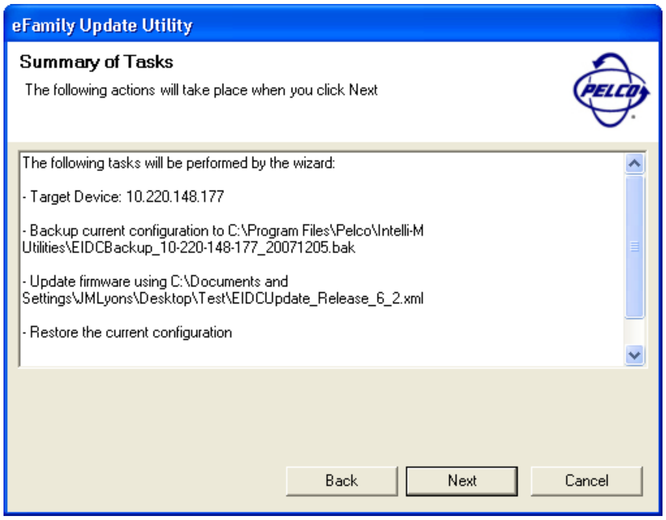
○ Skip restore configuration step

Figure A-10: Example Of Browse Button Being Used Screen

An additional option is also given to restore the Event History on the previously backed up file to the eFamily device.

5. **The "Summary of Tasks" screen will be displayed. Check the summary of tasks the update utility will perform.**

A screen similar to that shown in Figure A-11 will be displayed listing the tasks that will be performed by the utility. Check the list to make sure the tasks listed are the ones desired. The "Back" button can be used to make changes to the tasks that are to be done.



Summary of Tasks

The following actions will take place when you click Next

The following tasks will be performed by the wizard:

- Target Device: 10.220.148.177

- Backup current configuration to C:\Program Files\Pelco\Intelli-M Utilities\EIDCBackup_10-220-148-177_20071205.bak

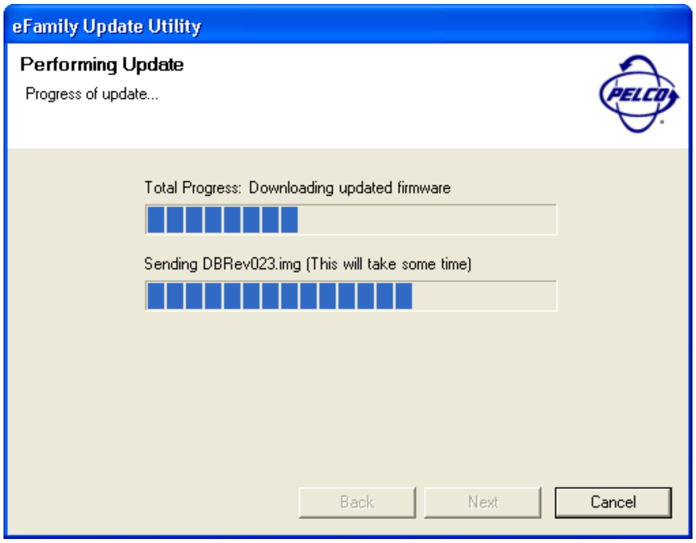
- Update firmware using C:\Documents and Settings\JMLyons\Desktop\Test\EIDCUpdate_Release_6_2.xml

- Restore the current configuration

Figure A-11: Connection Information Request Screen

6. Click the “Next” button to upgrade data to the eFamily device.

As the update proceeds, the screen will provide details about the update process. Refer to Figure A-12.



eFamily Update Utility

Performing Update

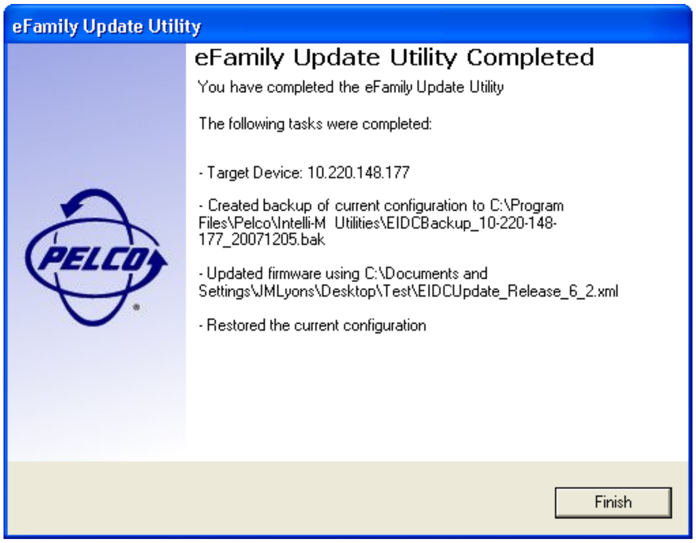
Progress of update...

Total Progress: Downloading updated firmware

Sending DBRev023.img (This will take some time)

Figure A-12: Update In Process Screen

Once the update is complete, a screen similar to that shown in Figure A-13 will be displayed indicating that the update is complete.



eFamily Update Utility

eFamily Update Utility Completed

You have completed the eFamily Update Utility

The following tasks were completed:

- Target Device: 10.220.148.177

- Created backup of current configuration to C:\Program Files\Pelco\Intelli-M Utilities\EIDCBackup_10-220-148-177_20071205.bak

- Updated firmware using C:\Documents and Settings\JMLyons\Desktop\Test\EIDCUpdate_Release_6_2.xml

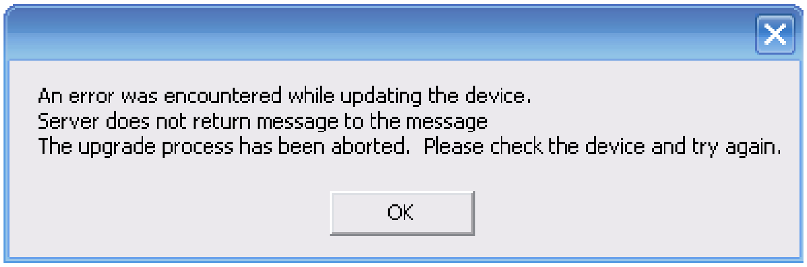
- Restored the current configuration

Figure A-13: Update Complete Screen

Click the “Finish” button to close the utility, or click the back button to update a different eFamily device.

Errors That Occur During Update

If any problems occur during the update process, an error message similar to that shown in Figure A-14 with details about the problem will be displayed.



An error was encountered while updating the device.
Server does not return message to the message
The upgrade process has been aborted. Please check the device and try again.

Figure A-14: Example Error Message

Dismiss the message by clicking the "OK" button. Verify that the device is online and operating properly. Use the "Back" button to verify the information specified on each screen, and then attempt the update again.

> **Important:** It is very important that neither the Supervisor Plus software nor the Web Interface is actively monitoring the device during the update process. These processes will interfere with the ability of the eFamily Update Utility to configure your device. It is highly recommended that the device be removed from normal operation and isolated on the network prior to updating the firmware.