interlogix

United Technologies

TruPortal™

SOFTWARE USER GUIDE

Interlogix® TruPortal™ Software User Guide, product version 1.6. This guide is item number 461043001B, dated October 31, 2014.

Trademarks and patents   Interlogix, TruPortal, TruVision, and logos are trademarks of United Technologies. Microsoft, Internet Explorer, and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. Apple, iPad, iPhone, and iTunes are registered trademarks of Apple Inc. Android is a trademark of Google, Inc. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer   Interlogix
3211 Progress Drive, Lincolnton, NC 28092

Authorized EU manufacturing representative:
UTC Building & Industrial Systems B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Version   This document applies to TruPortal version 1.6.

Certification $C \in \mathcal{C}$ N4131

FCC compliance   This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Class A: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Class B: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

There is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

ACMA compliance

Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Canada

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-0330 du Canada.

European Union directives

1**2004/108/EC (EMC directive):** Hereby, United Technologies declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.

2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Contact information

www.interlogix.com

Customer support

www.interlogix.com/support

GNU Public Licenses

Linux Kernel 2.6.30, Pthreads, Larry DooLittle, Flex Builder, and Buildroot are licensed under the GNU General Public License, version 2. A copy of the license can be retrieved at http://www.gnu.org/licenses/gpl-2.0.html.

YAFFS2 and GNU tar are licensed under the GNU General Public License, version 3. A copy of the license can be retrieved at http://www.gnu.org/licenses/gpl-3.0.html.

uClibc, iClibc locale, GPG Gnu Privacy Guard, gpgme GnuPG Made Easy are licensed under the GNU Lesser General Public License, version 3. A copy of the license can be retrieved at http://www.gnu.org/licenses/lgpl-3.0.html.

OpenSSL, AstraFlex Components and LIGHTTPD are licensed under a Modified BSD License

Copyright © 1998—2011 The OpenSSL Project. All rights reserved.

Copyright © 2008, Yahoo! Inc. All rights reserved.

Copyright © 2004, Jan Kneschke, incremental. All rights reserved.

CMockery and Google Protocol Buffers (C) are licensed under the Apache License, Version 2.0 (the "License")

Flex-IFrame

Google Protocol Buffers (C++) is licensed under the New BSD License.

gSOAP is licensed under the gSOAP Public License (modified MPL license)

mini_httpd is licensed under the Acme Labs Freeware License.

Apache log4Net is licensed under the Apache License version 2.0.

Table of Contents

CHAPTER 1   *Introduction*

TruPortal™ is a web-based access control solution that is designed to be simple to use, yet sophisticated. It is compatible with a variety of access control hardware components, including:

- Input devices that detect conditions or events, such as door bells or alarms.
- Output devices such as lights and locks that respond to input devices and/or action triggers.
- TruVision™ Digital Video Recorders (DVRs) and Network Video Recorders (NVRs).

The TruPortal User Interface software is embedded on the System Controller and can be used to:

- Control access for up to 64 doors based on user-defined schedules.
- Configure schedules to include recurring holidays.
- Add up to 10,000 users and badges to the System.
- Add reader schedules to help automate the System.
- Enforce Anti-passback (APB).
- Create reader groups.
- Monitor events remotely and automate linking of events to recorded video.
- Open, lock, lock out and reinstate doors remotely.

Note: For an Underwriters Laboratories of Canada (ULC) s319-listed installation and/or UL 294 installation, remote access features are supplementary.

Mobile versions of the User Interface are also available for iOS6 and Android™ devices. These companion apps can be used to remotely monitor system activity and perform basic administration. Refer to the *TruPortal Release Notes* for details.

In addition to the User Interface software, the System includes the following programs:

- The **Installation Wizard** can be used to detect the System Controller on a network, synchronize the time on the System Controller with the time on the local client workstation, and configure network settings. The Installation Wizard can also be used to determine the new IP address of an System Controller if the IP address has changed. See Using the Installation Wizard on page 9.
- The **Upgrade Wizard** can be used to upgrade the System Controller from an earlier version. *Existing TruPortal 1.0 and goEntry 3.0 customers should use the Upgrade Wizard instead of the Installation Wizard to upgrade the System Controller.* See Using the Upgrade Wizard on page 11.

- The **Import/Export Wizard** can be used to import persons and credentials data from an existing database in Comma Separated Values (CSV) format, as well as export data. It can also be used to delete persons and credential data in batch mode and export events. See the *Import/Export Wizard User Guide* included on the Utilities disc for details.

Conventions Used in this Documentation

TruPortal documentation is included on the product disc and the text in each document is formatted to make it easy to identify what is being described.

- Where a term is defined, the word is represented in *italics*.
- Field names are shown in **bold**.
- Menus and menu choices are shown in ***bold italics***. All menu choices have accelerator keys, that can be used to select the menu choices using the keyboard. The underlined letter represents the accelerator key for that menu item. Accelerator keys are written, for example, <Alt>, <C>.
- Keyboard keys are represented in angle brackets. For example: <Tab>, <Ctrl>.
- Keyboard key combinations are written in two ways:
  - <Ctrl> + <Z> means hold down the first key and press the second
  - <Alt>, <C> means press the first key, then press the second
- Buttons on the screen are represented in square brackets; for example: [Modify], [Cancel].

Click the **View Help** button ( ) in the top-right corner of the TruPortal User Interface to access a searchable, electronic version of the *TruPortal Software User Guide* via the online help system.

Click the **Show Tool Tips** button ( ) to display context-sensitive information when hovering over fields and icons in the TruPortal User Interface. Tooltips can be toggled on and off by clicking the same button. Maximize the browser window to display all tool tips; tool tips may not appear if the browser window is too small.

Click the **Disable Wizards** button ( ) to turn off the ability to use wizards for configuration. Wizards can be toggled on and off by clicking the same button. This setting is saved for each user.

Installing Hardware

The first step in setting up the System is to install the hardware components that will be used by the System (inputs, outputs, doors, readers, cameras, etc.) according to manufacturer instructions. Be sure to record data about door configurations that can be used later in naming the devices, reader groups, and areas when the devices are configured in the User Interface.

Note: Existing TruPortal 1.0 or goEntry 3.0 customers that already have all hardware installed and configured can skip this step and use the **Upgrade Wizard** to upgrade the System Controller. See Using the Upgrade Wizard on page 11.

After installing hardware components, connect the System Controller to a local client workstation or to Local Area Network (LAN), and then use the Installation Wizard to detect the System Controller on the network, as described in Preparing for Configuration on page 7.

System Architecture Overview

The System Controller functions as the brain of the System that receive information and sends out information. It contains the database that stores all data for devices, schedules, persons, etc., as well as the User Interface software that can be accessed from a computer via a web browser.

Various components can be connected to the System Controller, including door controllers, readers, input/output expansion modules, siren relays, strobe relays, and strike relays. These components can be considered the arms of the System; they feed data into the System and also carry out actions requested by the System.

System architecture diagram
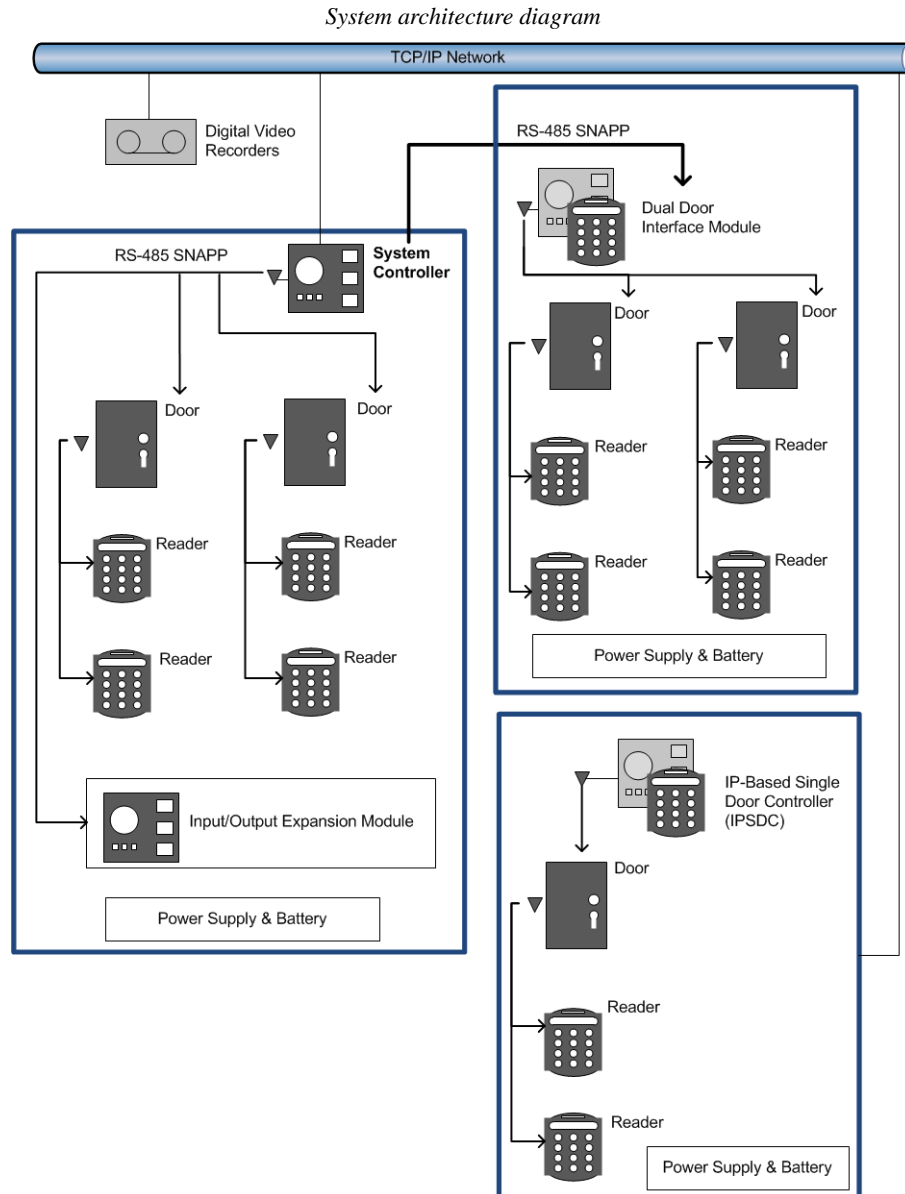
In addition to hard-wired components, the System Controller can communicate with proprietary Internet Protocol (IP)-based Single Door Controllers (IPSDCs). Plus, companion iPad®, iPhone®, and AndroidTM apps enable users to remotely monitor system activity and perform basic administrative tasks, such as adding or deleting users.

Documenting the Physical Location of Each Device

As each device for each door (locks, sensors, readers) is installed, provide a description for each device, and list the serial numbers of devices associated with each door in an installation chart like the one provided below. This data can be used later when devices are configured in the User Interface.

Door Description	Reader Serial Numbers	Door Controller Serial Numbers	I/O Expansion Serial Number	Linked Camera
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			

Door Description	Reader Serial Numbers	Door Controller Serial Numbers	I/O Expansion Serial Number	Linked Camera
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			

Connecting to a Local Client Workstation or LAN

The System Controller can be connected directly to a local client workstation or to a Local Area Network (LAN). There are two RJ-45 100BaseT Ethernet jacks on the System Controller. Port 1 is configurable; Port 2 has a fixed IP (Internet Protocol) address, 169.254.1.200. Refer to the System Controller Quick Reference Guide to identify the jacks.

If connecting the System Controller directly to a local client workstation, use the static Ethernet jack and a Category 6 (CAT6) Ethernet cable. If connecting to a LAN, use the configurable Ethernet jack and a CAT6 Ethernet cable. Consult the site network administrator to determine how the System Controller should be configured, as discussed in Determining Network Settings on page 8.

Note: If multiple network appliances use a single network drop by means of a switch or small router, make sure there is not more than one switch or router between the System Controller and the network drop.

Installing an Enrollment Reader

If planning to use the optional enrollment reader (TP-RDR-LRN) to read credential data, install and configure the reader on a client workstation according to the manufacturer's instructions. See Using an Enrollment Reader on page 68 for details.

CHAPTER 3

Preparing for Configuration

After hardware devices are installed, the following steps should be performed before launching the User Interface to perform a full configuration of the System:

1. Consult with the site network administrator to decide how network settings should be configured. See Determining Network Settings on page 8.

2. *If you are an existing TruPortal 1.0 or goEntry 3.0 customer and all hardware is already installed and configured*, use the Upgrade Wizard to upgrade the System Controller instead of using the Installation Wizard. See Using the Upgrade Wizard on page 11.

    If you are a new TruPortal user, follow the steps in Using the Installation Wizard on page 9 to:

    •   Detect the System Controller on the local area network.

    •   Change the default password for the main Administrator account to enhance security.

    •   Synchronize the date and time on the System Controller with the local client workstation.

    •   Configure the network settings of the System Controller.

3. Configure any installed IPSDCs to recognize the IP address of the System Controller *before* configuring the IPSDCs in the User Interface. Establishing this network connection ensures that IPSDCs will be detected when the System Controller scans for hardware changes. For more information, see Configuring IP-Based Single Door Controllers on page 106.

Determining Network Settings

Before using the Installation Wizard to perform an initial configuration of the System Controller, consult with the site network administrator to determine the answers to the following questions:

- **Should the IP address of the System Controller be static or dynamic?** Operators will access the User Interface by typing the System Controller's IP address into a web browser address field. If the IP address of the System Controller uses the Dynamic Host Configuration Protocol (DHCP), then operators must use a virtual URL or other alias to access the System Controller. If the actual IP address assignment is changed by the network, the operators will not be able to find it.

- **Should the Service Port be changed?** The default Service Port for an HTTPS connection is 443; the default value for an HTTP connection is 80. Typically, this port only needs to be changed if it conflicts with an existing port used on the network. If the port is changed, users will need to append the port number to the IP address of the System Controller to log into the System (e.g., https://IPaddress:*port*).

Note: Ports 0 through 1024 (i.e., *well-known ports*) are reserved for privileged services. It is recommended that these ports not be used as the service port.

- **If a static IP address will be used, what are the subnet mask, default gateway, and Domain Name Server (DNS) values for the network?** This information will be needed when configuring network properties for the System Controller.

- **Should a Hypertext Transfer Protocol Secure (HTTPS) connection be used?** HTTPS is highly recommended to prevent unauthorized access to the System. This secure protocol encrypts the packets between the client browser and the System Controller, preventing someone from gathering user information by spying on network traffic. There may be circumstances that require non-secure HTTP. For example, if the System Controller is accessed through a Web proxy server that does not support HTTPS, then the only option is to disable HTTPS.

  After installation, the System can also be configured to use a Secure Shell (SSH) connection that authenticates remote client workstations and allows remote users (including technical support representatives) to log into the System. Refer to Configuring Network Security on page 16.

Using the Installation Wizard

This section describes how to use the Installation Wizard to:

• Detect the System Controller on the local area network.

• Change the default password for the main Administrator account to enhance security.

• Synchronize the date and time on the System Controller with the local client workstation.

• Configure the network settings of the System Controller.

Note: If you are an existing TruPortal or goEntry user, run the **Upgrade Wizard** to upgrade the System Controller from an earlier version instead of using the Installation Wizard. See Using the Upgrade Wizard on page 11.

The Installation Wizard can also be used to determine the new IP address of an System Controller if the IP address has changed.

Note: The Installation Wizard is not compatible with Microsoft® Windows® XP.

To use the Installation Wizard:

1. Verify that the System Controller is connected to the local area network so that it can be detected by the Installation Wizard.

2. Insert the product disc in the local client workstation's CD/DVD drive.

Note: If the disc image was downloaded and extracted to the client workstation's hard drive, open Windows Explorer, navigate to the disc image on the hard drive, and double-click the **start.hta** application to launch the Utilities software.

The Utilities software will determine if the client workstation includes the programs required to run the User Interface.

3. If prompted, click **.NET 4.5 Framework** and/or **Bonjour** to install the software.

4. Click the **Installation Wizard** icon.

5. When the Introduction page appears, select a **Language** and click [Next].

The Installation Wizard will search for any System Controllers on the network.

6. Select the System Controller in the list and click [Next].

7. On the Login page, type the current **Password** for the Administrator account.

The default **User Name** for the Administrator account is admin.

The default **Password** for the Administrator account is demo.

> **IMPORTANT:** The Administrator account has access to all aspects of the System. Leaving the default password unchanged is dangerous. People familiar with the product may know the default password.

8. Type the new password in the **New Password** and **Confirm Password** fields and click [Next].

9. On the Date/Time page, select the **System Controller Time Zone**.

10. If the **Panel Date and Time** and **Client Date and Time** values appear in red, either the time zone set on the System Controller is different from the time zone on the client workstation, or the time varies between the two devices by more than 10 seconds.

Click [Time Sync] to synchronize the time zone and time on the System Controller with the time zone and time on the client workstation.

Note: After the initial configuration is complete, the System can be synchronized with a Network Time Protocol (NTP) server. See Setting the Date and Time on page 15

11. Click [Next] to continue to the Network Configuration page.

12. Select **Static** or **Dynamic** as the connection type for the System Controller.

   To configure a static IP address:

   a. Type the **IP Address** for the System Controller that users will type into an Internet web browser to connect to the System.

   b. (Optional) Change the **Service Port** for the System Controller.

Note: The default Service Port for an HTTPS connection is 443; the default value for an HTTP connection is 80. Ports 0 through 1024 (i.e., *well-known ports*) are reserved for privileged services. It is recommended that these ports not be used as the Service Port. If the port is changed to a different value, users will need to append the port number to the IP address of the System Controller to log into the System (e.g., https://IPaddress:*port*).

   c. Type the **Subnet Mask** for the network to which the System Controller is connected.

   d. Type the **Default Gateway** for the network.

   e. Type the **DNS Server** for the network.

13. Select **Enable HTTPS Connection** to use a secure hypertext protocol

   IMPORTANT: HTTPS is highly recommended to prevent unauthorized access to the System.

14. Click [Apply] to save the network configuration.

15. To experiment with different network configurations, click [Reboot System Controller].

   The Panel Discovery page will appear and detect the System Controller again. Return to the Network Configuration page to edit settings, as necessary.

16. To access the primary User Interface and begin configuring the System, click the hyperlink that displays the IP address of the System Controller. See Configuring the System on page 13 for details.

17. Click [Finish] to close the Installation Wizard.

18. If IPSDCs are installed, configure each IPSDC to recognize the IP address of the System Controller *before* configuring the IPSDC in the User Interface. See Configuring IP-Based Single Door Controllers on page 106.

19. Proceed to Configuring the System on page 13.

Using the Upgrade Wizard

Existing TruPortal 1.0 or goEntry 3.0 customers can use the **Upgrade Wizard** to upgrade the System Controller remotely from a local client workstation from one version of the product to another version (for example, from version 1.0 to version 1.5). This process involves downloading files from the product website, and then using the Upgrade Wizard to back up data, update the firmware and core code on the System Controller, and then restore data.

Before using the Upgrade Wizard, note the following details:

> **IMPORTANT:** Do not power cycle the System Controller (i.e. turn it off and unplug the power) during an upgrade.

> **IMPORTANT:** *Upgrading* is different than *updating the firmware*. A firmware update only impacts the firmware, while an upgrade impacts both the firmware and the core code on the System Controller. Do not use the *System Administration > Firmware Updates* page to upgrade the System Controller; use the Upgrade Wizard instead.

- After an upgrade, the System Controller cannot be converted back to a previous version.
- The Upgrade Wizard is not compatible with Microsoft Windows XP.
- (Recommended) Run the Upgrade Wizard directly from the physical TruPortal DVD, as opposed to a mounted ISO image.
- Although the Upgrade Wizard provides an option to back up data, an extra backup file can be created as a precaution (see Create a Backup File on page 88). Configuration settings can also be backed up (see Saving and Restoring Custom Settings on page 89). To save an historical record of events, use the Import/Export Wizard to export events in CSV format.
- If upgrading from goEntry to TruPortal, card format information will be preserved.
- Make sure that all users are logged out of the System before using the Upgrade Wizard.
- Make sure that any backup and restore processes are finished.
- The upgrade will be faster and more reliable if the System Controller uses a static IP address. (To change this setting, see Configure Network Settings on page 17.) If a dynamic IP address is used, the IP address may change during the upgrade and the process will stop. If this occurs, use the Installation Wizard to obtain the new IP address and then restart the Upgrade Wizard.
- A [Finish] button appears on many wizard pages; click it to stop the upgrade, if necessary.

To use the Upgrade Wizard:

1. Log into the product web site and download the following files to a local client workstation:
   - The ISO image of the latest version of the Utilities disc.
   - The NGP.bin source file that will be used to update the firmware.

   IMPORTANT: Do not change the name of the downloaded files.

2. Use a third-party application to mount (i.e., add) the downloaded ISO image to the local client workstation.
3. In Windows Explorer, navigate to the **\PanelUpgradeWizard** folder in the ISO image.
4. Double-click **PanelUpgradeWizard.exe**.

   The wizard will create a folder called **\<local documents>\PanelUpgradeWizard** that includes two subfolders: **\Backups** and **\Logs**.
5. When the Introduction page appears, select a **Language** and click [Next].

6. Log in as a user with Execute permissions for the Firmware Updates feature, and then click [Next].

   The Source File page displays details about the firmware on the System Controller.

7. Click [...] to browse to the folder where the NGP.bin file was downloaded.

8. In the Open dialog box that appears, click the NGP.bin file to select it, and then click [Open].

   The Source File page displays details about the NGP.bin file.

9. Click [Next].

10. On the Backup page, type the path where data will be backed up, or browse to its location.

Note: Although the **Create Backup File** check box can be cleared to skip backing up data, it is recommended that users leave this check box selected to back up data before an upgrade. This option is intended for factory use only.

   IMPORTANT: If no backup file is created while using the Upgrade Wizard, photos will not be preserved and will need to be restored from an earlier backup.

11. Click [Backup].

12. When a "Backup Successful" message appears, click [Next].

13. On the next page, click [Firmware Upgrade].

   A summary of the Upgrade Wizard's progress appears. This process may take five to ten minutes. Red squares will appear next to any errors that occurred.

14. When the upgrade is complete, click [Next].

15. If data was backed up in step 11, the Restore page displays the location to which files were backed up.

    a. Click [Restore] to load the backed up data back onto the System Controller.

    b. When the "Restore Successful" message appears, click [Next] to verify that the upgrade occurred on the Upgrade Results page.

16. When the Upgrade Results page appears, click [Finish] to exit the wizard.

17. If a goEntry System was upgraded to TruPortal, review the card format descriptions on the *System Administration > Card Formats* page and update them, if necessary. (Card format descriptions are upgraded in English only.)

18. If IPSDCs are installed, configure each IPSDC to recognize the IP address of the System Controller *before* configuring the IPSDC in the User Interface. See Configuring IP-Based Single Door Controllers on page 106.

Configuring the System

TruPortal is designed so that, once configured, persons and credentials can be added and removed quickly, and access to a facility can be managed. During configuration, the following information will be defined:

- The areas, doors, credential readers, video surveillance, and auxiliary security systems at a site.
- Access levels needed by the various groups of persons who work at a site.
- Access schedules for regular days and holidays.
- Operator roles for the people who will be managing and monitoring the System.

This is organized sequentially, with tasks arranged in the order they should be completed to configure the System.

> **IMPORTANT:** If any IPSDCs are installed, configure them to recognize the IP address of the System Controller *before* configuring them in the User Interface. See Configuring IP-Based Single Door Controllers on page 106.

1. Logging into the System.
2. Setting the Date and Time.
3. Create a Certificate Signing Request.
4. Import a Security Certificate.
5. Configure Network Settings.
6. Configure Site Security.
7. Set the System Language.
8. Add a Card Format.
9. Scan for Hardware Changes.
10. Assign Meaningful Names to Hardware.
11. Configure the System Controller.
12. Optional: Configure I/O Expansion Modules.
13. Configure a Door Controller.
14. Configure a Door.
15. Configure Readers.
16. Optional: Add a DVR/NVR.
17. Optional: Add a Video Camera.
18. Optional: Link Cameras to Devices to Track Video of Events.
19. Optional: Add an Area.
20. Optional: Configure Anti-Passback.
21. Optional: Assign Readers to Areas.
22. Optional: Add a Holiday Group.
23. Optional: Add a Schedule.
24. Optional: Add a Reader Group.
25. Add an Access Level.
26. Optional: Add an Operator Role.
27. Optional: Configure an Email Server.
28. Optional: Add an Email List.
29. Optional: Add User-Defined Fields.
30. Optional: Scheduling Door and Reader Behavior.
31. Importing Persons and Credentials from a CSV File.
32. Optional: Configuring Action Triggers.
33. Optional: Configuring a Network Share.
34. Creating a Backup and Restore Point.
35. Optional: Add an Action Trigger Record.
36. Optional: Add a Language Pack.

Logging into the System

1. Launch an Internet browser.

2. Type the IP address for the System in the browser address bar.

Note: If the default service port for the System was changed, append the port number to the IP address (e.g., https://IP address:*port*).

3. If using Internet Explorer® and a warning about the security certificate appears, select **Continue to this website (not recommended)**.

4. Type a **Username**.

5. Type a **Password**.

6. (Optional) Select a different **Language** for the User Interface.

   By default, the System includes four languages — English, Spanish, French, and Dutch — but more can be added. See Managing Language Packs on page 92.

7. Click [Log In].

8. If this is the first time the User Interface is being used on the client workstation, click **Accept** when the License Agreement page appears.

The **Home** page displays several wizards that can be used to quickly add persons, credentials, access levels, schedules, and holidays. Click a wizard icon and follow the onscreen prompts to add new items, or refer to the relevant section of this document for step-by-step instructions.

To log out of the System later, click the **Logout** icon in the top-right portion of the User Interface.

Setting the Date and Time

The System supports time synchronization with a Network Time Protocol (NTP) server. This option, if enabled in both the User Interface and a DVR/NVR, keeps the DVR/NVR and the System synchronized in time. Without this, System time may drift relative to DVR/NVR time which can impact schedules and cause difficulty in retrieving video related to an access event.

Note the following details about NTP time synchronization:

• The NTP client will attempt synchronization every hour.

• To use this option, the System Controller must be able to access the NTP server via User Datagram Protocol (UDP) port 123. If this port is not accessible, the System time will not synchronize with the NTP server, and "NTP Sync Failed" events will be logged. Consult with the site network administrator.

• If the System time is manually changed to be within one minute prior to the start of a schedule assigned to a door, the scheduled door mode will take effect immediately.

To set the date and time:

1. Select *System Administration > System Settings*.

2. Click the **Date and Time** tab.

3. Select a **Time Zone**.

4. Select a local **Date and Time**.

5. (Optional) Synchronize time:

   a. Select the **Synchronize with NTP server** check box.

   b. Click [Accept Changes].

    c. Type the IP address of the NTP server.

    d. Click [Accept Changes].

    e. Click [Sync now].

6. Click [Accept Changes].

Configuring Network Security

The Network Configuration tab of the *System Administration > System Settings* page displays various network settings and can be used to assign a security certificate and configure network properties, including secure browsing.

Create a Certificate Signing Request

Secure Sockets Layer (SSL) is an encryption technology that protects data being transmitted between your web server and users' web browsers to prevent eavesdropping, data tampering, etc. The use of SSL on a website is usually indicated by a padlock icon in web browsers, but can also be indicated by a green address bar.

To enable SSL in the System, create a Certificate Signing Request (also known as a *CSR* or a *certification request*), submit it to a Certificate Authority, and then import the signed certificate. A self-signed certificate can also be installed. This block of encrypted text is generated on the server that the certificate is used on; it contains information such as the organization name, common name (i.e. domain name), locality, and country.

To create a Certificate Signing Request:

1. Select *System Administration > System Settings*.

2. Click the **Network Configuration** tab.

3. Click [Create Certificate Signing Request].

    The Certificate Signing Request dialog box appears.

4. Type the requested information and click [Generate].

Note: Type either the IP address or the Fully Qualified Domain Name (FQDN) of the server in the **Common Name** field. If the panel is configured to use a DHCP-assigned IP address, then it is highly recommended that the DHCP server be configured to always assign this IP address to the panel. Otherwise each time the panel is assigned a different IP address, a new certificate will need to be generated and installed.

    The Certificate Signing Request (CSR) text appears in the text box on the right side of the dialog box.

5. To use a self-signed certificate, click [Install Self-Signed Certificate].

    The System Controller will reboot automatically.

6. To use a signed certificate:

    a. Copy CSR text and save to a local file to send to a certificate authority.

    b. Close the Certificate Signing Request dialog box.

    c. See Import a Security Certificate on page 16.

Import a Security Certificate

1. Select *System Administration > System Settings*.

2. Click the **Network Configuration** tab.

3. Click [Import Certificate]. The Upload Certificate dialog box appears.

4. Click [Select File].

5. Browse to and select the certificate file.

6. Click [Open].

7. Click [Upload].

   The System Controller will reboot automatically.

Configure Network Settings

The network settings for the System are initially set up in the Installation Wizard, but can be updated on the **Network Configuration** tab of the *System Administration > System Settings* page, as described next. See Determining Network Settings on page 8 to learn more about configuration options.

1. Login as a user with Modification permissions for the Network Configuration feature.

2. Select *System Administration > System Settings*.

3. Click the **Network Configuration** tab.

4. Click [Configure].

   The Network Properties dialog box appears.

5. To use a dynamic connection, select **Obtain an IP address automatically using DHCP**.

6. To use a static connection, select **Use the following IP address** and type.

   To configure a static IP address:

   a. Type the **IP Address** for the System Controller.

   b. Type the **Subnet Mask**.

   c. Type the **Default Gateway**.

   d. Type the **DNS Server**.

7. (Optional) Change the **Service Port** for the System Controller.

Note: The default Service Port for an HTTPS connection is 443; the default value for an HTTP connection is 80. Ports 0 through 1024 (i.e., *well-known ports*) are reserved for privileged services. It is recommended that these ports not be used as the Service Port.

          If the port is changed to a different value, communicate that information to users because they will need to append the port number to the IP address of the System Controller (e.g., https://IPaddress:*port*) to log back in after the System reboots.

8. Select **Enable HTTPS Connection** to use a secure hypertext protocol.

   IMPORTANT: HTTPS is highly recommended to prevent unauthorized access to the System.

9. If the HTTPS setting was changed, clear the browser cache, especially if using Firefox or Chrome.

10. To use an SSH connection that authenticates remote client workstations and allows remote users (including technical support representatives) to log into the System, select **Enable SSH Connection**.

Note: Refer to Configuring Security on page 18 to learn about setting a password for an SSH service account.

11. Click [Save] to accept the network configuration changes.

   A message will appear to indicate that the System Controller must be rebooted to apply the changes to the network configuration.

12. Click [Save Changes].

   The System will reboot. Any users that are currently logged in will lose their connection and must log in again. If the IP address of the System Controller changed, update any IPSDCs in the System to recognize the new IP address. See Using the ICT to Configure IPSDCs on page 109.

Configuring Security

The **Security** tab of the *System Administration > System Settings* page can be used to configure certain aspects pertaining to the physical security of a facility.

PIN Codes

The System can be configured for access with a credential only, a credential and Personal Identification Number (PIN), PIN only, or PIN or credential. Requiring people to present a badge (credential) and type a PIN code provides added security by preventing access with a found or stolen badge. Readers can be configured to Credential Only, Credential and PIN, PIN Only, or PIN or Credential based on schedules. (See Scheduling Door and Reader Behavior on page 49.) Note: In PIN Only mode, all PINS in the system must be unique.

Max PIN Length
PINs can be 4, 6, or 9 digits in length.

Max PIN Attempts
Allows person a set number of chances to enter their PINs correctly.

PIN Lock Out Time
If a person enters an incorrect PIN too many times, the credential ID will be prevented from access at that reader for the length of time specified by this option. After the Lock Out Time has elapsed, the credential ID will have access privileges restored.

Door Fallback Mode

Credential information is stored on the System Controller. If a dual door controller loses communication with the System Controller, credentials scanned at a reader cannot be verified. In such a case, the door controller must validate access requests if anyone is to enter the facility.

Note: IPSDCs have a separate fallback mode.

Input EOL Terminations

Doors can be wired to detect if they are open or closed, forced entry, and tampering. Such a door is said to be *supervised*. A door without such detection circuits is said to be unsupervised, even if it has a reader and door strike or magnetic lock. For supervised doors, this option describes the type of resistor(s) used and how the circuit is wired. There are two main types that are monitored: 1,000 Ohm and 4,700 Ohm circuits. These can be wired with dual resistors, or with a single resistor wired in series or parallel relative to the door sensor.

Note: IPSDCs support only 1K/Dual supervision, as configured by setting switches on the panel. Refer to the *IP-based Single Door Controller Quick Reference* for details.

Set SSH Password for Service Account

An SSH connection can be enabled on the **Security** tab of the *System Administration > System Settings* page to authenticate remote users (including technical support representatives) that log into the System. Use the [Set SSH Password for Service Account] button to set the password.

IPSDCU Fallback Mode

Credential information is stored on the System Controller. If an IPSDC loses communication with the System Controller, credentials scanned at a reader cannot be verified. Select **Use Local Cache Table** to grant access if the card matches one of the last 50 credentials used to successfully gain access, as stored in the local cache of the IPSDC.

Note the following details about IPSDCU fallback mode:

- For the first 40—60 seconds of network connectivity loss, the IPSDC will continue to try to verify credentials via the System Controller. If the System Controller cannot be reached, credentials will be declined until IPSDC fallback mode starts.
- If credentials are changed or deleted, all data cached on IPSDCs is cleared.

Encrypt IPSDC Communications

By default, this check box is selected to encrypt communications between the System Controller and IPSDCs to enhance data security.

Configure Site Security

1. Select *System Administration > System Settings*.
2. Click the **Security** tab.
3. Select a PIN Max Length.

   IMPORTANT: When a new Maximum PIN Length is saved and there are existing credentials with PIN numbers longer than the new maximum length, a warning prompt will appear to indicate that existing PIN numbers will be truncated to the new length. The prompt will allow the user to continue or cancel the save operation.

4. Select the number of Max PIN Attempts.
5. Select a PIN Lock Out Time.
6. Select a Door Fallback Mode:
   - **No Access**: No access is granted whatsoever.
   - **Site Code Access**: Access is granted if the card matches one of the formats defined on the *System Administration > Card Formats* page, and the site code on the card matches the site code defined for the format.
   - **All Access**: Access is granted if the card matches any format defined on the *System Administration > Card Formats* page.
7. Select an option for Input EOL Terminations.
8. If an SSH connection was enabled on the Network Configuration tab, click Set SSH Password for Service Account to set a password for remote users logging into the System.
9. Select an IPSDCU Fallback Mode.
   - **No Access**: No access is granted whatsoever
   - **Site Code Access**: Access is granted if the card matches one of the formats defined on the *System Administration > Card Formats* page, and the site code on the card matches the site code defined for the format

- • **All Access**: Access is granted if the card matches any format defined on the *System Administration > Card Formats* page.
- • **Use Local Cache Table**: Access is granted if the card matches one of the last 50 credentials used to successfully gain access.

10. (Recommended) Leave the Encrypt IPSDCU Terminations check box to encrypt communications between the System Controller and IPSDCs and enhance data security

11. Click [Accept Changes].

Configuring the Primary System Language

A primary System Language can be defined on the System Options tab of the *System Administration > System Settings* page to determine the language used for functions performed by the System, such as assigning default device names, scheduled backups, and automated emails.

The System Language is also used if a user logs in and selects a language that is not currently available, or if a user performs a language-related action (for example, loading events on the *Events* page) and the language that the user logged in with is not available anymore. This may occur if a language pack is removed while users are still logged into the System.

Set the System Language

1. Select *System Administration > System Settings*.
2. Click the **System Options** tab.
3. Select a **System Language**.
4. Click [Accept Changes].

Configuring Card Formats

Credentials (identification badges) used for electronic access control store data in various formats. In order to read the data correctly, the card format has to be added to the configuration. The credential ID stored on the card includes a card number, a facility code, and an issue code.

Before a credential can be recognized, the System must be configured to recognize the card format — the way the data is formatted on the ID badge. Four default card formats are provided and more can be added. However, the System should be configured to recognize only those formats that are actively being used.

The default card formats provided include:

- • 26 Bit (H10301) Wiegand facility code 200
- • 32 Bit 14443 cascade 1
- • 37 Bit (I10304) facility 40
- • 40 Bit CASI 4002

Note the following details about card formats:

- • If the System is upgraded from an earlier version, existing card formats will be preserved.
- • The System is pre-configured for several popular commercial card formats, and supports up to eight card formats active simultaneously. If a desired card format is not listed, it can be added as a custom type.

- A *raw card format* does not include a facility code, but instead treats all data bits on the card as part of the access credential. Raw format credential cards are easier to configure than cards with facility codes included for this reason.

- Many standard card formats include a facility code as part of the credential ID. This allows for greater sophistication in configuring site security, but also adds complexity to configuration. For example, if a facility code is used and a door goes into fallback mode because it cannot communicate with the System Controller, the door can be configured to open if a card with a valid facility code is scanned at the reader. This is because the door controller does not store the full person database, but can store the facility code.

Add a Card Format

1. Select *System Administration > Card Formats*.
2. Click [Add].
3. Type a descriptive name in the **Format Name** field.
4. Select a **Format Type**.
5. Type the **Facility Code**, if required.
6. For a custom format, type other data as required.
7. Click [Accept Changes].

Remove a Card Format

1. Select *System Administration > Card Formats*.
2. Select the Card Format to be removed.
3. Click [Remove].

   The Remove Item dialog box appears.
4. Click [Remove].

Configuring Devices

This section describes how to configure the following devices:

- System Controller
- Inputs and outputs
- Door controllers
- Doors
- Readers
- Input/output expansion modules

To learn about configuring DVRs/NVRs and cameras, see Configuring Video Devices on page 33.

Before You Begin

Before configuring devices on the *System Administration > Devices* page, complete the following steps:

1. If IPSDCs are installed, they must be configured to recognize the IP address of the System Controller *before* configuring the IPSDCs in the User Interface. Establishing this network connection ensures that each IPSDC will be detected when the System Controller scans for hardware changes. See Configuring IP-Based Single Door Controllers on page 106.
2. Use the [Scan for Hardware Changes] button to discover devices, as described next.
3. (Optional, but recommended) Replace generic device names. See Assign Meaningful Names to Hardware on page 23.

Scan for Hardware Changes

Before configuring devices, click the [Scan for Hardware Changes] button on the *System Administration > Devices* page to discover the following types of proprietary devices located downstream from the System Controller and add them to the Device Tree automatically:

- Dual door interface modules
- Input/output expansion modules
- IPSDCs that have already been configured to recognize the System Controller

Another way to add door controllers on the *Devices* page is to select the System Controller and then click [Add]. Select the type of controller being added, fill out the remaining fields, and click [Accept Changes].

The System will assign generic, default names to the devices that can be customized later (see Assign Meaningful Names to Hardware on page 23) and display devices in a tree hierarchy on the *System Administration > Devices* page. Some default names are sequential (e.g., Input11, Input12, etc.). Doors and readers inherit the serial number of their parent door controller. For example, if a door controller has the serial number 1234, the doors located downstream of the door controller will be named Door 1234-1, Door 1234-2, etc.

Note: If the serial number of a door controller changes (for example, if a door controller is replaced), all child objects (doors and readers) that still use default names should be updated to reflect the new serial number of the parent door controller. See Replace a Door Controller on page 25.

To detect hardware devices in the System:

>　**IMPORTANT:**　Door controllers will go offline during the scan, which usually takes several minutes.

1.　Select *System Administration > Devices*.

2.　Select the System Controller.

3.　Click [Scan for Hardware Changes].

4.　Click [Accept Changes].

　　If the System detects any issues (for example, if no backup battery is installed), a notification will appear in a black box at the top of the User Interface; click inside the box to open the *Monitoring > Diagnostics* page and learn more about the issues. See Diagnostics on page 96.

Assign Meaningful Names to Hardware

Regardless of whether the System has a few devices or many devices of various types, effective naming conventions are essential for a successful deployment. The use of meaningful and well-structured names for inputs, outputs, door controllers, readers, etc. will help to:

•　Identify the location and function of each device.

•　Organize devices into meaningful groups.

•　Aid in the monitoring of access events.

Instead of using generic names assigned to devices by the Installation Wizard (e.g., *Door Controller 8888*), use pertinent elements in each device name to provide a frame of reference regarding the device type, location, or another category that is meaningful for an installation, such as *Main Lobby, East Wall Doors* for a door controller.

>　**Note:**　If default names are not customized, remember that any changes made to the name of a parent object must also be made to any child objects (for example, the doors and readers connected to a door controller) to avoid inconsistent device names.

Before beginning this task, consult the installation chart created when devices were installed, as described in Documenting the Physical Location of Each Device on page 5.

1.　Select *System Administration > Devices*.

2.　Select the System Controller.

3.　Type a descriptive **Device Name**.

4.　Click [Accept Changes].

5.　Select the first door controller on the list.

6.　Compare the **Serial Number** to the installation chart to confirm that the correct device was selected in the User Interface.

7.　Type a descriptive **Device Name**.

8.　Click [Accept Changes].

9.　Repeat for each of the devices in the hierarchy.

Configure the System Controller

The System Controller can accept four general purpose auxiliary inputs and produce two general purpose output signals, which must be manually activated. The inputs can be used for accessories such as a room motion detector, or for inputs from other systems, such as a fire alarm system. These represent optional configurations, and should only be enabled if installed. General purpose inputs can be configured to unlock all doors automatically when triggered, as in the case of a fire alarm or other emergency.

1. Select *System Administration > Devices*.

2. Select the System Controller.

3. Click the **General** tab.

4. Select a **Linked Camera** if one is configured to monitor the System Controller's physical location.

5. Click the Inputs tab.

6. For each general purpose auxiliary input that is connected:

   a. Select **Enabled**.

   b. Type a meaningful name.

   c. Select the **Type**.

   d. (Optional) Select **Unlock All Doors** if the input is from an alarm or emergency system.

   e. (Optional) Select a **Linked Camera** if one is associated with the input source (for example, a camera associated with a room motion detector).

7. Click the Outputs tab.

8. For each general purpose auxiliary output that is connected:

   a. Select **Enabled**.

   b. Type a meaningful name.

   c. Select **Active On/Off** if the relay should be energized when the output is off, otherwise clear the check box.

   d. (Optional) Select a **Linked Camera** if one is associated with the output.

9. Click [Accept Changes].

10. Click [Reboot Controller] to restart the System Controller.

Configure Inputs and Outputs

Inputs and outputs are general purpose options that can configured to meet the needs of a site. An input might be a signal from a motion detector, for example. An output is an electrical pulse from the System Controller to some device.

Use the *System Administration > Devices* page to configure inputs and outputs. Inputs and outputs can be monitored from the *Monitoring > Inputs/Outputs* page, and outputs can be activated manually from that page. Outputs can also be controlled by action triggers.

Configure a Door Controller

Note: If any IPSDCs are installed, configure them to recognize the IP address of the System Controller *before* configuring them in the User Interface. See Configuring IP-Based Single Door Controllers on page 106.

Dual door controllers can be connected to as many as four readers on two doors. IPSDCs can be connected to two readers on a single door. Each door may have two readers, one for access and one for exit, commonly used with Anti-passback.

1. Select *System Administration > Devices*.
2. Expand the tree below the System Controller.
3. Select the Door Controller.
4. Select the **Number of Doors** attached to this controller.
5. (Optional) Select a **Linked Camera** if one is associated with the door controller's panel.
6. Click [Accept Changes].

Note: If all doors are locked out when a new door controller is added, the new door controller will remain unlocked. To be locked out, all doors must be reinstated, then all doors locked out again.

Replace a Door Controller

IMPORTANT: If a door controller is replaced, be sure to update child objects (door and readers) to reflect the new serial number of the parent door controller before using the [Scan for Hardware Changes] button on the *System Administration > Devices* page, as described next. Otherwise, the configuration information will be overwritten.

To replace a door controller and preserve its configuration information:

1. Back up the database, as described in Create a Backup File on page 88.
2. Replace the door controller board.
3. (FOR IPSDCS ONLY) Use the Integrated Configuration Tool (ICT) to configure the new IPSDC to recognize the IP address of the System Controller. See Configuring IP-Based Single Door Controllers on page 106.
4. Update the serial number of the door controller on the *System Administration > Devices* page.
5. If child objects (doors and readers) still use default names, update them to reflect the new serial number of the parent door controller.
6. Reboot the System Controller. See Rebooting the System Controller on page 96.
7. Log back in after the System Controller reboots.

    The door controller may appear to be offline until it is able to connect to the System Controller.
8. (Recommended) Back up the database and save the updated configuration after the door controller comes online with the new serial number. See Backing Up Data on page 87 and Saving and Restoring Custom Settings on page 89.

Configure Doors

Each door needs to be configured for:

- The length of time it should be unlocked when a valid credential is presented.
- The length of time it can be held open before triggering an alarm.
- The type of door strike used (either standard locks or magnetic locks).
- Whether a reader is required for access only, or for both access and exit.
- The types of events and alarms monitored by the door circuitry.
- Auxiliary inputs and relays. For example, a door can be configured for an automatic opener and extended Request to Exit (RTE) to facilitate access by the disabled.

Configure a Door

1. Select *System Administration > Devices*.
2. Expand the tree below the System Controller.
3. Expand the tree below the door controller.
4. Select the door to configure.

Note: Some fields will not appear on the *Devices* page if a door is connected to an IPSDC, which does not support auxiliary input/output types or tamper input points. Refer to the *IP-based Single Door Controller Quick Reference* to learn about modifying DIP switch settings for input types. After changing DIP switch settings, reboot the IPSDC.

5. Select a Normal Grant Access Time.
6. (Optional) Select an Extended Grant Access Time.
7. Select a Door Held Time.
8. (Optional) Select an Extended Door Held Time.
9. Select a **Door Strike Mode**.
    - Timed Unlock
    - Lock on Close
10. (Optional) Select a **Linked Camera** if one is positioned to monitor the door.
11. Select an Access Mode.
12. (Optional) Select Request to Exit Enabled if the door is wired for it.
13. (Optional) If Request to Exit Enabled is selected, select Do Not Activate Strike on RTE to prevent the door strike from energizing when the Request to Exit contact closes.
14. (Optional) Select any alarms the door is wired for:
    - Door Held Open
    - Door Forced Open
    - Tamper
15. (Optional) If an alarm light or klaxon is wired to the door, select "Door Held/Forced" from the **Aux Relay** list.
16. Configure the sensor Input Types for:
    - **Door Contact** sensor
    - **Request to Exit** button or sensor
    - **Aux** input from the Extended Request to Exit or magnetic lock contact sensor
    - **Tamper** circuitry

Note: The Aux and Tamper inputs listed above do not apply to doors connected to IPSDCs.

17. Click [Accept Changes].

18. Repeat for each door.

Configure a Door for Disabled Access

Events are recorded whenever doors are held open too long and when access is granted but the door is not opened. With an optional alarm light or klaxon, the System can trigger a physical alarm if the door is forced or held open too long.

To accommodate the needs of those who may require more time to open or pass through a door, the System allows users to identify which credentials are granted this permission, and allows users to configure a door for optional features, such as an automatic door opener, and extra time for Request to Exit sensors. This is done on a credential-by-credential basis to preserve site security, as the longer a door is held open, the easier it is for people to enter without presenting a credential. See Add a Credential on page 68.

1. Select *System Administration > Devices*.

2. Expand the tree below the System Controller.

3. Expand the tree below the Door Controller.

4. Select the Door to configure.

Note: Some fields will not appear on the *Devices* page if a door is connected to an IPSDC, which does not support auxiliary input/output types or tamper input points. Refer to the *IP-based Single Door Controller Quick Reference* to learn about modifying switch settings for input types.

5. Select a Normal Grant Access Time.

6. Select an Extended Grant Access Time.

   This is the amount of time the door will remain unlocked so the person can open it.

7. Select a Door Held Time.

8. Select an Extended Door Held Time.

   This is the amount of time the door can remain open so the person can pass through.

9. Select a **Door Strike Mode**.

   • Timed Unlock

   • Lock on Close

10. (Optional) Select a **Linked Camera** if one is positioned to monitor the door.

11. Select an Access Mode.

12. (Optional) Select Request to Exit Enabled if the door is wired for it.

13. (Optional) If Request to Exit Enabled is selected, select Do Not Activate Strike on RTE to prevent the door strike from energizing when the Request to Exit contact closes.

14. (Optional) Select any alarms the door is wired for:

   • Door Held Open

   • Door Forced Open

   • Tamper

15. If the door is wired for a door opener:

   a. Select "Extended RTE" from the Aux Input list.

   b. Select "Door Opener" from the Aux Relay list.

    c. Select an **Aux Relay On Time**.

16. Configure the sensor Input Types for:

- **Door Contact** sensor
- **Request to Exit** button or sensor
- **Aux** input from the Extended Request to Exit or magnetic lock contact sensor
- **Tamper** circuitry

Note: The Aux and Tamper inputs listed above do not apply to doors connected to IPSDCs.

17. Click [Accept Changes].

18. Repeat for each door.

Configure a Door for Magnetic Locks

• WARNING! • When configuring a door with magnetic locks, it is important to use the "Mag Lock Bond Sense" option to prevent the door magnets from prematurely activating and slamming the door shut, potentially causing injury.

1. Select *System Administration > Devices*.

2. Expand the tree below the System Controller.

3. Expand the tree below the Door Controller.

4. Select the Door to configure.

Note: Some fields will not appear on the *Devices* page if a door is connected to an IPSDC, which does not support auxiliary input/output types or tamper input points. Refer to the *IP-based Single Door Controller Quick Reference* to learn about modifying jumper settings for input types.

5. Select a Normal Grant Access Time.

6. Select an Extended Grant Access Time.

This is the amount of time the door will remain unlocked so the person can open it.

7. Select a Door Held Time.

8. Select an Extended Door Held Time.

This is the amount of time the door can remain open so the person can pass through.

9. Select a **Door Strike Mode**.

- Timed Unlock
- Lock on Close

10. (Optional) Select a **Linked Camera** if one is positioned to monitor the door.

11. Select an Access Mode.

12. (Optional) Select Request to Exit Enabled if the door is wired for it.

13. (Optional) If Request to Exit Enabled is selected, select Do Not Activate Strike on RTE to prevent the door strike from energizing when the Request to Exit contact closes.

14. (Optional) Select any alarms the door is wired for:

- Door Held Open
- Door Forced Open
- Tamper

15. Select "Mag Lock Bond Sense" from the Aux Input list.

16. (Optional) If an alarm light or klaxon is wired to the door, select "Door Held/Forced" from the Aux Relay list.

17. Configure the sensor Input Types for:

    • **Door Contact** sensor

    • **Request to Exit** button or sensor

    • **Aux** input from the Extended Request to Exit or magnetic lock contact sensor

    • **Tamper** circuitry

Note: The Aux and Tamper inputs listed above do not apply to doors connected to IPSDCs.

18. Click [Accept Changes].

19. Repeat for each door.

Door Configuration Options

Normal Grant Access Time
When a valid credential is scanned by the reader, the door will be unlocked for the time selected here.

Note: Schlage AD-400 wireless locks ignore this setting. Configure the **Relatch After** value in the Schlage Utility Software instead. See the *TruPortal Wireless Locks Quick Reference* for details.

Extended Grant Access Time
When a valid credential with the **Use extended strike/held times** option selected (as configured on the *Access Management > Persons* page) is scanned by the reader, the door will be unlocked for the **Normal Grant Access Time** plus the **Extended Grant Access Time**. This allows users to configure the System to comply with legislation governing access by individuals with disabilities.

Note: Schlage AD-400 wireless locks ignore this setting. Configure this feature in the Schlage Utility Software instead. See the *TruPortal Wireless Locks Quick Reference* for details.

Door Held Time
When a valid credential is scanned by the reader, the door can be held open for the **Normal Grant Access Time** plus the **Door Held Time**. An event is recorded if a door is held open longer than that and the **Door Held Open** alarm option is selected.

Extended Door Held Time
When a valid credential with the **Use extended strike/held times** option selected (as configured on the *Access Management > Persons* page) is scanned by the reader, the door can be held open for **Normal Grant Access Time** plus the **Extended Door Held Time**. An event is recorded if a door is held open longer than that and the **Door Held Open** alarm option is selected. This allows users to configure the System to comply with legislation governing access by individuals with disabilities.

Request to Exit Enabled
If the door is alarmed for being forced open, held open too long, and tampering, then Request to Exit (RTE) must be used in conjunction with either a button to be pressed for exit or a reader used for exit, or some kind of sensor that detects someone approaching the door from the inside. Otherwise, every time someone exits, a force door alarm will be generated.

Do Not Activate Strike on RTE
A Request to Exit contact is typically a button located near the associated door. Select this option to prevent the door strike from energizing when the RTE contact closes. When a cardholder pushes the button, an RTE is sent to the System Controller. (RTEs are also known as REXs.)

If this check box is selected, the door strike will NOT energize when the RTE contact closes. If this check box is not selected, the door strike energizes when the RTE contact closes.

Door Strike Mode
Timed Unlock
The door will unlock when access is granted and will remain unlocked until the time specified in **Normal Grant Access Time** expires.

If the door **Aux Input** is configured for Mag Lock Bond Sense, the strike relay will remain active until the magnetic contact sensor is active, the door contact is closed, and the door unlock time has expired.

Note: IPSDCs do not support Aux input and output. Schlage AD-400 wireless locks ignore this setting.

Lock On Close
The door will unlock when access is granted and will remain unlocked until either the time specified in **Normal Grant Access Time** expires, or the door is opened and closed, whichever occurs first.

If the door **Aux Input** is configured for *Mag Lock Bond Sense*, the strike relay will remain active until the magnetic contact sensor is active, the door contact is closed, regardless of unlock time.

Note: IPSDCs do not support Aux input and output. Schlage AD-400 wireless locks ignore this setting.

Access Mode
Reader In Only
The door has a reader to scan credentials for entry, but does not require a person to present a credential to exit.

Reader In Reader Out
The door has readers to scan credentials both for entry and exit. This is required for Anti-passback configurations.

Alarm Enabled
Door Held Open
Select this option if the door is wired to detect its opening. If held open longer than the time selected for **Door Held Time**, an event will be recorded on the *Events* page.

Door Forced Open
Select this option if the door is wired to detect forced entry. If a person opens the door without presenting a credential that is granted access, an event will be recorded on the *Events* page. Configure with an alarm light or klaxon wired to the **Aux Relay** if a physical alarm should occur if the door is forced.

Tamper
Select this option if the door is wired to detect reader tampering. If tampering occurs, an event will be recorded on the *Events* page.

Note: The **Tamper** option controls the tamper input point only, not the Door Contact, Request to Exit, or Aux Input points. Also, this option will not appear on the *System Administration > Devices* page if a door is connected to an IPSDC, which does not support reader tamper input.

Aux Input

Note: This field will not appear on the *System Administration > Devices* page if a door is connected to an IPSDC, which does not support auxiliary input/output types. Refer to the *IP-based Single Door Controller Quick Reference* to learn about modifying jumper settings for input types.

None
Indicates the input is not used and not monitored.

Extended RTE
Intended for use only with the Door Opener option selected for **Aux Relay**.

Mag Lock Bond Sense
Intended for doors that use a magnetic lock instead of a door strike. This detects the output from the magnetic lock indicating the door has bonded to the magnet. The System will not activate the magnet until the door bond sensor sends a signal indicating the door has made contact with the magnet and the door contact sensor indicates the door is closed. This prevents the magnet from activating prematurely and causing the door to slam closed.

If "Timed Unlock" is selected for **Door Strike Mode**, then the magnet will remain inactive until that time has expired. However, it will still not activate until the magnetic bond sensor and door contact sensor signals are received indicating the door is closed and bonded to the magnet.

Aux Relay

Note: This field will not appear on the *System Administration > Devices* page if a door is connected to an IPSDC, which does not support auxiliary input/output types. Refer to the *IP-Based Single Door Controller Quick Reference* to learn about modifying jumper settings for input types.

None
Indicates the relay is not used and not energized.

Door Held/Forced
A typical use for this option is to have the relay trigger some physical alarm, such as a siren or light, whenever the door is held or forced open.

Door Opener
Typically used with a door configured with a single reader for entry and a manual release wired for RTE, and a push button for an Extended RTE automatic opener. The RTE input unlocks the door for the duration that the manual release is active so that someone can exit normally. The Aux input (Extended RTE) activates the Aux Relay for the specified Aux Relay On Time. This relay output activates a door opener that automatically unlocks and opens the door for a person needing assistance.

This setting only makes sense if **Aux Input** is configured for Extended RTE.

Input Types

NO (Normally Open)

The sensor switch is normally open.

NC (Normally Closed)

The sensor switch is normally closed.

Unsupervised

The circuit is not wired with a continuity circuit to detect tampering.

Supervised

The circuit is wired with a continuity circuit to detect tampering.

Note: For IPSDCs, refer to the *IP-based Single Door Controller Quick Reference* for information about how to configure the switch settings based on input type selection.

Configure Readers

1. Select *System Administration > Devices*.
2. Expand the tree below the System Controller.
3. Expand the tree below the Door Controller.
4. Expand the tree below the Door.
5. Select the Reader to configure.
6. Select an **Access Method**.
   - Credential Only
   - Credential and PIN
   - PIN Only
   - PIN or Credential
7. Select a **Linked Camera** if one is position to watch this door and reader.
8. Click [Accept Changes].
9. Repeat for other readers.

Reader Configuration Options

Credential Only

A person need only present a valid credential (ID badge) to gain access.

Credential and PIN

A person needs to present a valid credential and enter a Personal Identification Number (PIN) to gain access. This prevents someone gaining access with a stolen or found credential. Some facilities use **Credential Only** during the day and **Credential and PIN** after hours, when the facility is empty.

PIN Only

A person need only enter a valid Personal Identification Number (PIN) to gain access.

PIN or Credential

A person needs to present either a valid credential or enter a Personal Identification Number (PIN) to gain access.

Configure I/O Expansion Modules

1. Select *System Administration > Devices*.

2. Select the IO Expander.

3. Click the **General** tab.

4. Select a **Linked Camera** if one is configured to monitor the System Controller's physical location.

5. Select **Tamper Alarm Enabled** if the enclosure is wired for tamper detection.

6. Click the **Inputs** tab.

7. For each general purpose auxiliary input that is connected:

   a. Select **Enabled**.

   b. Type a meaningful name.

   c. Select the **Type**.

   d. (Optional) Select **Unlock All Doors** if the input is from an alarm or emergency system.

   e. (Optional) Select a **Linked Camera** if one is associated with the input source (for example, a camera associated with a room motion detector).

8. For each general purpose auxiliary output that is connected:

   a. Select **Enabled**.

   b. Type a meaningful name.

   c. Select **Active On/Off** if the relay should be energized when the output is off, otherwise clear the check box.

   d. (Optional) Select a **Linked Camera** if one is associated with the output.

9. Click [Accept Changes].

Configuring Video Devices

Video records of access events can be reviewed by accessing the video recorded on a DVR/NVR from the cameras associated with a device connected to the System Controller. When an event happens at a device, the System keeps a record of the date and time of the event. If a camera is linked to that device, the System uses the event date and time to create a hyperlink to the recorded video on the DVR/NVR to which the camera is attached.

Linking a camera to a device enables the System to associate an event at that device with the video recorded from the camera during the time of the event. The System does not control the camera or DVR/NVR directly, but it uses the information to tell the DVR/NVR the date and time and which camera recorded the video to playback.

Video surveillance cameras are one of two general types: either stationary or capable of panning, tilting, and zooming (PTZ). Users can control PTZ cameras if:

• Internet Explorer is being used as the browser,

• Microsoft .NET Framework 4.5 (or later) is installed,

• ActiveX controls are enabled in the browser, and

• The camera is connected to a DVR/NVR.

Add a DVR/NVR

Before adding a DVR/NVR, see the Release Notes to determine the minimum firmware revision required. Consult the DVR/NVR documentation for firmware update instructions.

1. Select *System Administration > Devices > Video Devices*.

2. Click [Add] and choose the appropriate DVR/NVR model. If the model of the TruVision recorder is not listed, try to add it by selecting **TVR Generic** or **TVN Generic**.

3. Type a descriptive name for the device in the **Device Name** field.

4. Type the **IP Address** of the device.

5. Type the **User Name** for logging into the device.

6. Type the **Password** for logging into the device.

7. Click [Accept Changes].

8. Click the link below **Web Browser Configuration and Control** to confirm the connection and check the configuration of cameras attached to the device.

Add a Video Camera

Before performing this task, a DVR/NVR must be added to the System.

1. Select *System Administration > Devices > Video Devices*.

2. Select the DVR/NVR with the camera to be added.

3. Select *Add > Camera.*

4. Type a descriptive name for the camera in the **Device Name** field.

   For example, "Main Lobby Camera."

5. Select the appropriate **DVR Input**.

   This is the channel on the DVR/NVR to which the camera is physically connected.

6. Select a **Video Stream Bandwidth**.

   If the bandwidth is not known, log into the web-based interface of the DVR/NVR and examine the setting for the camera.

7. Type the desired **Pre-Event Playback Duration**.

   This is the length of time leading up to the event that will appear in the playback. For example, a forced door event will be recorded in the System when the door is forced open, however, the person who forced the door may have been tampering with it for several seconds before successfully forcing it open.

A camera can also be set up to monitor the physical location of the System Controller. Refer to Configure the System Controller on page 23.

Add Video Layouts

Video layouts determine how many camera inputs can be monitored from a computer screen at one time.

1. Select *Monitoring > Video Layouts*.

2. Click [Add].

3. Type a descriptive name in the **Video Layout Name** field.

   For example, if four cameras are watching the loading dock area, create a 2x2 layout and name it "Loading Dock Cameras."

4. Select a **Video Layout Type**.

5. Select a camera for each cell of the layout.

6. Click [Accept Changes].

Link Cameras to Devices to Track Video of Events

Readers will generate events for access granted and access denied, so if a camera is linked to a reader, users will have a visual record of each person who entered (or was denied entry) by that reader.

Doors will generate events if forced open, held open too long, and for momentary unlocking, so if a camera is linked to a door, users will have a record of each access security incident.

Auxiliary inputs and outputs are optional devices connected to either the System Controller or an I/O Expansion Module. To link a camera to these devices, use the Input or Output tab of the appropriate System Controller.

1. Connect the System (via a TCP/IP network) to the DVR/NVR and camera.

   a. See Add a DVR/NVR on page 34.

   b. See Add a Video Camera on page 34.

2. Select *System Administration > Devices*.

3. Select the device from the hierarchical tree.

4. Select the appropriate camera from the **Linked Camera** list.

Configuring Areas

Areas represent the spaces in the physical floor plan of a facility, specifically the entrances and exits to those spaces. Defining areas allows users to identify which readers lead into those spaces, and which readers lead out of those spaces into adjoining areas. Areas are used to track the physical location of persons in the facility, which can be viewed in the Roster Report, and for Anti-passback (APB) tracking of credentials.

Add an Area

Before assigning readers to an area, the area must be created.

1. Select *Access Management > Areas > Area Definition*.
2. Click [Add].
3. Type a descriptive name in the **Area Name** field.
4. Select an **Anti-Passback Auto Reset** option.

   If "Never" is selected, an Anti-passback violation will have to be reset manually.
5. Click [Accept Changes].

Assign Readers to Areas

Assigning readers to areas is what defines areas in the System. The System records what reader a credential is scanned at, and based on area assignment, notes which area the person with that credential must be in and what readers that person must pass before moving to another area.

> **IMPORTANT:** Be sure that reader assignments are correct. If a credential is detected at a reader that is not contiguous to the last reader, then an Anti-passback violation is triggered. For example, if Lab A adjoins the main corridor and is physically set up so that Reader 1 grants access and Reader 2 grants exit, but a user mistakenly assigns Reader 3 as the exit, then every person attempting to leave Lab A will cause an Anti-passback violation.

1. Select *Access Management > Areas > Reader Assignments*.
2. For each reader:
   a. Select the **From Area**. This is the area where the reader is located.
   b. Select the **To Area**. This is the area the person will enter, once the credential is accepted at the reader.
   c. Select **Anti-Passback**:
      • None
      • Soft
      • Hard
3. Click [Accept Changes].

Remove an Area

Note: The Default Area cannot be removed.

1.   Select *Access Management > Areas > Area Definition*.

2.   Select the area to remove.

3.   Click [Remove].

     The Remove Item dialog box appears.

4.   Click [Remove].

Configuring Anti-Passback

Anti-passback requires a credential be used to enter and exit an area so that the System knows which area the credential holder is currently occupying. The System keeps a record of personnel movements in secure areas, and prevents passage to areas that are logically impossible.

If a person uses a credential to enter an area configured for Anti-passback, and then leaves the area (through a door held open by another person, for example), the System will not know the person has left the specific area. As a result, if the System is configured for hard Anti-passback enforcement, it will prevent that credential from being used to enter another area, including the one just left, until the credential's location is reset to a default or neutral area.

Anti-Passback Options

An Anti-passback violation occurs when a person presents a credential (ID Badge) to enter an area, but somehow leaves the area without presenting the ID. The event is triggered when the person tries to enter another area that is not physically connected to the person's last known area.

None
Anti-passback is not used.

Soft
An event is recorded when a credential violates anti-passback rules.

Hard
The credential violating anti-passback rules is prevented from accessing any areas until the credential's location is reset to a neutral or default area.

Configure Anti-Passback

To configure anti-passback, add areas to the System that match the areas in the site or floor plan, assign readers to those areas, and add credentials.

1.   See Add an Area on page 36.

2.   See Assign Readers to Areas on page 36.

3.   See Add a Credential on page 68.

Note: The Credential pane of the *Access Management > Persons* page allows users to exempt individual credentials from anti-passback enforcement.

Creating Holiday Groups

Holidays are exceptions in workplace schedules.Creating a holiday group for those days will cause the System to override the regular schedule on those days. If a holiday should not override a certain schedule, then the holiday group must be included in that schedule.

For example, a facility may be open every Monday to Friday except for certain annual holidays, when only the housekeepers and network administrators should have access to the facility. The housekeepers may do extensive cleaning when the facility is closed for normal business. The network administrators may use holidays to do extensive maintenance or upgrades that would be disruptive on a regular workday.

To accommodate these needs, create a holiday group for those days when the regular staff will not report to work. Then create two schedules and two access levels, one for regular staff and one for support staff (i.e., housekeepers and network administrators). Include the holiday group in the support staff schedule, but not in the regular staff schedule. By default, when the holiday group is created, it will automatically be "excluded" from schedules and the schedule will not operate on that holiday.

When configuring the support staff access level, assign the support staff schedule to the readers and reader groups that the support staff will use. (Remember to "include" the holiday group by selecting it on the schedule so that this group of people will have access granted during the holidays.) When configuring the regular staff access level, assign the regular staff schedule to the readers and reader groups that the regular staff will use.

Note the following details about how holidays impact schedules:

•   When a date is designated as a holiday, the System makes an exception to all normal operations on that particular date or set of date unless customized schedule programming is created to take effect on the same date.

   For example, if a door is scheduled to automatically unlock every day from 8:00 a.m. to 5:00 p.m., that door will remain locked on a holiday rather than unlocking as it normally would. Another example occurs if a person normally has card access to a particular door on Wednesdays and a programmed holiday occurs on a Wednesday, then that person cannot access the door on that day.

•   To make an exception for a person that needs building access on a holiday, that person must be assigned to a schedule that is excluded from the holiday group.

   For example, to grant a person access to the building on Christmas day, adjust the access level of the person (for example, an access level called "Support Staff"), link the access level to a specific schedule (for example, a schedule called "24/7"), and then adjust the 24/7 schedule to include the Christmas day holiday.

•   To perform a scheduled unlock on a holiday, add the holiday to a schedule that is assigned to a particular door.

Add a Holiday Group

IMPORTANT: The creation of a holiday group will take effect immediately. The holidays added to this group will be excluded from ALL schedules, thereby removing the specified days from normal operations on that particular date or set of dates and causing the System to override the regular schedule. Refer to Creating Holiday Groups on page 38 for details.

1. Select *Access Management > Holidays*.

2. Click [Add].

3. Type a descriptive name in the **Holiday Group Name** field.

    By default, a newly created holiday group has one holiday in it.

    a. Choose the date and pattern of the holiday:

        •   **Single**: a one time event.

        •   **Repeats yearly**: an event that occurs on the same date each year, such as the 25th of December.

        •   **Custom**: an event that repeats yearly on a specified pattern, such as the last Monday of May.

    b. For a single or repeating holiday, type the start date in the **Date** field, or click the **Calendar** icon next to the **Date** field to select a date from the Calendar pop-up window.

    c. Type the number of days that the holiday spans in the **Duration** field. (By default, a newly created holiday is one day long. Valid values are 1 to 366.)

4. To add another holiday to the group, click [Add] in the holiday list pane and repeat step a through step c.

5. Click [Accept Changes].

Add a Holiday to a Holiday Group

1. Select *Access Management > Holidays*.

2. Select the holiday group to be modified.

3. Add a holiday to the group:

    a. Click [Add] in the holiday list pane.

4. Create intervals for the schedule.

    a. To create additional intervals, click [Add] on the Interval List pane.

    b. Click the check box above each day that should be added to the interval.

    c. Type values for the start and end times.

    d. For a single or repeating holiday, type the start date in the **Date** field, or click the **Calendar** icon next to the **Date** field to select a date from the Calendar pop-up window.

    e. Type the number of days that the holiday spans in the **Duration** field.

5. Click [Accept Changes].

Copy a Holiday Group

1. Select *Access Management > Holidays*.

2. Select the holiday group to be copied.

3. Click [Copy].

4. Type a descriptive name in the **Holiday Group Name** field.

5. Make changes to holidays in the copied group as needed.
6. Click [Accept Changes].

Remove a Holiday Group

Note: A holiday group that is in use cannot be deleted.

1. Select *Access Management > Holidays*.
2. Select the holiday group to be removed.
3. Click [Remove].

   The Remove Item dialog box appears.
4. Click [Remove].

Creating Schedules

Schedules are used to determine when a person will be granted access at a reader, or when a door will automatically lock or unlock. Up to 64 schedules can be created and used in the System, including the following pre-defined schedules:

- All Days 24/7
- Weekdays 8AM-5PM
- Weekdays 9AM-6PM
- Weekdays 7AM-7PM

An *interval* is the period of time during which a schedule is active. Schedules can include multiple intervals. For example, if the office cleaning staff vacuums the floors on Wednesdays, but on the other days of the week cleans only the rest rooms and trash bins, they would need access for more hours on Wednesday than on other days of the week. In this case, one interval could be created for Wednesday and another for the other days of the week.

Note the following details about schedules:

- Schedule times are expressed in hours and minutes, not seconds, but interval start times are relative to the start of the minute (0 seconds), and interval end times are relative to the end of the minute (59 seconds). In the pre-defined 24/7 schedule, notice that the start time is 12:00 AM and the end time is 11:59 PM. Expressed in seconds, the start time is 12:00:00 AM and the end time is 11:59:59 PM, a one second difference. A schedule that passes midnight must be set up this way, because if 12:00 AM was entered as the start and end time, the schedule would be active for only 59 seconds (from 12:00:00 to 12:00:59).
- Action triggers, schedules, and manual control can all impact the state of devices and are treated equally by the System. The last operation executed determines the state of a device.
- When a date is designated as a holiday, the System makes an exception to all normal operations on that particular date or set of dates unless customized schedule programming is created for the same date. Refer to Creating Holiday Groups for details about how holidays impact schedules.
- Schedules to control reader access times are assigned via the *Access Management > Access Levels* page.
- Schedules to control door locking are assigned via the *Monitoring > Doors* page.

Add a Schedule

1. Select *Access Management > Schedules.*

2. Click [Add].

3. Type a descriptive name in the **Schedule Name** field.

4. Click **Holiday Groups**.

5. Select the holiday groups that are included in this schedule.

Note: Holidays are exceptions to normal access schedules. Including a holiday group in a schedule keeps that holiday group from overriding that schedule. For example, if a holiday group for bank holidays is created and the business office is closed on those days, that holiday group should not be selected for the schedule for the office workers access level. However, if the shipping department works on holidays, the bank holiday group could be selected for the schedule for the shipping workers access level, thus preventing the bank holiday group from overriding the shipping schedule.

6. Click [Accept Changes].

Add an Interval to a Schedule

1. Select *Access Management > Schedules.*

2. Select the schedule to modify.

3. Create intervals for the schedule.

   a. To create additional intervals, click [Add] on the Interval List pane.

   b. Click the check box above each day that should be added to the interval.

   c. Type values for the start and end times.

4. Click [Accept Changes].

Remove an Interval from a Schedule

1. Select *Access Management > Schedules.*

2. Select the schedule to modify.

3. Select the interval to remove.

4. Click [Remove] on the interval list pane.

5. Click [Accept Changes].

Copy a Schedule

1. Select *Access Management > Schedules.*

2. Select the schedule to copy.

3. Click [Copy].

4. Type a descriptive name in the **Schedule Name** field.

5. Add, remove or change time intervals as required.

6. Click [Accept Changes].

Remove a Schedule

1. Select *Access Management > Schedules.*

2. Select the schedule to remove.

3. Click [Remove].

   The Remove Item dialog box appears.

4. Click [Remove].

Creating Reader Groups

Reader groups are useful when a large number of readers and doors exist in a facility. Reader groups allow users to cluster several readers according to a common characteristic, and assign these as a group to access levels. For example, all the readers in the basement of a building might be added to a group.

The grouping need not be according to physical area. For example, a reader group called housekeeping might be used in an access level that grants access to all secure cleaning-supply storage closets.

Reader groups appear on the *Access Management > Access Levels* page, allowing users to grant access to all readers in a group with a single selection, rather than reader by reader.

Add a Reader Group

1. Select *Access Management > Reader Groups*.

2. Click [Add].

3. Type a descriptive name in the **Reader Group Name** field.

4. Select each Reader in the group.

5. Click [Accept Changes].

Copy a Reader Group

1. Select *Access Management > Reader Groups*.

2. Select the reader group to copy.

3. Click [Copy].

4. Type a descriptive name in the **Reader Group Name** field.

5. Add or change reader assignments as desired.

6. Click [Accept Changes].

Remove a Reader Group

1. Select *Access Management > Reader Groups*.

2. Select the reader group to remove.

3. Click [Remove].

   The Remove Item dialog box appears.

4. Click [Remove].

Configuring Access Levels

Access levels determine which doors a credential has access to and when. For example, if a facility has an office and a warehouse, and office workers are not allowed in the warehouse, then an Access level for office workers could be created which includes only those doors in the office area.

The *Access Management > Access Levels* page is used to assign schedules to readers and reader groups. Access levels are then assigned to credentials, determining which days and times a person with that credential can gain entry through the readers in that access level.

Add an Access Level

1. Select *Access Management > Access Levels*.
2. Click [Add].
3. Type a descriptive name in the **Access Level Name** field.
4. Select the readers and reader groups to include in this access level.
5. Select a schedule for each selected reader.
6. Click [Accept Changes].

Copy an Access Level

For a large number of readers, creating a new access level can be time consuming. Copying an existing access level allows users to reuse a similar configuration and make only the few changes required for the new access level.

1. Select *Access Management > Access Levels*.
2. Click the access level to be copied.
3. Click [Copy].
4. Type a descriptive name in the **Access Level Name** field.
5. Make any needed changes to the readers and reader groups in this access level.
6. Clear the check box next to any readers that should not be included in this access level.
7. Click [Accept Changes].

Remove an Access Level

1. Select *Access Management > Access Levels*.
2. Click the access level to be removed.
3. Click [Remove].

    The Remove Item dialog box appears.
4. Click [Remove].

Configuring Operator Roles

An operator role is a group permissions policy. When a person is added and granted the ability to log into and operate the System, that operator is granted certain permissions to change, execute or merely view features and data. Rather than manually configure access to each feature or datum for each

operator individually, the operator role feature allows users to assign access privileges common to each type of operator based on their respective job roles.

Note the following details about operator roles:

- The predefined settings cannot be changed for the Administrator role.
- Only an Administrator can modify settings for the Operator, Guard, View Only, and Dealer roles.
- The Administrator role cannot be deleted.
- The Operator role cannot be deleted if it is currently assigned to one or more persons.

Examples of how the various operator roles can be used include:

- **Administrator**: The primary user responsible for managing the System.
- **Operator**: Information technology specialists who use the System to perform tasks such as backing up databases, assigning access levels, etc.
- **Guard**: Security personnel responsible for monitoring the facility who use the System to control PTZ cameras, doors, inputs, etc., as well as display video, run reports, and execute action trigger records manually.
- **View Only**: Supervisors who need read-only access to the System for management purposes.
- **Dealer**: Resellers and consultants responsible for the initial setup of the System.

The various permission levels include:

- **None**: The operator cannot visit or view this page.
- **View**: The operator can see the page or data, but cannot make changes or execute commands.
- **Modification**: The operator can change settings.
- **Execute**: The operator can execute commands.

To display a list of the default permission levels assigned to operator roles, see Pre-Defined Operator Role Permissions on page 111.

Add an Operator Role

1. Select *System Administration > Operator Roles*.
2. Click [Add].
3. Type a descriptive name for the role in the **Role Name** field.
4. Select a **Permission** for each feature.
5. Click [Accept Changes].

Modify an Operator Role

Note: The Administrator role cannot be modified.

1. Select *System Administration > Operator Roles*.
2. To rename, type a descriptive name for the role in the **Role Name** field.
3. Change the **Permission** for each feature, as needed.
4. Click [Accept Changes].

Copy an Operator Role

Copying an existing operator role allows users to reuse a similar configuration and make only the few changes required for the new role.

1. Select *System Administration > Operator Roles*.
2. Select the role to be copied.
3. Click [Copy].
4. Type a descriptive name for the role in the **Role Name** field.
5. Change the **Permission** for each feature, as needed.
6. Click [Accept Changes].

Remove an Operator Role

Note:　　　Roles that are currently assigned to users cannot be deleted.

1. Select *System Administration > Operator Roles*.
2. Select the role to be removed.
3. Click [Remove].

   The Remove Item dialog box appears.
4. Click [Remove].

Configuring Email

The System can be configured to send automated emails when certain events occur, such as a database backup, or when an action trigger is executed.

The System includes one predefined email list to which recipients can be added for automated email messages. Up to ten email lists, each of which can contain up to ten recipients, can be created for use with automated emails.

To use the automated email feature, configure the System to use either an internal or external Simple Mail Transfer Protocol (SMTP) server, and add at least one email recipient to the predefined email list.

Configure an Email Server

The System can be configured to access either an internal, enterprise SMTP email server, or an external SMTP server (such as Gmail) to send automated emails.

Check with your Internet Service Provider (ISP) or email service provider to determine the IP address or hostname for the email server, and its port number. Also, ask if the email server uses the Secure Sockets Layer (SSL) protocol to encrypt data.

Note:　　　Some ISP and email service providers limit the amount of emails that can be sent each day and may charge extra for any quantity over that amount. In some cases, a provider will block the account when the maximum quantity is exceeded. If these issues are restrictive, consider using a paid SMTP relay service or hosting an internal email server.

1. Select *System Administration > Email > Server Settings*.
2. Select **Enable Email Notifications**.
3. If connecting to a secure email server, select the **Enable Authentication** check box.
   a. Type the IP address or hostname of the email server in the **Email Server** field.
   b. Type the port number of the email server in the **Port** field.

If the email server uses SSL, the default value is 465; otherwise, the default value is 25.

    c. If the email server uses SSL, select the **Requires SSL** check box.

    d. Type the user name for the email service account in the **User** field.

    e. Type the password for the email service account in the **Password** field.

4. If connecting to an email server that does not require a user name and password, leave the **Enable Authentication** check box unselected.

    a. Type the IP address or hostname of the email server in the **Email Server** field.

    b. Type the port number of the email server in the **Port** field.

    If the email server uses SSL, the default value is 465; otherwise, the default value is 25.

    c. If the email server uses SSL, select the **Requires SSL** check box.

    d. Type the name that will appear on automated emails in the **Sender Name** field.

    e. Type the email address that will appear on automated emails in the **Sender Email** field.

    If recipients should not reply to automated emails, consider creating a "no reply" email account such as "noreply@yourdomainname.com" that can be used as the sender address.

5. Click [Accept Changes].

6. Click [Test Email Server] to check the email server settings.

Modify an Email List

Recipients can be added and removed from an email list, and the name of the list can be changed, as described next. The System includes one predefined email list, to which at least one email recipient must be added for automated emails.

1. Select *System Administration > Email > Email Lists*.

2. Click the email list to select it.

3. To rename an email list, type a descriptive name for the list in the **Email List Name** field.

4. To add a person to the list:

    a. Type the name of the person in the **Display Name** field.

    b. Type the email address of the person in the **Email Address** field.

    c. Click [Add].

5. To remove a person from the list:

    a. Click the name of the person to select it.

    b. Click [Remove].

6. Click [Accept Changes].

Add an Email List

The System includes one predefined email list, to which at least one recipient must be added to support automated emails. Up to ten email lists can be created, each of which can contain up to ten recipients. An existing email list can also be copied and then modified it as necessary.

1. Select *System Administration > Email > Email Lists*.

2. Click [Add].

3. Type a descriptive name for the email list in the **Email List Name** field.

4. For each person being added to the email list:

    a. Click [Add].

    b. Type the name of the person in the **Display Name** field.

    c. Type the email address of the person in the **Email Address** field.

5. When finished adding recipients to the email list, click [Accept Changes].

Remove an Email List

Note: An email list cannot be deleted if it is currently being used by the System.

1. Select *System Administration > Email > Email Lists*.

2. Click the email list to select it.

3. Click [Remove].

The Remove Item dialog box appears.

4. Click [Remove].

Disable Email Notifications

To quickly disable all email notifications, clear the **Enable Email Notifications** check box on the *Server Settings* page. Note, however, that this will impact any action triggers that involve automated emails.

1. Select *System Administration > Email > Server Settings*.

2. Clear the **Enable Email Notifications** check box.

3. Click [Accept Changes].

Configuring User-Defined Fields

Person records in the database can have user-defined fields associated with them that can be used to enter personal data about personnel, such as vehicle license plate number or home telephone number. A field must be enabled to appear on the *Access Management > Persons* page. When a field is disabled, it will be removed from the database, and all data contained in that field for each Person record will be lost.

Every database must have a way to identify one record from another. Since some names are very common, using employee surnames as a unique database record identifier will not work. For this reason, organizations frequently assign each employee or member a unique identification number.

    IMPORTANT: For best results, use a person record identifier, such as an employee number, that is unique to each person in the organization. Without a way to identify each record as unique, then updates, imports, exports and other database maintenance actions may result in changes being made to the wrong record.

When user-defined fields are created, they can be designated as protected. The settings for this option determine whether the user-defined fields with the Protected feature selected are visible or modifiable by various operator roles. This gives an added level of privacy for sensitive information, such as home telephone numbers. For example, if users with the Operator role should be able to view all

personal information and users with the Guard role should be able to view only non-protected personal information, change the operator role settings as shown in the following table:

Role	User-Defined Fields Setting	Protected user Fields Setting
Operator	View Only	View Only
Guard	View Only	None

Add User-Defined Fields

The user-defined fields are part of the Person records in the database. A field must be enabled to appear on the *Access Management > Persons* page.

1. Select *System Administration > System Settings*.
2. Click the **User-Defined Fields** tab.
3. For each field:
    a. Select **Enabled**.
    b. Type a **Label**.
    c. (Optional) Select **Required**.
    d. (Optional) Select **Protected**.
4. Click [Accept Changes].

Rearrange User-Defined Fields

The user-defined fields are part of the Person records in the database. A field must be enabled to appear on the *Access Management > Persons* page. If a field is disabled, it will be removed from the database, and all data contained in that field for each Person record will be lost.

> **IMPORTANT:** Do not edit the field labels in an attempt to rearrange their order. The data is associated with the field, not the field label. Changing the label will not rearrange the order, but will cause the data to be mislabeled.

1. Select *System Administration > System Settings*.
2. Click the **User-Defined Fields** tab.
3. Use the Order arrows to move fields upward or downward.

    The order of fields on this tab matches the order of fields on the *Access Management > Persons* page.

Remove a User-Defined Field

A field must be enabled to appear on the *Access Management > Persons* page. If a field is disabled, it will be removed from the database, and all data contained in that field for each Person record will be lost.

1. Select *System Administration > System Settings*.
2. Click the **User-Defined Fields** tab.
3. Clear the **Enabled** check box for the field and data to be deleted.
4. Click [Accept Changes].

Scheduling Door and Reader Behavior

The Schedule View tab on the *Monitoring > Doors* page is used to override default door and reader behavior according to a schedule. For example, during business hours a public door, such as to a showroom or retail area, may need to remain unlocked. After normal business hours, certain readers can be set to require both a credential and a PIN (useful to prevent access with lost or stolen credential cards) so the reader can be configured to request a credential only by default (*System Administration*

> *Devices*) and request a credential and PIN after business hours (*Monitoring > Doors > Schedule View*).

Note: Do not confuse door and reader behavior with access. The *Access Management > Access Levels* page is used to assign schedules to readers and reader groups. Access levels are then assigned to credentials, determining what days and times a person with that credential can gain entry through the readers in that access level. The mode of access, credential only or credential and PIN, is not relevant to the access level. (See Configuring Security on page 18.)

1. Select *Monitoring > Doors*.

2. Click the **Schedule View** tab.

3. For each door and reader combination:

   a. Select a **Schedule**.

   b. Select a **Schedule Mode**.

   For doors the Schedule Modes are:

   - Unlocked
   - First Card In
   - Locked

   For readers the Schedule Modes are:

   - Credential Only
   - Credential and PIN
   - PIN Only
   - PIN or Credential

Importing Persons and Credentials from a CSV File

The Import/Export Wizard provided on the Utilities disc can be used to add or delete multiple sets of persons and credentials data in batch mode from another source, such as a human resources database or another access control system.

Note: Persons can also have a user account on the System, allowing them to log into and use the System. User account information is not processed by the Import/Export Wizard.

The Import/Export Wizard can be used to map the fields of a CSV file to the System database table, and import persons and credentials data from another source, such as a human resources database or another access control system. Refer to the *Import/Export Wizard User Guide* for details.

Note: A person record consists of user-defined fields for personal information, access credentials (badge ID, PIN, access level) and optional user account information to allow login to the System. Import and export of user account data is not supported. Only user-defined personal data and credential data can be imported and exported.

Person records can also be added individually, as described in Managing Persons on page 65.

Configuring Action Triggers

With the Action Triggers feature, a set of trigger conditions can be defined along with corresponding actions that will be executed when the trigger conditions are satisfied. For example, if an exterior door is forced open between the hours of 7 p.m. and 7 a.m., an action trigger can be executed that will cause sirens to blare, lights to flash, and an automated email to be sent to all site supervisors.

The *System Administration > Action Triggers* page contains two tabs, **Triggers** and **Actions**, as described next.

Understanding Triggers

Use the **Triggers** tab on the *Action Triggers* page to define trigger conditions that will execute actions. A trigger consists of one or more condition groups, and a condition group consists of one or more condition statements.

Each condition statement includes four drop-down list boxes where users can:

- Specify an entity type, such as **Door** or **Schedule**.
- Specify an qualifier related to the selected entity type. If **Door** is selected as the entity type, options in this list box will include **Any**, **All**, and a list of doors defined in the System.
- Specify whether the condition should be true or false.
- Select a condition that would trigger an action. If **Door** is selected as the entity type, options include **Secure**, **Unlocked**, **Locked Out**, **Held Open**, **Forced Open**, **Tampered**, **Open**, and **Mag Sensor Trouble**.

The following table lists available trigger conditions for each entity type:

Trigger conditions	Notes
Entity: Area	
Unlocked - Any Door	A door belongs to an area if either of its readers is configured to enter or exit the area on the ***Access Management > Areas > Reader Assignments*** page. The one exception is "Locked Out – Any Door", which only considers readers that enter the selected area.
Locked Out - Any Door	
Held Open - Any Door	
Forced Open - Any Door	
Tampered - Any Door	Becomes true when doors in the area meet the condition. Becomes false when doors do not meet the condition. Outside areas are not supported. See corresponding door trigger for condition details.
Open - Any Door	
Secure - All Doors	
Mag Sensor Trouble - Any Door	If an area is not associated with any doors, the "Any Doors" conditions will always be false, and the "All Doors" conditions always be true.
Entity: Door	
Unlocked	Becomes true when door strike is activated. Becomes false when door strike is deactivated.
Locked Out	Becomes true when door is locked out. Becomes false when door lockout is no longer active

Trigger conditions	Notes
Held Open	Becomes true when door held open alarm is active. Becomes false when door held open alarm is restored.
Forced Open	Becomes true when door forced open alarm is active. Becomes false when door forced open alarm is restored.
Tamper	Becomes true when door tamper alarm is active. Becomes false when door tamper alarm is restored. Includes tamper on Door Contact, Request to Exit, Auxiliary Input, and Tamper.
Open	Becomes true when door is open. Becomes false when door is closed. Includes door forced and held open conditions.
Secure	Becomes true when door strike is inactive and door is closed. Becomes false when door strike is active or door is open.
Mag Sensor Trouble	Becomes true when mag sensor alarm is active. Becomes false when mag sensor alarm is restored.
Entity: Input	
Inactive	Becomes true when input is inactive. Becomes false when input is not inactive.
Active	Becomes true when input is active. Trigger false when input is not active.
Tampered	Becomes true when input is tampered. Trigger false when input is not tampered.
Entity: Output	
On	Becomes true when output is on. Trigger false when input is not on.
Off	Becomes true when output is off. Trigger false when input is not off.
Entity: Module	
Tampered	Becomes true when peripheral reports tamper condition. Becomes false when peripheral reports tamper conditions restored.
Communications Error	Becomes true when communications with peripheral is lost. Becomes false when communications is restored.
Entity: Reader	
Granted	Becomes true/false for any type of access granted event. Will be followed by another access granted event.
Granted - No Entry	Becomes true/false when door is not opened and no APB violation occurs.

Trigger conditions	Notes
Granted - Entry Made	Becomes true when door is opened and reader leads to non-outside area.
Granted - Entry Made Soft APB	Becomes true/false if door is opened and reader leads to non-outside area and soft APB violation.
Granted - No Entry Soft APB	Becomes true/false if the door is not opened, and the reader leads to a non-outside area with a soft APB violation.
Granted - Egress Made	Becomes true/false if the door is opened, and the reader leads to an outside area with no APB violation.
Granted - Egress Made Soft APB	Becomes true/false if the door is opened, and the reader leads to an outside area with a soft APB violation.
Granted - No Egress Soft APB	Becomes true/false if the door is not opened, and the reader leads to an outside area with a soft APB violation.
Denied - Any Reason	Becomes true/false when access is denied for any reason.
Denied - Invalid Credential	Becomes true/false when accessed is denied due to unknown credential.
Denied - Facility Code	Becomes true/false when access is denied due to invalid facility code.
Denied - Issue Code	Becomes true/false when access is denied due to invalid issue code.
Denied - PIN	Becomes true/false when access is denied due to invalid PIN. There is no explicit trigger for when the max invalid PIN attempts are reached and cardholder is locked out.
Denied - Unauthorized	Becomes true/false when access is denied due to no access level.
Denied - Hard APB	Becomes true/false when access is denied due to hard APB violation
Denied - Door Locked Out	Becomes true/false when access is denied due to door locked out.
Denied - Inactive	Becomes true/false when access is denied due to credential active from/to out of range.
Entity: Schedule	
In Effect	Becomes true when schedule starts. Becomes false when schedule ends.
Holiday In Effect	Becomes true when a schedule is not in effect because of a holiday. (The times of day that the trigger is active is based on the schedule.) Becomes false when the holiday ends. See Considerations for Schedule-Based Action Trigger Records on page 55.

Trigger conditions	Notes
15 Minutes Before Start	Becomes true when 15 minutes prior to schedule start. Becomes false when schedule starts.
15 Minutes Before End	Becomes true when 15 minutes prior to schedule end. Becomes false when schedule ends.
Entity: System	
Lockout All Doors - Command	Becomes true when lockout goes active. Becomes false when lockout is no longer active.
Unlock All Doors - Command	Becomes true when unlock goes active. Becomes false when unlock is no longer active.
Trouble	Becomes true when External/Wall Tamper goes active. Becomes false when tamper condition goes inactive.
Backup Battery Low	Becomes true when battery voltage drops below 11.7 VDC. Becomes false when battery voltage goes above 11.7 VDC.
Memory Battery Low	Becomes true when battery voltage drops below 2.0 VDC. Becomes false when battery voltage goes above 2.0 VDC. Only checked every 6 hours.
AC Power Failed	Becomes true when AC power is removed. Becomes false when AC power is restored.
Fuse Tripped	Becomes true when any fuse trips. Becomes false when all fuses are restored.
Time Changed	Becomes true when time is changed. Will not rearm for one minute. Automatically becomes false after one minute.

Note the following details about triggers:

- Up to ten groups of condition statements can be created, with up to ten condition statements across all groups (for example, two groups could have five conditions each).

- To start a new group of condition statements, click the [+] button that appears above the condition statements in an existing group. Click the [-] button to remove a group of condition statements.

- A second level of [+] and [-] buttons appears next to each individual condition statement. Click the [+] button to add a new condition statement; click the [-] button to remove a single condition statement.

- For either one specific group of condition statements or for all groups of condition statements, **Any Can Occur** or **All Must Occur** can be selected.

- If **Any** or **All** is selected as the qualifier for an entity in a condition statement, any new objects added to the System of the same entity type are automatically included in the condition evaluation. For example, if condition statement is created to monitor all readers and a new reader is installed, the new reader is added to the group of readers being monitored automatically.

- The trigger conditions for readers will always trigger false immediately after triggering true. Also, deactivation actions are not typically used with reader trigger conditions.

- If a system entity (for example, a reader) is defined in a condition statement and then the entity is deleted from the System, the corresponding condition statement will also be deleted. If the entity is recreated, a new condition statement can be created for the entity.
- An event is logged whenever a trigger condition statement changes state between true and false.
- Duplicate condition statements can be included in the same condition group.
- Disabled inputs and outputs can be included in a trigger statement, but they will have no effect on the trigger evaluation.
- Action trigger records can be configured to occur when a trigger is deactivated.
- Action trigger records can include trigger conditions without any resulting actions.

In addition, note that trigger conditions are assumed to be in an indeterminate state and will transition to either true or false to execute the corresponding actions:

- For all records when the System starts up.
- For each record when a record is configured and saved.
- For affected records when a referenced entity is deleted.

Considerations for Schedule-Based Action Trigger Records

When creating condition statements for action trigger records that involve schedules, remember that Holiday Groups can be either included or excluded from a schedule, depending on how the Holiday Group is configured for the schedule on the *Access Management > Schedules* page.

- If a Holiday Group is *included* in a schedule (i.e. the check box is selected), then the schedule will be active on the days defined in the Holiday Group for the hours defined in the schedule. This is regardless of what days of the week are selected for the schedule.
- If a Holiday Group check box is *excluded* from a schedule (i.e. the check box is cleared), then the schedule will not be active at any time during the days defined in the Holiday Group. This is regardless of what days of the week are selected for the schedule.
- If the same day is part of one Holiday Group that is *included* in a schedule and is also part of another Holiday Group that is *excluded* from the same schedule, the day will be *included* in the schedule.

To guarantee that an action will be triggered regardless of whether or not a day is a holiday, create an "or" statement with the trigger conditions by using the "Any Can Occur" option. For example, add one trigger condition that will be true when a Weekdays 9AM - 6PM schedule is in effect, and a matching trigger condition will be true when holidays are in effect.

The following example shows when a Holiday in Effect trigger is active if a holiday negatively impacts a schedule for a Weekdays 7AM - 7PM schedule:

	Wed. 2/13 7AM - 7PM	Thu. 2/14 7AM - 7PM	Fri. 2/15 7AM - 7PM	Sat. 2/16 7AM - 7PM	Sun. 2/17 7AM - 7PM	Mon. 2/18 7AM - 7PM	Tues. 2/19 7AM - 7PM
No holidays defined							
In Window	Active	Active	Active			Active	Active
Holiday in Effect							
Holiday 1 (2/14-2/16) check box is cleared							
Holiday 2 (2/15-2/18) check box is cleared							
In Window	Active						Active
Holiday in Effect		Active	Active			Active	
Holiday 1 (2/14-2/16) check box is selected							
Holiday 2 (2/15-2/18) check box is cleared							
In Window	Active	Active	Active	Active			Active
Holiday in Effect						Active	

Understanding Actions

Use the **Actions** tab on the *System Administration > Action Triggers* page to define the actions that will be executed when a trigger condition becomes true or false. (Action triggers can also be executed on the *Monitoring > Action Triggers* page. See)

For example, a condition statement can be defined on the Triggers tab to specify that an action will occur if any door is forced open. An action can then be configured on the Actions tab that when the condition statement becomes true, an automated email will be sent out to all supervisors. If a door is forced open after this action trigger record is created, an automated email will be sent to all on-site supervisors.

Up to 32 action trigger records can be created to result in two types of actions:

• Activation actions are executed when a trigger condition becomes true, and
• Deactivation actions are executed when a trigger condition becomes false.

Multiple action trigger records can be configured to execute the same action, or control the same system entity. For example, a record can be configured to turn on a siren output and send an automated email when any of several emergency inputs go active, and another record can be configured to turn the siren off and send email when the emergency reset goes active.

The following table lists available actions:

Actions	Notes
Entity: System Controller	
Reset APB	Resets anti-passback of all credentials to a neutral state (i.e free pass).
Entity: Doors / Readers	
Lock	Locks door. **Note:** Does not affect reader access mode.
Unlock	Unlocks door. **Note:** Does not affect reader access mode.
Open	Unlocks door strike for normal grant access time. **Note:** Does not affect reader access mode.
Open Extended	Unlocks door strike for extended grant access time. **Note:** Does not affect reader access mode.
First Card In	Sets door mode to "Pending First User".
Aux Relay On	Turns on door aux relay.
Aux Relay Off	Turns off door aux relay.
Door Buzzer On	Turns on door buzzer output. **Note:** IPSDCs do not support this action.
Door Buzzer Off	Turns off door buzzer output. **Note:** IPSDCs do not support this action.
Lockout Door	Lockout door (affects strike and in/out readers).
Reinstate Door	Reinstate door (affects strike and in/out readers).
Card+PIN - In Reader	Sets reader to "Credential and PIN" access mode. **Note:** Does not affect door strike.
Card+PIN - Out Reader	Sets reader to "Credential and PIN" access mode. **Note:** Does not affect door strike.
Card+PIN - In/Out Readers	Sets reader to "Credential and PIN" access mode. **Note:** Does not affect door strike.
Card Only - In Reader	Sets reader to "Credential Only" access mode. **Note:** Does not affect door strike.
Card Only - Out Reader	Sets reader to "Credential Only" access mode. **Note:** Does not affect door strike.
Card Only - In/Out Readers	Sets reader to "Credential Only" access mode. **Note:** Does not affect door strike.
PIN Only - In Reader	Sets reader to "PIN Only" access mode. **Note:** Does not affect door strike.

Actions	Notes
PIN Only - Out Reader	Sets reader to "PIN Only" access mode. **Note:** Does not affect door strike.
PIN Only - In/Out Readers	Sets reader to "PIN Only" access mode. **Note:** Does not affect door strike.
PIN or Card - In Reader	Sets reader to "PIN or Credential" access mode. **Note:** Does not affect door strike.
PIN or Card - Out Reader	Sets reader to "PIN or Credential" access mode. **Note:** Does not affect door strike.
PIN or Card - In/Out Readers	Sets reader to "PIN or Credential" access mode. **Note:** Does not affect door strike.
Entity: Output	
On	Turns output on.
Off	Turns output off.
Pulse On	Pulses output on, then back to off, for the selected duration. **Note:** The accuracy of pulse duration varies depending on the pulse length. See Pulse Duration Accuracy on page 115.
Pulse Off	Pulses output off, then back to on, for the selected duration. **Note:** The accuracy of pulse duration varies depending on the pulse length. See Pulse Duration Accuracy on page 115.
Entity: Area	
Reset APB	Resets APB of all credentials that are in areas to neutral (i.e free pass).
Unlock - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Lock - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Aux Relay On - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Aux Relay Off - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Buzzer On - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area. Note: IPSDCs do not support this action.

Actions	Notes
Buzzer Off - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area. Note: IPSDCs do not support this action.
First Card In - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Lockout - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Reinstate - Doors	See corresponding door command. Affects all doors with in or out readers associated with the area.
Credential and PIN - Entry Readers	See corresponding door command. Affects all readers that can enter the area.
Credential and PIN - Exit Readers	See corresponding door command. Affects all readers that can exit the area.
Credential and PIN - All Readers	See corresponding door command. Affects all readers that can enter or exit the area.
Credential Only - Entry Readers	See corresponding door command. Affects all readers that can enter the area.
Credential Only - Exit Readers	See corresponding door command. Affects all readers that can exit the area.
Credential Only - All Readers	See corresponding door command. Affects all readers hat can enter or exit the area.
PIN Only - Entry Readers	See corresponding door command. Affects all readers that can enter the area.
PIN Only - Exit Readers	See corresponding door command. Affects all readers that can exit the area.
PIN Only - All Readers	See corresponding door command. Affects all readers hat can enter or exit the area.
PIN or Credential - Entry Readers	See corresponding door command. Affects all readers that can enter the area.
PIN or Credential - Exit Readers	See corresponding door command. Affects all readers that can exit the area.
PIN or Credential - All Readers	See corresponding door command. Affects all readers hat can enter or exit the area.
Entity: Email Notification	
Send Email	See explicit requirement below.

Note the following details about action trigger records:

- Up to 10 actions can be included per action trigger record. These actions can be any combination of activation and/or deactivation actions.
- Actions can be configured to occur when a trigger is deactivated.
- Use the **Status** field on the top of the *System Administration > Action Triggers* page to enable or disable action trigger records.
- Action triggers can be executed manually on the *Monitoring > Action Triggers* page. See Controlling Action Triggers on page 84.

Note: To provide a quick way to secure all doors in a facility, create an action trigger record to lock all doors, and then trigger it manually on the *Monitoring > Action Triggers* page when necessary.

- Disabled inputs and outputs can be included as an action, but they will have not be implemented until the input or output is enabled.
- Action triggers, schedules, and manual control can all impact the state of devices and are treated equally by the System. The last operation executed determines the state of a device.
- Action triggers do not override the global "Lockout All Doors" or "Unlock All Doors" door states.
- If an entity (for example, a reader) is defined in an action trigger record and then the entity is deleted from the System, all corresponding action trigger records will also be deleted. If the entity is recreated, new action trigger records can be created for the entity.
- If the System is configured to send automated emails, an action trigger record can be created to send a notification to an email list when a trigger condition changes. Email delivery will be attempted for the selected Retry Limit duration relative to when the action was triggered.
- IPSDCs do not support Buzzer On and Buzzer Off actions.
- If an action trigger is directed to an entity whose parent module is offline, the action will have no effect on that entity when the module comes back online. In other words, actions are not persisted or queued.
- Output actions will not log an Output On or Output Off event unless the output physically changes state. For example, if an output is on and action trigger occurs to turn that output on, there will be no Output On event generated.

In addition, note that trigger conditions are assumed to be in an indeterminate state and will transition to either true or false to execute the corresponding actions:

- For all records when the System starts up.
- For each record when a record is configured and saved.
- For affected records when a referenced entity is deleted.

Add an Action Trigger Record

1. Select *System Administration > Action Triggers*.

2. Click [Add].

3. Type a descriptive name for the record, up to 64 characters long, in the **Action Trigger Name** field.

4. Select values in the four drop-down list boxes to create the first condition statement that will trigger an action.

5. To create additional condition statements in the same group:

   a. Click the [+] button on the same line as the last condition statement.

   b. Select values in the four drop-down list boxes.

   c. Repeat step a and step b for each new condition statement.

   d. If necessary, click the [-] button to remove a condition statement.

6. To create a new group of condition statements, click the [+] button that appears on the same line as the **Any Can Occur** drop-down list box.

7. Adjust the **Any Can Occur** drop-down list boxes to create logical operators (i.e., AND/OR statements) for the condition statements in each group.

8. Click [Accept Changes].

9. Next, click [Actions] to configure the action(s) that will occur when any or all (depending on how triggers are configured) condition statements are true.

   The Actions tab includes two sections: Activation Actions and Deactivation Actions. Actions can be added to either or both of these sections, as necessary.

10. To add System, Area, Output, or Door actions:

    a. Click [Add] beneath the Activation Actions or Deactivation Actions section.

    b. Select the type of action being added.

    c. In the Configure Actions dialog box, select each entity and the action that will occur.

    d. Click [Ok] to close the Configure Actions dialog box.

11. To add Email actions:

Note: Avoid adding large quantities of Email actions to avoid "spamming" recipients.

    a. Click [Add] beneath the Activation Actions or Deactivation Actions section.

    b. Select **Email Actions**.

    c. In the Configure Actions dialog box, select each email distribution list to which a message will be sent when a trigger condition changes. Messages can also be sent to all lists.

    d. Type the **Email Text**.

    e. Select a **Retry Timeout** value. If the initial email fails due to a connection error, the System will try to send the message again, doubling the length of time between each attempt until the Retry Timeout value is reached.

    f. Click [Ok] to close the Configure Actions dialog box.

12. Click [Accept Changes].

Copy an Action Trigger Record

1. Select *System Administration > Action Triggers*.
2. Click the action trigger record to select it.
3. Click [Copy].
4. Edit the record, as necessary.
5. Click [Accept Changes].

Remove an Action Trigger Record

1. Select *System Administration > Action Triggers*.
2. Click the action trigger record to select it.
3. Click [Remove].

   The Remove Item dialog box appears.
4. Click [Remove].

Configuring a Network Share

As described in Backing Up Data on page 87, backups can be scheduled to occur automatically and the resulting backup file will be sent to a shared network resource, known as a *network share*.

Network shares can be configured for a network folder, or for a remote file system that uses one of the following communications protocols:

- File Transfer Protocol (FTP)
- File Transfer Protocol Secure (FTPS)
- Common Internet File System (CIFS)

Add a Network Share

To configure a network share for scheduled backups:

1. Select *System Administration > Network Share*.
2. Click [Add].
3. Select a communications protocol in the **Protocol** field to connect to a remote file system, or select *None* to use a network folder.

   Note: As data is entered in the fields on the page, the **Share Name** field will change to reflect the new information.

4. If FTP or FTPS was selected in step 3, type the port number of the connection in the **Port** field.
5. Type the IP address or hostname of the network share in the **Host** field.
6. Type the directory location of the network share in the **Host** field.
7. If a remote file system protocol was selected in step 3, type the user name needed to log into the system in the **User** field.
8. If a remote file system protocol was selected in step 3, type the password needed to log into system in the **Password** field.
9. Click [Accept Changes].

Copy a Network Share

1. Select *System Administration > Network Share*.

2. Click the network share to select it.

3. Click [Copy].

4. Edit the network share, as necessary.

5. Click [Accept Changes].

Remove a Network Share

1. Select *System Administration > Network Share*.

2. Click the network share to select it.

3. Click [Remove].

The Remove Item dialog box appears.

4. Click [Remove].

Creating a Backup and Restore Point

After configuring the System, it is important to:

• Create a backup file that includes all records, photos, and settings configured in the System. See Backing Up Data on page 87.

• Create a restore point that includes all of the data normally saved in a backup file, plus the custom settings of the System Controller. This information will be saved on the System Controller and can be restored later to return the System to its initial operating state. See Saving and Restoring Custom Settings on page 89.

Managing Access

Access to a facility and the User Interface can be managed by:

- Adding and removing persons,
- Adding, deactivating, reactivating, and removing credentials, and
- Adding and removing user accounts.

Managing Persons

Each individual in an organization can have access to the building and access to the System. Access to the physical facility is controlled by means of a credential (commonly called an ID badge). Access to the System is controlled by means of a user account to log into the System Controller. To keep the user accounts and credentials organized, the System associates both with one record for each individual in an organization. This individual database record is called a "person" because it corresponds to an actual person.

The distinction between persons, credentials, and user accounts is important. First, everyone who needs to enter a facility will need a credential (an ID badge with an encoded number that is recognized by the System). However, not everyone who needs access to the facility will also need access to the System with a user account. Second, only those who operate and manage the System will need user accounts. Third, in some cases, operators are located off-site at a central station and therefore do not require a credential to access the physical facility even though they have a user account.

The database records, "persons," allow users to conveniently manage credentials and user accounts from one record, rather than maintaining separate databases for system users and facility access credentials.

Add a Person

Before adding person records, be sure to:

- Assign each person record a unique identification number of some kind. This may be an employee number, for example.

- Add any necessary user-defined fields that can be used to enter personal data about personnel, such as vehicle license plate number or home telephone number. See Configuring User-Defined Fields on page 47.

There are several ways to add person records:

- By using the *Access Management > Persons* page, as described next.
- By using the adding Add Person Wizard available on the *Home* page.
- By using the Import/Export Wizard provided on the Utilities disc to import person records and credential data that already exists in CSV format (for example, if such data was exported from another access control system or employee database). Refer to the *Import/Export Wizard User Guide* for details.
- By using the optional Learn-In Reader. See Using an Enrollment Reader on page 68.
- By using the link in an event generated when an unknown person attempts access.

To add person records on the *Access Management > Persons* page:

1. Click *Access Management > Persons*.
2. Click [Add].
3. Type a **First Name** and a **Last Name**.
4. Click the **Details** tab.
5. Type the requested information in the user-defined fields.
6. If the person will use the System software, click the **User Account** tab and create the account. See Add a User Account on page 70.
7. Click [Accept Changes].
8. If the person requires a credential for access to the physical facility, see Add a Credential on page 68.

Remove a Person

The System can store up to 10,000 person records. However, persons no longer requiring access to a site or to the System should be removed from the database.

Note: To remove a number of persons in one batch, use the Import/Export Wizard provided on the Utilities disc.

1. Click *Access Management > Persons*.
2. Select the Person from the list of persons.
3. Click [Remove].

   The Remove Item dialog box appears.
4. Click [Remove].

Upload a Person ID Photo

Persons can have an identification photo associated with their records. A thumbnail of this photo will appear whenever an access event occurs involving that person's credential.

Note the following details about uploading photos:

- Supported file formats include GIF, JPG, and PNG.
- Photos up to 200 KB in size can be uploaded, but will be automatically resized to 10 KB or less, in JPG format.

- Total photo storage is limited to 40 MB.
- If larger photos are uploaded, the 40 MB maximum may be exhausted before the capacity of 10,000 is reached.

To upload a photo:

1. Click *Access Management > Persons*.
2. Select the Person from the list of persons.
3. Click the ID Photo icon next to the person's name.

   The Upload Photo dialog box appears.
4. Click **Select File**.

   The Select File dialog box appears.
5. Select a photo to upload and click **Open**.
6. Click **Upload**.
7. The Select File dialog box disappears.
8. Click [Accept Changes].

Note: To update an existing photo, click the existing photo and repeat these steps.

Remove a Person ID Photo

1. Click *Access Management > Persons*.
2. Select the Person from the list of persons.
3. Click the ID Photo icon next to the person's name.

   The Upload Photo dialog box appears.
4. Click **Remove**.
5. When the confirmation message appears, click **Remove**.

Managing Credentials

Every person who needs to enter a facility will need a credential (i.e., an ID badge with an encoded number that is recognized by the System). Before assigning a credential, add the person to the database. See Add a Person on page 65.

Note: Whenever credentials are changed or deleted, the local cache on IPSDCs is cleared to prevent unauthorized access in case IPSDCU Fallback Mode is being used. See IPSDCU Fallback Mode on page 19.

Using an Enrollment Reader

The optional enrollment reader (TP-RDR-LRN) can be connected with a local client workstation and then used to read credentials. The credential data will be automatically inserted into the **Credential ID** field on the *Access Management > Persons* page. This device can save time if numerous credentials are being added.

Install and configure the reader on the local client workstation according to the manufacturer's instructions, which are available online at www.rfideas.com. Download the pcProx Configuration Utility, which includes documentation for the pcProx Plus reader (i.e., the TP-RDR-LRN).

Note the following details about configuring the enrollment reader:

- If using credentials with a facility code, configure the reader to separate the facility code from the credential code on the badge.
- The pcProx Configuration Utility uses .hwg files to configure the enrollment reader. Use the Casi_card.hwg configuration file to recognize CASI Prox badges.

Add a Credential

Before adding a credential to a person, first create a record for that person. See Add a Person on page 65.

1.   Select *Access Management > Persons*.
2.   Select the Person needing the credential.
3.   Click [Credentials].
4.   Click [Add Credential].
5.   Click the **General** tab.
6.   Type the **Credential ID**.

     If the optional enrollment reader is attached to the local client workstation, click inside the **Credential ID** field and then swipe the person's badge card through the reader to populate the field.

7.   (Optional) Type the **PIN** code.

Note: Use a pound sign (#) at the end of each PIN, especially if the PIN length is less than the **Max PIN Length** defined on the Security tab of the *System Administration > System Settings* page. Pound signs are required for PINs used on devices connected to IPSDCs.

8.   (Optional) Select **Use extended strike/held times** if the person with this credential needs extra time to open and pass through doors.
9.   (Optional) Select **Anti-Passback Exempt** if using anti-passback and this credential is not to be tracked.

10. (Optional) Select an **Active From** and **Active To** date if the credential has a limited duration for its validity.

11. Click the **Access Levels** tab.

12. Select the Access Levels that apply to this credential.

13. Click [Accept Changes].

A credential may also be added using the link in an event generated when an invalid credential is used to attempt access.

Remove a Credential

A credential does not need to be removed to prevent its use. For example, if an individual reports a lost credential, rather than delete the credential right away, it can be deactivated until such time as the individual has had time to search for it. If the credential cannot be found, then, when the individual requests a new credential, the lost credential can be removed. See Prevent Use of a Lost or Stolen Credential on page 69.

1. Select *Access Management > Persons*.

2. Select the Person with the credential to be deleted.

3. Click [Credentials].

4. Click the credential to be deleted.

5. Click [Remove Credential].

6. Click [Remove].

7. When the Remove Item dialog box appears, click [Remove].

Managing Lost or Stolen Credentials

If an individual reports a lost credential, rather than delete the credential right away, it can be deactivated until such time as the individual has had time to search for it. If the credential cannot be found, then, when the individual requests a new credential, the lost credential can be removed.

There is an added advantage to deactivating a credential. While any invalid credential scanned at a reader will generate an event, if the credential is still assigned to a person, then the event will specifically indicate that person as trying to use an invalid credential. If video cameras are monitoring door and reader events, an image of the person who attempted to use the credential after it was reported stolen will exist. Searching the Events database for the person who lost the credential will show all incidents associated with that person before and after the credential was reported lost. This is a way to establish an association between the theft victim and the perpetrator.

Prevent Use of a Lost or Stolen Credential

Use this task to deactivate a credential instead of removing it.

1. Select *Access Management > Persons*.

2. Select the Person with the credential to be deactivated.

3. Click [Credentials].

4. Click the credential to be deactivated.

5. Click the **Active To** field.

   The Calendar popup window appears.

6. Select a date in the past.

7. Click [Accept Changes].

Restore a Found Credential

1. Select *Access Management > Persons*.

2. Select the Person with the credential to be deactivated.

3. Click [Credentials].

4. Click the credential to be reactivated.

5. Clear the **Active To** field.

6. Click [Accept Changes].

Managing User Accounts

User accounts allow people to log into the System. A user account is associated with a person database record, just as a credential is. However, a person does not need to have a user account in order to have access to the facility with a credential.

Add a User Account

Before adding a user account for a person, first create a record for that person. See Add a Person on page 65.

1. Log in as an Administrator or Dealer. (The other operator roles do not have permission to modify user accounts.)

2. Select *Access Management > Persons*.

3. Select the person to modify.

4. Click the **User Account** tab.

5. Select **Can log on**.

6. Type a **User Name**.

7. Click [Set Password].

8. Type the new password in the **Enter new password** and **Confirm password** fields.

9. Click [OK].

10. Select a **Role**.

11. Click [Accept Changes].

Change a User Name and Password

1. Log in as an Administrator or Dealer. (The other operator roles do not have permission to modify user accounts.)

2. Select *Access Management > Persons*.

3. Select the person to modify.

4. Click the **User Account** tab.

5. Type a new **User Name**.

6. Click [Set Password].

7. Type the new password in the **Enter new password** and **Confirm password** fields.

8. Click [OK].

9. Click [Accept Changes].

Deactivate a User Account

1. Login as an Administrator or Dealer. (The other operator roles do not have permission to modify user accounts.)

2. Select *Access Management > Persons.*

3. Select the person to modify.

4. Click the **User Account** tab.

5. Clear the **Can log on** check box.

6. Click [Accept Changes].

Creating Reports

Five pre-defined reports allow users to view information stored in the server database:

Access History
A summary of access attempts by person, filtered by Date Range, Person Name (wildcard), Reader, Area, and Grant or Deny response.

Credential
A list of credentials assigned, filtered by Person Name (wildcard), Credential ID (wildcard), Access Levels, and Active or Inactive status.

Reader Access
A list of Persons with access to each reader, filtered by Person Name (wildcard) and Reader.

Roll Call
A list of Persons by current area or last reader, filtered by Person Name (wildcard), Reader, Area, and events. Select **Include "Access/Egress Granted - No Entry" events** to include events that occurred when access or egress was granted, but whether or not access or egress actually occurred cannot be determined.

Roster
A list of all Persons in the database, filtered by Person Name (wildcard) and Login privileges.

Note the following details about reports:

- Reports are displayed in HTML format, in an Internet browser window. If using Internet Explorer 7 or earlier, the product logo in the upper right corner will not display properly. This is a limitation of older versions of Internet Explorer.

- If entity names (e.g., device names, person names) change, the updated entity name will be reflected in the next report.

Create a Report

1. Select *Reports*.
2. Select the type of report to create.
3. Fill out the report-specific fields, as desired.
4. Click [View] to display the report in a new browser window.
5. To export a report:
   a. Click [Export].
   b. When prompted, click [Save].
   c. In the dialog box that appears, navigate to the location where the report will be saved in CSV format.
   d. Click [Save].

Note: If the "Generating reports" notification continues to appear and the main User Interface dims, the local client workstation may be low on memory. Close the browser window to end the session, close open programs that are not currently needed, log back in, and try to create the report again.

Searching for Persons

The Search feature filters the database by listing those person records with a field matching all or part of the search query.

Search Persons

1. Select *Access Management > Persons*.
2. Click [Search] and select a field to search.

   The [Search] button appears next to the Search text box and looks like a magnifying glass. When it is clicked, a list of fields that can be searched drops down beneath the button.
3. Type the search term.
4. Press <Enter>.

Cancel a Search

The Search results will continue to filter the database, even if a user navigates to another page and returns to the *Persons* page, until the search is cancelled.

1. Select *Access Management > Persons*.
2. Click the **X** to clear the search field.

CHAPTER 6   *Monitoring Access*

During day to day operations, facility access can be monitored and controlled by:

• Viewing events.
• Watching security camera video, if cameras were installed.
• Overriding scheduled door behavior to open, unlock, lock out, reinstate, or secure doors.
• Responding to alarms.

Monitoring Events and Alarms

The *Events* page provides a record of:

- Access issues
  - Unauthorized access
  - Anti-passback violations
  - Doors held open too long
  - Users logging into the System
- System and device status messages
  - Changes in system state, such as updates to the date and time
  - Mode changes for devices
  - Changes in the state of action triggers
  - Database and event backups
- Alarms
  - Door tampering
  - Doors forced open
  - System failures or problems

Note the following details about the *Events* page:

- Any event associated with a device linked to a camera will have a video record of the event.
- To sort events, click a column header.
- The *Events* page will auto-scroll when new events are generated if the list is sorted by Date and Time with the most recent event at the top, and the list is showing the previous new event at the top (i.e., the list is scrolled all the way to the top).
- Click a device in the Device column to access the *Monitoring > Doors* page and display details about a device.

Click an event to display a detail pane that shows the date and time of the event, along with a description of the event. Additional event information is provided, depending on whether the event is person-related (for example, Access Granted) or device-specific (for example, Door Unlocked):

- For person-related events, the detail pane will also include the person's name, credential, and photo, if available. Double-click a photo to access the *Access Management > Persons* page and display details about the individual.
- For device-specific events, the detail pane will include an event description, date, time, device information, and event-related video, if available.

Click [Close] on the detail pane when finished reviewing event information.

View Latest Events

The latest events are displayed at the bottom left corner of the page. If an event occurs while you are working on another page, a summary of the event, including a thumbnail photo of the person associated with the event, can be displayed by moving the mouse cursor over the event.

The popup window will display the date and time of the event, a description of the event, and the credential. Below that will appear the person's photo and name.

Load More Events

The *Events* page displays the most recent events. To view older events than those displayed, load them to the browser from the System first. The Load More Events command will load the next 500 events (or fewer, if there are less than 500).

1. Select *Events*.
2. Click the circular [Events] action button.
3. Select **Load More Events**.
4. (Optional) To stop the operation, click **Cancel** when it appears.

Load All Events

The *Events* page displays the most recent events. To view older events than those displayed, load them to the browser from the System first. The Load All Events command will load all of the events on the System Controller to the browser, and may take several minutes to complete.

1. Select *Events*.
2. Click the circular [Events] action button.
3. Select **Load More Events**.
4. (Optional) To stop the operation, click **Cancel** when it appears.

Search for Events

Use the search feature to filter the list of displayed events by one or more facets.

1. Select **Events**.
2. Click the **Filter** icon at the right of the page.
3. Type search criteria in the appropriate fields.

    The more criteria used, the narrower the search results will be.
4. Press <Enter>.

Export Events

The System can store up to 65,535 events. Once this limit is reached, older events are deleted as needed to make room. Use the Export Events command to store a record of events in a comma-separated-values (CSV) format file.

1. Select *Events*.
2. Click the circular [Events] action button.
3. Select **Export Events**.
4. Choose the location on the client workstation where the file will be saved.
5. Type a descriptive filename with the extension .**csv**.
6. Click **Save**.

Monitoring Video of Events

The System can display the live or recorded video from specific cameras, and associate recorded video with events at specific devices, such as readers and doors. (See Configuring Video Devices on page 33.)

Links to event-specific video are found on the *Events* page. Use the *Monitoring > Video* page to monitor the video feed from one or more cameras. Video clips of live or recorded video can be downloaded to a local client workstation.

Before You Begin

Before playing video on either the *Events* or *Monitoring > Video* page, make sure that the security settings for Internet Explorer are set properly, as described next.

1. Open Internet Explorer.

2. On the Tools menu, click **Internet options**.

3. Switch to the Security tab and click [Custom level...].

Note: If the **Custom level...** button is not enabled, network security policies may be in place to prevent users from changing Internet Explorer settings. Contact the network administrator or run Internet Explorer as an administrator.

4. Scroll down the Security Settings list to display the ActiveX controls and plug-ins settings.

5. For Automatic prompting for ActiveX controls, click **Enable**.

6. For Download signed ActiveX controls, click **Enable** or **Prompt**.

7. For Initialize and script ActiveX controls not marked as safe for scripting, click **Enable** or **Prompt**.

8. For Run ActiveX controls and plug-ins, click **Enable** or **Prompt.**

9. For Script ActiveX controls marked safe for scripting, click **Enable** or **Prompt**.

10. Scroll down the Security Settings list to display the Miscellaneous settings.

11. For Active scripting, click **Enable** or **Prompt**.

12. Scroll down the Security Settings list to display the Scripting settings.

13. For Use Pop-up Blocker, click **Disable**.

14. Click **OK**, and then click **OK** again to save the settings.

Also, the first time video is accessed, a message will appear to indicate that a proprietary video player must be installed. Click [Download and Install] to install the software. (If network security policies block the download, contact the network administrator or run Internet Explorer as an administrator.) After a message appears to indicate that the video player was installed successfully, log out of the System and then log back in to access video.

IMPORTANT: Existing TruPortal 1.0 or goEntry 3.0 users must uninstall (if applicable) the current version of the TruPortal ActiveX Control via the *Control Panel > Programs and Features > Uninstall a Program* option before installing the updated proprietary video player.

Replay Event Video

Events with associated recorded video will have a hyper-linked camera icon (▣) next to the Event Description on the **Events** page.

1. Select *Events*.

2. Scroll to or search for the event.

3. Click the **Camera** icon that appears next to the Event Description.

   The Event Detail pane appears at the bottom of the page, along with a video frame.

4. Click [Play Event Video].

5. Hover over the bottom of the video frame to display controls that can be used to play and record video. See Video Controls Reference on page 78.

Monitor Video

While the *Events* page displays recorded video of events linked to specific devices, the *Monitoring > Video* page lets users monitor overall site security. For example, if a suspicious person is lurking in the parking lot, this would not trigger a door or reader event, but if a camera is watching the parking lot, the person could be detected by a user watching that camera.

Note: Before live or recorded video can be monitored, add at least one video layout. See Add Video Layouts on page 35.

To monitor video:

1. Select *Monitoring > Video*.

Note: If a message appears to indicate that the video player needs to be installed, click [Download and Install]. When installation is complete, log out and then log back in to play event video. See Before You Begin on page 76 for details.

2. Select a **Layout**.

3. To view live video, click [Live].

4. To view recorded video, click [Playback] and select an option from the menu that appears.

5. (Optional) To reposition a PTZ camera, click the **PTZ** button to open and adjust the PTZ controls.

Download a Video Clip

Video clips can be downloaded from the *Events* and *Monitoring > Video* pages, as described next.

1. Hover over the bottom of the video frame to display controls that can be used to play and record video. See Video Controls Reference on page 78.

2. To download a clip of live video:

   a. Click [Playback].

   b. Select **Live** from the menu that appears.

   c. Click the **Record Live/Playback Video** button.

   d. Browse for a folder in the dialog box that appears, and then click **OK**.

   e. Click the **Record Live/Playback Video** button again to stop the recording of live video.

      Note: Switching to playback mode while the video is downloading will stop the download process.

      The video clip is downloaded to the selected folder.

3. To download a clip of recorded video:

   a. Click the **Playback** button.

   b. Select **2 minutes** from the Playback menu that appears.

    c. Wait for 30 seconds.

    d. Click the **Record Live/Playback Video** button.

       A timebar appears on the video frame.

    e. Move the slider to the 1 minute mark and click **OK**.

    f. Browse for a folder in the dialog box that appears, and then click **OK**.

       The video clip is downloaded to the selected folder.

Note: If video cannot be downloaded from a camera connected to a TVR31, try adjusting the bandwidth throttle settings on the TVR31.

To view downloaded video clips, use the TruVision Navigator Player provided on the product disc in the \VideoPlayer folder.

Video Controls Reference

Video Controls
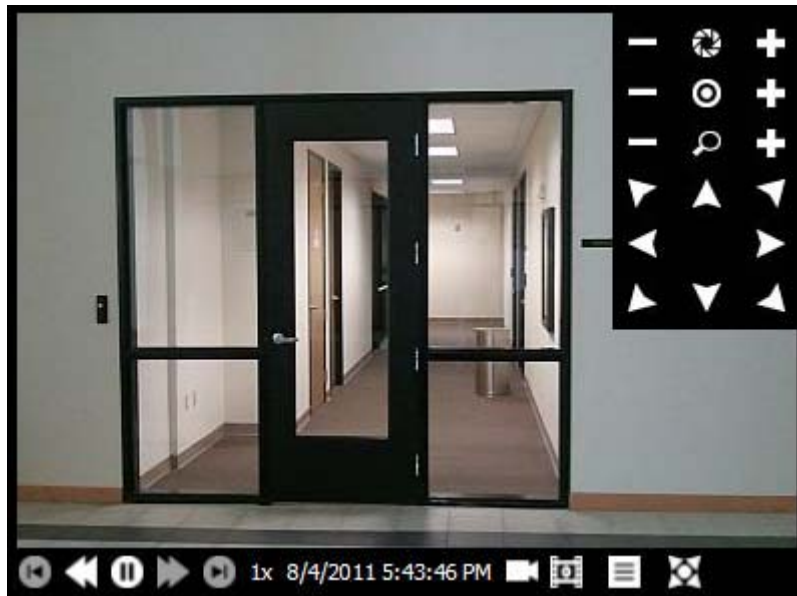
Icon	Feature	Function
![iris] − ⚙ ＋	Iris control	Opens or closes the camera iris to adjust for the amount of light available
![focus] − ⊙ ＋	Focus control	Adjusts the image focus.
![zoom] − 🔍 ＋	Zoom control	Adjusts the camera's zoom.
![pantilt]	Pan and Tilt controls	Moves the camera in the direction(s) indicated by the respective arrow.

Icon	Feature	Function
	Single Step Reverse control	Moves the recorded video back one frame.
	Reverse control	Moves the video backward.
	Play control	Plays the video feed (live or recorded).
	Pause control	Pauses the video feed (live or recorded).
	Forward control	Moves the recorded video ahead in fast forward.
	Single Step Forward control	Moves the recorded video ahead one frame.
	Live control	Switches from playback of recorded video to viewing live video.
	Playback control	Provides a menu of playback options, from live to several minutes in the past.
	Presets control	Quickly moves the camera to preset location.
	Enable PTZ control	Opens the Pan, Tilt, Zoom controls (only works with PTZ cameras).
	Record Live/ Playback Video control	Records video.

Controlling Doors

The *Monitoring > Doors* page shows the status of the doors, the assigned readers, recent events at those doors, and the assigned schedules. This page allows operators to lock out, open, reinstate, and unlock doors.

Open a Door

Use the Open Door command to open a door for someone without a credential.

1. Select *Monitoring > Doors*.
2. Click the **Event View** tab.
3. Click the **Individual Door Commands** action button for the door to be opened.
4. Select Open Door.

Unlock a Door

Use the Unlock Door command to override security for the door, allowing anyone to exit or enter without presenting a valid credential.

1. Select *Monitoring > Doors*.
2. Click the **Event View** tab.
3. Click the **Individual Door Commands** action button for the door to be unlocked.
4. Select Unlock Door.

Reinstate a Door

Use the Reinstate Door command to return the door to its normal mode of operation after unlocking it or locking it out.

1. Select *Monitoring > Doors*.
2. Click the **Event View** tab.
3. Click the **Individual Door Commands** action button for the door to be reinstated.
4. Select Reinstate Door.

Lock Out a Door

Use the Lockout Door command to lock a door and change the reader mode to prevent any credentials from being granted access at the door.

1. Select *Monitoring > Doors*.
2. Click the **Event View** tab.
3. Click the **Individual Door Commands** action button for the door to be locked out.
4. Select Lockout Door.

Secure a Door

Use the Secure Door command to lock a door.

1. Select *Monitoring > Doors*.
2. Click the **Event View** tab.
3. Click the **Individual Door Commands** action button for the door to be secured.
4. Select Secure Door.

Note: To provide a quick way to secure all doors in a facility, create an action trigger record to lock all doors, and then trigger it manually on the *Monitoring > Action Triggers* page when necessary. See Configuring Action Triggers on page 51.

Reinstate All Doors

Use the Reinstate All Doors command to return the readers connected to doors to their normal mode of operation after unlocking all doors or locking out all doors, unless a designated unlock input is active. An unlock input is configured on the *System Administration > Devices > Controller* page.

1. Select *Monitoring > Doors*.
2. Click the **Global Door Commands** action button at the top of the page.

3. Select Reinstate All Doors.

A Reader Reinstated event will be generated for each reader that was previously in the Locked Out state, along with a single All Doors Reinstated event for the System Controller. A Reader in Card Only Mode event or a Reader in Card + PIN Mode event is also generated for every door, depending on how the reader is configured on the *System Administration > Devices* page.

Lock Out All Doors

Use the Lockout All Doors command to lock all doors and change the reader modes to prevent any credentials from being granted access at the doors. Any actions that could impact the door strike will not have any effect until a global Reinstate All Doors command is executed.

1. Select *Monitoring > Doors*.

2. Click the **Global Door Commands** action button at the top of the page.

3. Select Lockout All Doors.

A "Reader Locked Out" event will be generated for each reader that was not already in the Locked Out state, along with a single "All Doors Locked Out" event for the System Controller.

Note: If all doors are locked out when a new door controller is added, the new door controller will remain unlocked. To be locked out, all doors must be reinstated, then all doors locked out again.

Unlock All Doors

Use the Unlock All Doors command to override security for the whole site, allowing anyone to exit or enter without presenting a valid credential. Any actions that could impact the door strike will not have any effect until a global Reinstate All Doors command is executed.

1. Select *Monitoring > Doors*.

2. Click the **Global Door Commands** action button at the top of the page.

3. Select Unlock All Doors.

A "Reader Reinstated" event will be generated for each reader that was locked out, along with a single "All Doors Unlocked" event for the System Controller.

Door Command Menus

Sometimes it is necessary to override normal scheduled behavior for a specific door (for example, if a door needs to be opened for a package delivery person), or for the entire site (for example, during a fire drill). If some disaster or emergency situation occurred near the facility, all doors may need to be locked out. Individual doors can be controlled from the **Event View** tab of the *Monitoring > Doors* page. The global door commands allow users to change the state of all doors on the site with one click.

Global Door Commands Menu

Note: After unlocking all doors or locking out all doors, use the **Reinstate All Doors** command before trying to control any door individually.

Unlock All Doors

Releases the locks on all doors, allowing free access and egress. This will be recorded as Event 14644. After issuing this command, reinstate all doors so that individual doors can be controlled directly.

Lockout All Doors

Locks all doors and ignores credentials, so that no one can enter or exit. This will be recorded as Event 14646. After issuing this command, reinstate all doors so that individual doors can be controlled directly.

Reinstate All Doors

Restores all doors to their normal state, unless a designated unlock input is active. An unlock input is configured on the *System Administration > Devices > Controller* page.

Individual Door Commands Menu

Open Door

Unlocks the door for the length of time specified in **Normal Grant Access Time** on the *System Administration > Devices* page.

Unlock Door

Releases the lock on the door, allowing free access and egress, until the door state is changed by either a reader schedule or a global ("all doors") command.

Reinstate Door

Restores the door to default behavior based on the schedule.

Lockout Door

Locks the door and ignores credentials, so that no one can enter or exit.

Secure Door

Locks the door.

Event View Tab

The **Event View** tab on the *Monitoring > Doors* page shows the most recent event at the door and associated readers, and the current status of each door and its readers. To control individual doors, use the **Event View** tab of the *Monitoring > Doors* page.

Schedule View Tab

The **Schedule View** tab on the *Monitoring > Doors* page can be used to modify door and reader behavior according to schedules, rather than manually as performed on the **Event View** tab.

For example, if a customer showroom has door from the parking lot to the showroom that should remain locked when the business is closed, but unlocked during business hours when a salesman is in the showroom, so customers can easily enter the building. In this case, select a door schedule for 9:00 AM to 5:00 PM and choose "First Card In" for the **Schedule Mode** if the showroom should be unlocked only after a salesperson used a credential to enter the room.

Schedule

Select a schedule from this list (schedules are created in *Access Management > Schedules*) to indicate when the selected Schedule Mode should be active.

Schedule Mode (Door)

Select an option from this list to set behavior for the specific door during the schedule.

Unlocked
The door will be unlocked and accessible without presenting a credential during the selected schedule.

First Card In
The door will go to locked at the beginning of the schedule and remain in this state until the first valid credential is swiped. At that point, the door will switch to an unlocked state.

Locked
The door will be locked and require a valid credential for entry during the selected schedule.

Schedule Mode (Reader)

Select an option from this list to set behavior for the specific reader during the schedule.

Credential Only
A person need only present a valid credential (ID badge) to gain access.

Credential and PIN
A person needs to present a valid credential and enter a Personal Identification Number to gain access. This prevents someone gaining access with a stolen or found credential. Some facilities use **Credential Only** during the day and **Credential and PIN** after hours, when the facility is empty.

PIN Only
A person need only enter a valid Personal Identification Number (PIN) to gain access.

PIN or Credential
A person needs to present either a valid credential or enter a Personal Identification Number (PIN) to gain access.

Door Fallback Mode

Credential information is stored on the System Controller. If a door controller cannot communicate with the controller to determine if access should be granted (for instance, due to a bad connection), the doors on that door controller will operate in fallback mode:

Restricted
No access is granted whatsoever.

Site Code
Access if granted if the card matches one of the formats defined on the *System Administration > Card Formats* page, and the site code on the card matches the site code defined for the format. The credential ID is not checked.

All
Access is granted if the card matches any of the formats defined on the *System Administration > Card Formats* page regardless of the site code or credential ID.

Controlling Inputs and Outputs

Inputs and outputs can be monitored from the *Monitoring > Inputs/Outputs* page, and outputs can be activated or deactivated manually from that page. Outputs can also be controlled by action triggers. To learn more about inputs and outputs, see Configure Inputs and Outputs on page 24

Activate or Deactivate an Output

1. Select *Monitoring > Inputs/Outputs*.
2. Click the **Activate/Deactivate** button for the Output.

   The state of the output changes.

Controlling Action Triggers

On the *System Administration > Action Triggers* page, action triggers can be configured to monitor one or more trigger conditions along with corresponding actions that will be executed when the trigger conditions are satisfied, as described in Configuring Action Triggers on page 51.

Depending on how they are configured, action trigger records can result in two types of actions:

- Activation actions that are executed when a trigger condition becomes true, and
- Deactivation actions that are executed when a trigger condition becomes false.

Once created, action triggers can be executed manually on the *Monitoring > Action Triggers* page to cause the corresponding action to be executed.

Note the following details about controlling action triggers:

- Action triggers that do not have an action defined for them will not appear on the *Monitoring > Action Triggers* page.
- Manual triggering does not have any priority over system triggering, nor is the trigger state persisted. Once an action is manually triggered, any future state change of the system trigger condition will cause the actions to be executed again.
- To provide a quick way to secure all doors in a facility, create an action trigger record to lock all doors, and then trigger it manually on the *Monitoring > Action Triggers* page when necessary.

Execute an Action Trigger Record Manually

1. Select *Monitoring > Action Triggers*.
2. Click the **Manual Trigger** action button for the action trigger record.
3. Select **Execute Activation Actions** or **Execute Deactivation Actions**.

Resetting Anti-Passback

Anti-passback requires that a credential be used to enter and exit an area. In this way, the System tracks which area the credential holder is currently occupying, keeps a record of personnel movements in secure areas, and prevents passage to areas that are logically impossible. If a person uses a credential to enter an area configured for anti-passback, and then leaves the area without using the credential (through a door held open by another person, for example), the System will not record

that the person has left the specific area. As a result, if the System is configured for hard anti-passback enforcement, it will prevent that credential from being used to enter another area, including the one just left, until the credential's location is reset to a default or neutral area.

1. Select *Monitoring > Anti-Passback Reset*.
2. To reset all persons:
   a. Click [Reset All].
   b. Select an area from the list.
3. To reset selected persons:
   a. Select a range of persons by clicking the first name in the list, holding <Shift>, and clicking the last person. The range of names is highlighted.
   b. Select individuals by clicking the first name desired, holding <Ctrl> and clicking on other names to select them.
   c. Click [Reset Selected].
   d. Select an area from the list.

CHAPTER 7   *Maintenance*

A few simple maintenance activities will help make sure the System runs efficiently with minimal trouble or disruption to service. These include backing up the database and checking for firmware updates.

Backing Up Data

Periodic backups of the System database are highly recommended to ensure quick recovery of security needs following a disaster. The System saves backups to the local client workstation, so a copy exists that is not on the System Controller. The encrypted backup file includes all records, photos, and settings configured in the System with the exception of:

- Door/reader states set manually via the ***Monitoring > Doors*** page, and
- Events.

Database backups can also be scheduled to occur automatically, with emails sent out after successful or failed backups. Events can also be backed up to a CSV file.

Create a Backup File

This section describes how to create a backup file and download it to a local client workstation. System data can be backed up to a file on the client workstation (as described here) or automated backups can be scheduled, as described in Schedule Automated Backups on page 88. (To back up events, refer to Back Up Events on page 89.)

1. Log into the System as a user with Execute permissions for the Backup Database feature.
2. Select *System Administration > Backup/Restore*.
3. Click [Download Backup File].

   The Backup Database dialog box appears.
4. Click [Download Backup File].
5. Select a location for the backup file.
6. Click [Save].

   > **IMPORTANT:** The database backup filename contains a validation checksum required to restore the System (for example, backup_1926651153.bak). Do not edit any characters that appear after the underscore character (_) in the filename.

Schedule Automated Backups

Automated backups can be scheduled to occur up to seven times per week, with the resulting backup file sent to a shared network resource (see Configuring a Network Share on page 62). If the System is configured to send automated emails, a notification is sent after a scheduled backup occurs.

> **Note:** Scheduled backups must occur at least 30 minutes apart.

1. Log into the System as a user with Execute permissions for the Scheduled Backups feature.
2. Select *System Administration > Backup/Restore*.
3. Click [Schedule Backup].
4. To create a schedule for a database backup:
   a. In the Database Schedule Configuration area of the page, select **Schedule Enabled**.
   b. Select the days when the schedule will be backed up.
   c. Select a time for the backup.
   d. Select the location where the backup file will be sent in the **Network Shares** field.
   e. (Optional) Click [Backup Now] to start the backup immediately.
5. To create a schedule for an event backup:
   a. In the Event Schedule Configuration area of the page, select **Schedule Enabled**.
   b. Select **Schedule Incremental** to back up only those events that occurred since the last backup occurred.
   c. Select the days when the schedule will be backed up.
   d. Select a time for the backup.
   e. Select the location where the backup file will be sent in the **Network Shares** field.
   f. (Optional) Click [Backup Now] to start the backup immediately.
6. (Optional) To send an automated email after a scheduled backup:
   a. Select **Send on success**, **Send on failure**, or both check boxes.
   b. Select an **Email List**.
7. Click [Accept Changes].

Back Up Events

Note the following details about events:

- Events cannot be restored from a backup file. The file is intended for recordkeeping purposes only.
- Events can be exported using the Import/Export Wizard provided on the Utilities disc, as described in the *Import/Export Wizard User Guide*.

To back up events:

1. Log into the System as a user with Execute permissions for the Backup Database feature.
2. Select *System Administration > Backup/Restore*.
3. Click [Schedule Backup].
4. In the Event Schedule Configuration area of the page, click [Backup Now].

   The Running Scheduled Backup dialog box displays the results of the operation.

Restore from a Backup

> **IMPORTANT:** Restoring a backup will overwrite the database, and any changes made since the date of the backup will be lost.

1. Log into the System as a user with Execute permissions for the Restore Database feature.
2. Select *System Administration > Backup/Restore*.
3. Click [Browse].
4. Navigate to the backup file.
5. Select the file and click [Open].
6. Click [Upload Backup File].

Saving and Restoring Custom Settings

Use the *System Administration > Save/Reset Settings* page to create a restore point that includes all of the data normally saved in a backup file, plus the custom settings of the System Controller. This is like a custom default state.

Instead of resetting the System Controller to a factory default state, which would then have to be reconfigured to specific requirements, the basic site configuration can be saved as a custom setting and reset to that, should the need ever arise. The information is stored on the System Controller and can be restored later using a preset security phrase.

Save Data and Custom Settings

This task creates a file with all current data and configuration settings stored on the System Controller.

1. Select *System Administration > Save/Reset Settings*.
2. Select **Save Custom Settings**.
3. Type a **Username**.
4. Type a **Password**.

5. Type the security phrase, exactly as shown (case sensitive).

6. Click **Save Custom Settings**.

Restore Custom Settings

IMPORTANT: Using this feature will erase all settings and data, and reset the System to use the settings and data stored in the custom settings file. Be sure to create a current backup before restoring custom settings.

IMPORTANT: After restoring custom settings, the System Controller will reboot. During this time, it will be offline for a few minutes. Therefore, it is best to use this feature during periods of little or no access activity, or credential holders will be forced to wait to gain entry if a Door Fallback Mode was not configured to allow access when the System Controller is offline.

1. Select *System Administration > Save/Reset Settings.*

2. Select **Restore Custom Settings**.

3. Type a **Username**.

4. Type a **Password**.

5. Type the security phrase, exactly as shown (case sensitive).

6. Click **Restore Custom Settings**.

   A Warning message appears, stating: "The Device is rebooting," and displaying a progress bar.

   When the progress bar completes, the server will go offline and the browser will display its default page when it cannot connect to a web address.

7. Clear the browser cache. (In Internet Explorer 8+, press <Ctrl>+<Shift>+<Delete>.)

Reset Factory Settings

IMPORTANT: This feature will erase all settings and data (except Network Configuration settings), and reset the System Controller to the factory default values. Be sure to create a current backup before resetting factory settings.

1. Select *System Administration > Save/Reset Settings*.

2. Select **Reset Factory Settings**.

3. Type a **Username**.

4. Type a **Password**.

5. Type the security phrase, exactly as shown (case sensitive).

6. Click **Reset Factory Settings**.

   A warning message appears, stating: "The Device is rebooting," and displaying a progress bar.

   When the progress bar completes, the server will go offline and the browser will display its default page when it cannot connect to a web address.

7. Clear the browser cache. (In Internet Explorer 8 or later, press <Ctrl>+<Shift>+<Delete>.)

   When the server comes back online, the End User Software License Acceptance (EULA) Form will be displayed.

8. Click **Accept**.

Updating the Firmware

Feature improvements are occasionally made available on the product web site in the form of firmware updates that can be downloaded and applied to the System Controller and any IPSDCs that may be installed.

Note: *Updating* the System Controller firmware is a different than *upgrading* the System, which impacts the core code of the System Controller in addition to the firmware. To switch from one version of TruPortal to a later version (for example, from version 1.0 to version 1.5) or to upgrade from goEntry to TruPortal, see Using the Upgrade Wizard on page 11.

Before You Begin

Before performing a firmware update, note the following details:

IMPORTANT: Connect a fully-charged backup battery to the System Controller before updating the firmware. The System Controller may be rendered inoperable and require replacement if power is lost during a firmware update. Refer to the *System Controller Quick Reference* for battery information.

IMPORTANT: Do not reset or restart an IPSDC during a firmware update or the IPSDC will become nonfunctional.

- Back up the database before updating the System Controller firmware. See Backing Up Data on page 87.
- Events stored on the System Controller are purged during a firmware update. To retain a record of existing events, back up events (see Back Up Events on page 89) or export events (see the *Import/Export Wizard User Guide*).
- Once started, a firmware update cannot be cancelled.
- Firmware cannot be reverted after a firmware update.
- During a System Controller firmware update, there will be two brief periods when credentials cannot be used to access doors. After the update is complete and the System Controller reboots, normal operation will resume.

Check for Firmware Updates

1. Download the firmware update files from the product web site.
   - System Controller firmware update files have an LFF extension.
   - IPSDCs firmware update files use this file name: IPSDCU.bin.
2. Log into the System as a user with Execute permissions for the Firmware Updates feature.
3. Compare the firmware updates available on the web site with the firmware revision numbers of the System Controller and any IPSDCs, as displayed on the *System Administration > System Settings* page.
4. Download any firmware updates that are more recent than the firmware on the System Controller and IPSDCs.
5. Select *System Administration > Firmware Updates*.
6. Select either **Update TruPortal Firmware** or **Update IP Door Controller Firmware**.
7. In the **New Firmware File** field, navigate to and select the firmware update file.

8. Click [Next].

9. Click [Update].

After a System Controller firmware update, the System Controller will restart. Log back in and switch to the *Monitoring > Diagnostics* page (see Diagnostics on page 96) to check for any problems with doors, controllers, and other newly installed hardware.

Managing Language Packs

The System provides the following flexibility in its approach to languages:

• A System Language determines the language used for functions performed by the System, such as assigning default device names, scheduled backups, and automated emails.

• Individual users can select a different, user-level language when logging into the System.

Four languages — English, Spanish, French, and Dutch — are provided with the System and users can switch the language for the User Interface when logging in. (See Logging into the System on page 15.)

Additional languages are provided in the form of *language packs* that are available on the product website. These language packs can be downloaded and added to the System. Language packs can also be removed.

Note the following details about language packs:

• Only four languages can be active at any one time.

• Before adding a new language to a new installation, an existing language must be removed.

Note:　　　Neither English nor the current System Language can be removed.

• After a new language is added, the language becomes available the next time the user logs in.

• If the currently-active language (for example, Spanish) is removed, a user must log out of the System and then log back in to select the new language.

• Language packs are created for specific versions of the System Controller firmware. The first two digits of the version number for the language pack (for example, *3.5x.xxxx*) must match the first two digits of the current firmware version, which is displayed on the *System Administration > Language Packs* page.

• When the System Controller firmware is updated, English and any other default language packs (Spanish, French, Dutch, and Portuguese) that are still installed are updated. To update any other language pack, download and install the appropriate language pack from the product website.

• Service pack upgrades do not impact language packs.

Add a Language Pack

1. Launch a supported Internet browser.

2. Download the desired language pack from the product website to a local client workstation or a shared file system.

3. Log into the System as a user with Modification permissions.

4. Select *System Administration > Language Packs*.

5. Click [Add].

Note: The [Add] button is only enabled if less than four language packs are currently installed. If necessary, remove a language pack (except English and the current System-level language pack) before adding a new language pack. See Remove a Language Pack on page 93.

6. In the Open dialog box, navigate to the folder to which the language pack (the file has a .NLS extension) was downloaded, select the file, and then click [Open].

7. When the Language Pack Add-On window appears, click [Install].

8. When installation is complete, click [Finish].

9. To begin using the new language:

    a. Log out of the System by clicking the **Logout** icon in the top-right portion of the User Interface.

    b. Follow the steps in Logging into the System on page 15 and select the new language in the **Language** field.

Remove a Language Pack

Note: Neither English nor the current System-level language pack can be removed.

1. Select *System Administration > Language Packs*.

2. Click the language pack to select it.

3. Click [Remove].

   The Remove Item dialog box appears.

4. Click [Remove].

Troubleshooting

Resolving Browser Issues

Clearing the cache and restarting the browser can solve many apparent problems, such as sudden strange behavior in the User Interface. Specific steps vary by browser make and version.

1. Log out of the System, log back in, and return to the **Home** page.
2. Clear the browser history and cache.
3. Close the browser and reopen.
4. Log into the System.

Note: After enabling or disabling HTTPS/SSL, be sure to clear the browser cache, especially if using Firefox or Chrome.

Here are some other tips for troubleshooting browser issues:

• If the System Controller is reset or the database is restored, Internet Explorer may temporarily display an XML page instead of the login page. If this occurs, refresh the browser page until the login page appears.

• The System supports the use of the [Back] and [Forward] browser buttons, but a blank page may appear occasionally while navigating backward or forward. If this occurs, refresh the browser page.

• For browsers other than Internet Explorer, the [Back] and [Forward] buttons may not work as expected when trying to navigate between tabs of a given page (for example, when switching between the Details and User Account tabs on the *Access Management > Persons* page). If this occurs, use a mouse to click the desired tab.

• Maximize the browser window to display all tool tips. Tool tips may not appear if the browser window is too small.

• When HTTPS security is enabled or disabled on the *System Settings > Network Configuration* page, the login page should appear automatically. If the login page does not appear, manually clear the browser cache and restart the browser to access the login page.

• Browser proxy settings may affect connectivity to the System Controller (which uses ports 80 and 443) when HTTPS is disabled. To resolve this issue, configure proxy servers to allow HTTP traffic over port 443 by either explicitly (1) specifying port 443 in the panel URL (for example, http://192.168.1.10:443), (2) adding an exception to proxy settings on the client, or (3)

configuring a service port that is unblocked by the firewall. See Configure Network Settings on page 17.

Rebooting the System Controller

1. Select *System Administration > Devices*.

2. Select the System Controller from the hierarchical device tree.

3. Click [Reboot Controller].

When the System Controller is powered only by a battery and voltage drops below 10.2 V, the board switches off until the main AC/DC power is restored.

Resetting the Administrator Password

The password for the default administrator account should be changed to enhance security. However, if the default administrator login was changed unintentionally or renamed to a user who is not the administrator, it may be necessary to reset the password.

To reset the username and password:

1. Using a text editor (such as Notepad), create a file that is blank. Save it as **resetpwd.txt**.

2. Transfer the file to a USB drive.

3. Plug the USB drive into the USB port of the TruPortal controller.

4. Cycle power to the controller. When the board powers up again, it will reset the Administrator account to its default username (admin) and password (demo).

5. Remove the USB drive from the controller.

If a user who is not an administrator has admin as a username, the system will automatically disable the login and delete the username (the user account itself will still remain in the database) before resetting.

When the password has been reset, the **resetpwd.txt** file is deleted. The results of the reset are written to a new file, **resetpwd.log**.

Diagnostics

Errors detected by the System are displayed on the *Monitoring > Diagnostics* page, along with System statistics, such as the numbers of inputs. All information is queried at login time and every minute thereafter. To manually refresh the data, click [Refresh].

To access the *Diagnostics* page:

• Select *Monitoring > Diagnostics*, or

• Click the Status Indicator that appears in the top center of the User Interface when errors or warnings occur.

Note the following details about the *Diagnostics* page:

• Red shading indicates a malfunction, such as offline devices. Yellow shading indicates a warning, such as a tamper condition.

- An ellipsis (...) appears if additional information about a category is available in a tool tip that can be displayed by hovering over the ellipsis.
- The System does not include actions for running specific diagnostic tests.
- Click [Download Diagnostic File] to create a single, encrypted file that includes a variety of system information, including configuration data and logs. No specific personnel information (for example, names or Social Security numbers) will be included in the file; refer to the Release Notes for details. The file can be saved locally and sent to Technical Support for use in troubleshooting issues.
- An accurate reading for DC current cannot be displayed when the System Controller is powered by a DC source. The DC current information is only displayed when the System Controller has AC power.

Diagnostic	Display Value	Status
AC Power	OK | Brownout | Fail	INF = OK WRN = Brownout ERR = Fail
DC Power	Voltage, Current	INF >= 10.0 VWRN < 10.0 V WRN = Current overload
Backup Battery	Voltage, Current, Charging | Discharging	INF >= 11.7 VWRN < 11.7 V ERR < 11.4 V, No Battery
Memory Battery	Voltage	INF >= 2.3 V WRN < 2.3 V ERR < 2.0 V
Fuses	OK | Fuse Name,…	INF = All OK ERR = If any not OK
Controller	OK | Problems,…	INF = OK WRN = If not OK
Modules	OK | ModuleName problem,…	INF = All OK WRN = If any tamper ERR = If any offline
Doors	OK | DoorName problem,…	INF = All OK WRN = If any held, forced, tamper ERR – If any offline
Digital Inputs	OK | InputName problem,…	INF = All OK WRN = If any tamper ERR – If any offline
Uptime	Last boot time, up days	INF = Always
CPU Load Avg	1m, 5m, 15m	INF 15m < 0.80 WRN 15m >= 0.80 ERR 15m >= 0.95

Diagnostic	Display Value	Status
Memory Usage	Used, Total	INF < 95% WRN >= 95% ERR = 100%
Main Storage	Percent	INF < 90% WRN >= 90% ERR = 100%
Pictures & Backup Storage	Used, Total	INF < 50% WRN >= 50% ERR >= 95%
ADP Boards	Used, Total	INF = Always
Doors	Used, Total	INF = Always
Readers	Used, Total	INF = Always
EIO Boards	Used, Total	INF = Always
Inputs	Used, Total	INF = Always
Outputs	Used, Total	INF = Always
DVRs	Used, Total	INF = Always
Cameras	Used, Total	INF = Always
Person	Used, Total	INF = Always
Credentials	Used, Total	INF = Always
Access Levels	Used, Total	INF – Always
Schedules	Used, Total	INF – Always
Holiday Groups	Used, Total	INF – Always
Holidays	Used, Total	INF = Always
Areas	Used, Total	INF = Always
Reader Groups	Used, Total	INF = Always
Operator Roles	Used, Total	INF = Always
Video Layouts	Used, Total	INF = Always
Card Formats	Used, Total	INF = Always

Fuses

The fuses protect DC power provided by the System Controller board for use by external peripherals.

Fuse	+V	0V
Aux 1	CN3.1	CN3.2

Fuse	+V	0V
Aux 2	CN3.3	CN3.4
Door Controller	CN10.2 CN17.2	CN11.4 CN18.4
Aux Input	CN21.1	CN21.3 CN22.2

Hardware Problem States

Hardware items can have the following problems:

Controller

• Tamper

Modules

• Offline
• Tamper

Doors

• Offline
• Forced
• Held
• RTE Tamper
• Door Contact Tamper
• Door Aux Tamper
• Door Tamper

Digital Input

• Offline
• Tamper

Troubleshooting Readers

If a reader is not responding as desired, use the [Scan for Hardware Changes] button (see Scan for Hardware Changes on page 22), verify that the reader appears in the Device Tree hierarchy on the *System Administration > Devices* page, and check the reader configuration. See Configure Readers on page 32.

If unexpected events occur for doors or readers connected to an IPSDC, check the IPSDC jumper and switch settings to make sure that the hardware is configured correctly. For example, the reader Device Input (DI) port, J2, has two digital inputs which are used for door status devices (door contacts and exit request input) and can be configured as either supervised or non-supervised digital inputs. If the inputs are configured as supervised digital inputs in the TruPortal User Interface, they require EOL resistors. Refer to the *IPSDC Quick Reference* for details.

Troubleshooting Schedules

If a schedule is not behaving as expected, review the following sections:

- Creating Holiday Groups on page 38
- Creating Schedules on page 40
- Considerations for Schedule-Based Action Trigger Records on page 55

Error, Warning and Event Messages

Tamper States

The System Controller does not distinguish which of the four door input are in tamper state when it logs tamper events. The real-time state of inputs in tamper can be viewed on the *Monitoring > Diagnostics* page.

Power and Battery Events

System Controller Shuts Down on Battery Power

If the System Controller is operating on battery power only and the battery voltage drops below 10.2 volts, the System Controller will shut down until AC power is restored.

Backup Battery Events

Backup Battery Events occur when the backup battery voltage drops below certain thresholds.

Event Code	Event Description	Cause
Event 14612	Backup Battery Critical	Voltage falls below 11.4V, or rises above 10.2V
Event 14613	Backup Battery Cutoff	Voltage falls below 10.2V, or rises above 9.0V
Event 14624	Backup Battery Low	Voltage falls below 11.7V, or rises above 11.4V
Event 14625	Backup Battery Restored	Voltage rises above 11.7V
Event 14649	Backup Battery Not Detected	Voltage falls below 9.0V

Note: If the System Controller is powered exclusively off of a backup battery, it will shutdown at 10.2V and the Cutoff and Not Detected events will not be generated.

Memory Battery Event

Event Code	Event Description
Event 14618	Memory Backup Battery Low

Fuse Events

Event Code	Event Description
Event 14651	Fuse Tripped
Event 14652	Fuse Restored

Device Events

Event Code	Event Description	Device
Event 4105	Device Communications Failed	Door Controller, I/O Expander
Event 4106	Device Communications Restored	Door Controller, I/O Expander
Event 4107	Tamper Alarm*	Controller, Door Controller, I/O Expander
Event 14622	System Trouble	Controller
Event 14623	System Restored	Controller
Event 14628	Device Failed	Controller
Event 14629	Device Restored	Controller
Event 14643	Tamper Restored*	Controller, Door Controller, I/O Expander

* Not applicable to built-in door controller

Device Communications Failed/Restored
Used to indicate communication errors with downstream devices. Occurs when communications between the RS-485 SNAPP bus and a configured downstream device are lost or established. Device will always show which module is affected.

Device Failed/Restored
Used to indicate general issues with downstream devices. Occurs when any device tamper input changes state (including External/Wall Tamper, but not Door Tamper), or when a VBUS communications error is detected. Device will always indicate Controller. For tamper events, there will be corresponding tamper event for the device. For VBUS error events, there is no way to report which device has the VBUS error, so there is no corresponding event to show which device has the VBUS error.

System Trouble/Restored
Used to indicate general issues with the System. Occurs when **External/Wall Tamper** changes state. **Device** will always indicate the System Controller. This event may be used in the future to identify other trouble conditions.

Door Tamper Events

Event Code	Event Description
Event 14633	Door Tamper Restored
Event 14632	Door Tamper Alarm

Door Tamper Alarm/Restored
Used to indicate tamper condition on any of the four door inputs - DR, RTE, TR, AUX. The tamper alarm event is generated when a tamper condition is detected on any of the inputs, or when TR is active. Additional tamper alarm events will not be generated for RTE, TR, and AUX until all tamper conditions are resolved, however additional tamper alarm events will be generated for DR while other tamper conditions still exist. The tamper restored event is only generated when the tamper condition is resolved on all four inputs, and TR is inactive

Auxiliary Input Events

Event Code	Event Description
Event 14640	Input Active
Event 14641	Input Tamper Alarm
Event 14642	Input Inactive
Event 4170	Input Disabled

Auxiliary Output Events

Event Code	Event Description
Event 10240	Output On
Event 11264	Output Off

"Objects Have Changed" Warning

From time to time, the local browser cache may become out of synchronization with the System. When this happens, the User Interface will be disabled, and the warning message will appear.

Click the text of the warning to reload the page.

"NTP Sync Failed" Event

The ability to synchronization the System with an NTP server, as discussed in Setting the Date and Time on page 15, requires that the System be able to access the NTP server via UDP port 123. If this port is not open (for example, if it is blocked by a firewall), an "NTP Sync Failed" event will be logged. Consult with the site network administrator to resolve this issue.

Video Player Errors

If problems displaying video are encountered, review Before You Begin on page 76 in addition to the following information.

No Active Video Connections

This message appears on the *Monitoring > Video* page and the Event Detail pane of the *Events* page.

The message means either:

• A camera device is not configured,

• The System lost communication with a connected DVR/NVR, or

• The video player is not installed, or is out of date. See Before You Begin on page 76.

Note: Video can only be viewed in Internet Explorer. Refer to the *Release Notes* for details.

If the error message is displayed when a camera icon next to an event is clicked:

1. Click [Play Event Video].

2. Either the video is displayed or the video player is not installed. See Before You Begin on page 76.

3. If neither happens and the message persists, verify the DVR/NVR and camera are operating:

   a. See Configuring Video Devices on page 33.

   b. See Link Cameras to Devices to Track Video of Events on page 35..

If the error message is displayed when *Monitoring > Video* is selected:

1. Double-click the video pane displaying the error message.

2. If the video does not appear:

   a. Select *Monitoring > Video Layouts*.

   b. Select the video layout being viewed.

   c. Make sure the correct camera is chosen for each drop-down list in each pane of the video layout.

3. If the correct camera is not shown in the list, verify that the camera is added to the *System Administration > Devices* page and operating:

   a. See Configuring Video Devices on page 33.

   b. See Add a Video Camera on page 34.

   c. See Add Video Layouts on page 35.

Reference

System Capacities

Attribute	Capacity
Number of persons	10,000
Number of unique credentials	10,000
Credentials per person	5
Access levels	64
Access levels per credential	8
Schedules	64
Time intervals per schedule	6
Holiday groups per schedule	8
Holiday groups	8
Holidays per holiday group	32
Holidays (total)	255
Areas	64
Reader groups	64
Operator roles	32
User-defined fields	10
Video layouts	64
Card formats	8
Email lists	10
Action Triggers	32

Attribute	Capacity
Number of retained events in event log	65,000
Device Capacities	
Number of doors (base board and dual door controllers) with readers in / Number of doors with readers in and out	64 / 32
Total number of Dual Door Interface Modules (including built in)	32
Total number of IP-based Single Door Controllers (IPSDCs)	62
Readers (total)	64
Inputs/Outputs	
Total number of system inputs (including the System Controller)	132
Total number of system outputs (including the System Controller)	66
Total number of Input/Output Expansion Add-Ons or Input/Output Expansion Add-On boards	8
DVRs/NVRs	4
Cameras	64
Ethernet ports	2
RS-485 SNAPP bus ports	4

Configuring IP-Based Single Door Controllers

Before configuring IP-based Single Door Controllers (IPSDCs) in the User Interface, each IPSDC must be configured to recognize the IP address of the System Controller. Establishing this network connection ensures that the IPSDC will be detected when the [Scan for Hardware Changes] button is used on the *System Administration > Devices* page.

Here is a high-level overview of the steps involved in configuring an IPSDC:

1. Install the IPSDC. See the *TruPortal IP-Based Single Door Controller Quick Reference* for details.
2. Follow the steps in Preparing Client Workstations to Use the Integrated Configuration Tool (ICT) on page 107. Before an IPSDC can be configured, the IP address of a local client workstation must be changed so that it is on the same sub-network as the IPSDC.
3. Review Before You Begin on page 108 to learn more about the ICT.
4. Follow the steps in Using the ICT to Configure IPSDCs on page 109.
5. Log into the TruPortal User Interface and access the *System Administration > Devices* page.
6. Use the [Scan for Hardware Changes] button so that the System Controller can discover the IPSDC and add it to the Device Tree. See Scan for Hardware Changes on page 22.
7. Configure the IPSDC in the TruPortal User Interface. See Configure a Door Controller on page 25.

Following are some additional details about IPSDCs:

- Feature improvements for IPSDCs are occasionally made available on the product web site in the form of firmware updates. See Updating the Firmware on page 91.

- IPSDCs can be configured to use a fallback mode if connectivity with the System Controller is lost. A local cache that stores the last 50 successful credentials can grant access. See Configuring Security on page 18.

- IPSDCs do not support Buzzer On and Buzzer Off actions configured for action triggers, tamper input points, or auxiliary input types. See the *TruPortal IP-Based Single Door Controller Quick Reference* for details about modifying jumper settings for input types.

- To replace an IPSDC, refer to Replace a Door Controller on page 25.

Preparing Client Workstations to Use the Integrated Configuration Tool (ICT)

The *Integrated Configuration Tool (ICT)* is a browser-based program that is built-in to each IPSDC that can be used to configure an IPSDC to recognize the System Controller.

The default IP address of an IPSDC is 192.168.6.6. Before using the ICT to configure an IPSDC, the local client workstation must be prepared so that it is on the same sub-network as the IPSDC. These steps vary depending on which operating system is used, as described next.

To prepare a Windows XP client workstation:

1. Click *Start*, *Control Panel*, then *Network Connections*.
2. Right-click on **Local Area Connection**. If the first option in the drop-down list box is:
   - **Disable**, then the connection is enabled. Go to step 3.
   - **Enable**, then select it to enable the connection. Return to step 1.
3. Select **Properties** from the drop-down list.
4. In the section **This connection uses the following items**:, select **Internet Protocol TCP/IP**.
5. Select **Properties**.
6. If this computer is set for:
   - **DHCP**, then **Obtain an IP address automatically** is already selected. Select **Use the following IP address**.
   - **Static**, then write down the IP address and Subnet number. Reset the computer to these values after the controller configuration is complete.
7. Enter the IP address 192.168.6.1, or a similar valid IP address (e.g., 192.168.6.x where x is any number between 1 and 254 except 6).
8. Change the subnet to 255.255.255.0.

   The default gateway does not need to be changed.
9. Click **OK** until all open windows are closed.
10. If a firewall is enabled on the client workstation, disable the firewall before starting the ICT.
11. Proceed to Using the ICT to Configure IPSDCs on page 109.

To prepare a Windows 7 client workstation:

1. Click the *Start* button, select *Control Panel*, *Network and Internet*, and then *Network and Sharing Center*.
2. In the **View your active networks** section of the form, click the **Local Area Connection** link.
3. In the **Local Area Connection** dialog box, click **Properties**.
4. In the Local Area Connection Properties dialog box, select either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**.

5. Click **Properties**.

   • If **Obtain an IPvx /Address Automatically** is already checked, select **Use the Following IPvx Address**, where x is the Internet Protocol Version being used (4 or 6).

   • If the connection is static, write down the IP address and Subnet mask number. Reset the computer to these values after the controller configuration is complete.

6. Enter the IP address, `192.168.6.1`, or a similar valid IP address (e.g., `192.168.6.x` where x is any number between 1 and 254 except 6).

7. Change the Subnet Prefix Length value to `255.255.255.0`.

   The default gateway does not need to be changed.

8. Click **OK** and **Close** until all open windows are closed.

9. If a firewall is enabled on the client workstation, disable the firewall before starting the ICT.

10. Proceed to .

To prepare a Windows 8 client workstation:

1. Click the **Network** icon to open the Network and Sharing Center.

2. Click **Change Adapter Settings**.

3. On the Network Connections window, right-click the **Local Area Connection** icon and select **Properties** from the menu.

4. In the Local Area Connection Properties dialog box, select either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**.

5. Click **Properties**.

   • If **Obtain an IPvx /Address Automatically** is already checked, select **Use the Following IPvx Address**, where x is the Internet Protocol Version being used (4 or 6).

   • If the connection is static, write down the IP address and Subnet mask number. Reset the computer to these values after the controller configuration is complete.

6. Enter the IP address, `192.168.6.1`, or a similar valid IP address (e.g., `192.168.6.x` where x is any number between 1 and 254 except 6).

7. Change the **Subnet Prefix Length** value to `255.255.255.0`.

   The default gateway does not need to be changed.

8. Click **OK** and **Close** until all open windows are closed.

9. If a firewall is enabled on the client workstation, disable the firewall before starting the ICT.

10. Proceed to .

Using the Integrated Configuration Tool

This section describes how to use the ICT to configure an IPSDC to recognize the IP address of the System Controller so that the IPSDC will be detected when the [Scan for Hardware Changes] button is used on the *System Administration > Devices* page.

Before You Begin

Before using the ICT, note the following details:

• The local client workstation that will be used to access the ICT must be properly configured. Refer to .

• If a firewall is enabled on the local client workstation, disable the firewall before starting the ICT.

- If an installation requires that an IPSDC and its corresponding host communicate through a firewall, use the ICT to configure the IPSDC firewall to allow connections through port 3001.

- Disable or bypass any network proxies while using the ICT.

- After configuration is complete, the ICT can be disabled to prevent unauthorized access. See Enabling and Disabling the ICT on page 110.

- If options are changed on an ICT form, click **Save** at the bottom of the form to save changes before switching to another form. This action saves the latest changes to a temporary configuration file.

- After completing all the forms, click **Apply Changes** and then click **Restart Application** for the changes to take effect. Changes will be saved to the configuration database on the IPSDC.

The following table describes the buttons available in the ICT interface:

Button	Usage	Result
Save	After changing values on any form	Saves changes to a temporary configuration file.
Apply Changes	After all changes are complete	Saves changes from the temporary configuration file to the configuration database.
Restart Application	After selecting **Apply Changes**	The ICT picks up the latest changes from the configuration database and starts again.
Restart Controller	After selecting **Apply Changes**	The IPSDC applies the latest changes and starts again.
Factory Defaults[a]	To restore IPSDC default settings	IPSDC settings are restored to factory defaults. The IP address settings are retained.
Change User/ Password	To set the user ID and/or password for logging into the ICT.	Changes the user ID and/or password for the ICT. The default values are `install, install.` For increased security, change the default values.

a. If the default network parameters are restored using the SW7 button, then all parameters (including the IP address of the IPSDC) will be modified.

Using the ICT to Configure IPSDCs

Follow these steps to configure an IPSDC to recognize the IP address of the System Controller. These steps can also be used to reconfigure an IPSDC if the IP address of the System Controller changes.

1. Use one of the following Internet browsers to open a browser window on the client workstation:
   - Microsoft Internet Explorer 7.0 or later
   - Netscape 7.0 or later
   - Mozilla Firefox 12.0 or later

2. In the browser **Address** field, enter the IP address of the IPSDC.

   The factory default IP address of an IPSDC is `192.168.6.6.` If you are not sure what the IP address of an IPSDC is, press and hold the Restore Defaults button (SW7) on the IPSDC for at least 5 seconds to restore its settings to factory default values.

3. When the ICT starts, type the **User ID** and **Password** for the ICT.

   The default values are `install` and `install.`

4. Click [Login].

The Controller Information page displays the Parameters form.

5. (Recommended) Change the default password to enhance security:

   a. Click [Change User/Password] to open the Change User/Password form.

   b. Type the **User ID**.

   c. Type the **New Password**.

   d. Retype the password in the **Confirm Password** field.

   e. Click [Change Credentials].

6. Click the Controller Parameters menu to open the Primary Network form.

7. To use a dynamic connection for the IPSDC, select **Use DHCP**. (Use this option if a DHCP server is in the network and the IPSDC can be reached via the console port.)

   To use a static connection (i.e., a set IP address):

   a. Type the **Controller IP**.

   b. Type the **Gateway IP**.

   c. Type the **Subnet Mask**.

8. Type the name of the IPSDC in the **Controller Name** field.

9. (Recommended) Record this information on the installation chart. See Documenting the Physical Location of Each Device on page 5.

10. Click **Save**.

11. Switch to the Panel Configuration tab and type the IP address of the System Controller in the **Panel IP Address** field.

12. Click **Save**.

13. If this completes the IPSDC configuration using the ICT, click **Apply Changes**, then **Restart Application**.

14. If the local client workstation used to access the ICT originally had a static IP address, reset the workstation to use the original address. See Preparing Client Workstations to Use the Integrated Configuration Tool (ICT) on page 107.

15. After an IPSDC is configured to recognize the IP address of the System Controller, it can be added to the System in two ways:

   • Use the [Scan for Hardware Changes] button to discover devices. See Scan for Hardware Changes on page 22, or

   • Add the IPSDC manually by selecting the System Controller on the *System Administration > Devices* page, clicking [Add], and selecting *IP 1 Door 2 Reader Controller*. Click [Accept Changes] when finished.

16. To complete the configuration of an IPSDC in the User Interface:

   • Configure system-wide IPSDC options on the Security tab of the *System Administration > System Settings* page. See Configuring Security on page 18, and

   • Configure controller-specific options on the *System Administration > Devices* page. See Configure a Door Controller on page 25.

Enabling and Disabling the ICT

Control access to the ICT by selecting one of two options:

• **Temporary**: Allows access to the ICT until the IPSDC resets.

• **Permanent**: Allows access until the ICT is manually disabled again.

   IMPORTANT: Before you begin, you must have physical access to the controller.

To enable the ICT temporarily:

1. Press and hold SW4 until D19 (i.e., the Watchdog LED) turns ON. Allow up to five (5) seconds for D19 to turn ON. (See the *IP-Based Single Door Controller Quick Reference* for switch locations.)
2. After D19 is ON, release SW4.
3. D19 turns OFF when the ICT is manually enabled.

   The ICT is now enabled until the controller reboots.

To enable the ICT permanently:

1. Complete the steps to enable the ICT temporarily, as listed above.
2. Log on to the ICT.
3. From the *Controller Parameters* menu, select *Other Parameters*.
4. Deselect **Disable Integrated Configuration Tool**, then click **OK**.
5. To make this selection permanent, click **Save**, **Apply Changes**, then **Restart Controller**.

   The IPSDC performs a system reboot automatically and the ICT is permanently enabled.

To disable the ICT:

1. Log on to the ICT.
2. From the *Controller Parameters* menu, select *Other Parameters*.
3. Select **Disable Integrated Configuration Tool**, then click **OK**.
4. To make this selection permanent, click **Save**, **Apply Changes**, then **Restart Controller**. The controller performs a system reboot automatically and the ICT is permanently disabled.

Pre-Defined Operator Role Permissions

As discussed in Configuring Operator Roles on page 43, an operator role is a group permissions policy that can be used to expand or limit the User Interface pages that users can see, as well as the actions that users can perform in the System.

The various permission levels include:

- **None**: The operator cannot visit or view this page.
- **View**: The operator can see the page or data, but cannot make changes or execute commands.
- **Modification**: The operator can change settings.
- **Execute**: The operator can execute commands.

The following table provides the default permission levels for the System.

Feature	Permission Levels	Administrator	Operator	Guard	View Only	Dealer
Access Levels	None, View, Modification	Modification	Modification	View	View	Modification
Action Triggers: Administration	None, View, Modification	Modification	View	View	View	Modification

Feature	Permission Levels	Administrator	Operator	Guard	View Only	Dealer
Action Triggers: Monitor	None, View, Execute	Execute	Execute	Execute	View	Execute
Anti-Passback Reset	None, View, Execute	Execute	Execute	Execute	View	Execute
Areas	None, View, Modification	Modification	View	View	View	Modification
Backup Database	None, Execute	Execute	Execute	None	None	Execute
Camera PTZ Control	None, Execute	Execute	Execute	Execute	None	None
Card Formats	None, View, Modification	Modification	View	None	None	Modification
Credentials	None, View, Modification	Modification	Modification	View	None	Modification
Date and Time	None, View, Modification	Modification	Modification	View	View	Modification
Devices	None, View, Modification	Modification	View	View	View	Modification
Diagnostics	None, View	View	View	View	View	View
Doors (including IPSDC)	None, View, Execute	Execute	Execute	Execute	View	Execute
Email Configuration	None, View, Modification	Modification	View	None	View	Modification
Events	None, View	View	View	View	View	View
Firmware Updates	None, Execute	Execute	None	None	None	Execute
Holidays	None, View, Modification	Modification	Modification	View	View	Modification
Input/Output	None, View, Execute	Execute	Execute	Execute	View	Execute
Language Packs	None, View, Modification	Modification	None	None	None	Modification
Network Configuration	None, View, Modification	Modification	View	View	View	Modification
Network Share	None, View, Modification	Modification	View	View	View	Modification

Feature	Permission Levels	Administrator	Operator	Guard	View Only	Dealer
Operator Roles	None, View, Modification	Modification	View	View	View	View
Persons	None, View, Modification	Modification	Modification	View	View	Modification
Protected User Fields	None, View, Modification	Modification	None	None	None	None
Reader Groups	None, View, Modification	Modification	Modification	View	View	Modification
Reports	None, Execute	Execute	Execute	Execute	Execute	Execute
Restore Database	None, Execute	Execute	None	None	None	Execute
Save/Reset Settings	None, Execute	Execute	None	None	None	Execute
Scheduled Backups	None, View, Modification	Modification	View	None	None	Modification
Schedules	None, View, Modification	Modification	Modification	View	View	Modification
Security	None, View, Modification	Modification	View	View	View	Modification
System Options	None, View, Modification	Modification	View	View	View	Modification
User Accounts	None, View, Modification	Modification	View	None	None	Modification
User-Defined Fields	None, View, Modification	Modification	Modification	View	View	Modification
Video	None, View	View	View	View	View	None
Video Layouts	None, View, Modification	Modification	Modification	View	View	Modification

Port Usage

Hardware devices use ports to allow software applications to share hardware features without interfering with each other.

The following table provides port information for various devices in the System:

Device	Port	Usage
System Controller	TCP/22	Secure Shell (SSH) connection

Device	Port	Usage
System Controller	TCP/80	TruPortal User Interface and utilities
System Controller	TCP/443	TruPortal User Interface and utilities
System Controller	TCP/3001	Low-level firmware updates
System Controller	UDP/5353	Scan for Hardware Changes discovery
TruVision TVN 10	TCP/8000	Default port for video stream
TruVision TVN 20	TCP/8000	Default port for video stream
TruVision TVN 21	TCP/8000	Default port for video stream
TruVision TVN 50	TCP/8000	Default port for video stream
TruVision TVR 10	TCP/8000	Default port for video stream
TruVision TVR 11	TCP/8000	Default port for video stream
TruVision TVR 12	TCP/8000	Default port for video stream
TruVision TVR 30	TCP/80	Default port for video stream
TruVision TVR 31	TCP/80	Default port for video stream
TruVision TVR 41	TCP/8000	Default port for video stream
TruVision TVR 42	TCP/8000	Default port for video stream
TruVision TVR 60	TCP/8000	Default port for video stream

Pulse Duration Accuracy

When configuring action triggers that turn a pulse on or off, note that the accuracy of the pulse duration varies depending on the pulse length, as detailed in the following table:

Duration	Accuracy Range
1 second	1
2 seconds	2
3 seconds	3
5 seconds	5
10 seconds	10
15 seconds	15
20 seconds	00:19 – 00:20
30 seconds	00:29 – 00:30
45 seconds	00:45 – 00:46
60 seconds	00:59 – 01:00
90 seconds	01:23 – 01:32
2 minutes	01:53 – 02:02
3 minutes	02:53 – 03:02
5 minutes	04:43 – 05:12
10 minutes	09:43 – 10:12
15 minutes	14:43 – 15:12
20 minutes	19:43 – 20:12
30 minutes	29:43 – 30:12
45 minutes	44:43 – 45:12
60 minutes	00:59:43 – 01:00:12
90 minutes	01:20:43 – 01:40:42
2 hours	01:40:43 – 02:00:42
4 hours	03:40:32 – 04:00:42
6 hours	06:00:43 – 06:20:42
8 hours	08:00:43 – 08:20:42
10 hours	10:00:43 – 10:20:42
12 hours	12:00:43 – 12:20:42
16 hours	16:00:43 – 16:20:42
20 hours	20:00:43 – 20:20:42

1 day	0d:23:40:43 – 1d:00:00:42
7 days	7d:00:20:43 – 7d:16:20:42

Glossary

Access Level

One or more reader/schedule combinations, used to control hardware access by one or more cardholders. Access levels can be assigned to active badges to define which readers a badge has access to and at which times.

ANSI

Acronym for the American National Standards Institute, a voluntary organization that creates standards for the computer industry.

APB

An acronym for anti-passback. The prevention of a badge gaining entry in an access control system when that badge has either recently entered the same Reader or Area (Timed APB) or is not considered to be in the proper current Area required to gain entry into the new Area (Area APB). Put simply, it is a method of monitoring a cardholder's entry and exit actions to ensure that the person does not transfer the card to another individual to gain access.

Anti-Passback

Anti-Passback can be used to establish a specific sequence in which credentials must be used in order to gain access to an area.

Area APB

Areas are defined by the Readers that enter and leave them. The current Area in which a Badge is located is recorded. When a badge attempts to gain entry into a given Area via a given Reader, it is denied access if it is not recorded as currently being in the Area the given Reader is configured to be leaving.

Card Type

Categorizes card encoding technologies, such as Magnetic, Wiegand, Smart Card, First Access, etc.

Credential

An ID badge with an encoded number that can be added to the System and used to grant or deny access.

DHCP

Acronym for Dynamic Host Configuration Protocol. A communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol addresses in an organization's network.

Door Contact

A two-part device that is used by a card access system to indicate whether a door is open or closed. Typically, one part is mounted on the door and the other part is

mounted in a similar position on the door frame.

Door Holder

A device that holds a door in the open position until it is instructed by the System to change status.

Door Strike

An electrical and/or magnetic device that is used to hold a door in a locked position. Opening a door strike requires some form of electrical charge initiated from a device such as a card reader.

Ethernet

A network standard of LAN communication using either coaxial or twisted pair cable. IEEE 802.3 is the Ethernet standard. There are the following different types of Ethernet: 10 Mbps (Mega (million) bits per second); 100 Mbps; 1 Gbps (Giga (billion) bits per second)

Event

An historical record of activity tracked by the System, such as individuals who were granted or denied access, anti-passback violations, and alarms that occurred.

Facility Code

An optional badge field that uniquely identifies a location. Wiegand card vendors typically provide the facility code and store it in the cards. For other cards, facility code is user-defined. A card reader can be placed in Facility Code Only mode, requiring the facility code before access is granted.

HTTP

Acronym for Hyper Text Transfer Protocol. HTTP defines how messages are formatted and transmitted and controls what actions web servers and browsers should take in response to various commands.

IP

Acronym for Internet Protocol, specifies the format for packets and the addressing scheme on a network.

IP Address

An identifier for a computer on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.120.4.72 could be an IP address.

IP Camera

A digital video camera that connects directly to the network with its own IP address and has the ability to transmit images using a standard communications protocols such as TCP/IP. An IP camera does not need to be connected to a PC or a video capture card.

IPSDC

Acronym for IP-based Single Door Controller.

LAN

Acronym for Local Area Network. A LAN links client workstations within a limited area via high-performance cables so that users can exchange information, share peripherals, and draw on the resources of a secondary storage unit called a file server.

LDAP

Acronym for Lightweight Directory Access Protocol. LDAP is a software protocol commonly used to talk with servers that store user information, including digital certificates. It enables anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. A connection to an LDAP server may be unencrypted, or it may be encrypted using SSL.

National Television Standards Committee

Commonly referred to as NTSC it is the common television video-signal used throughout the United States, and Japan.

Network Share

A shared network resource, such as an FTP site or a network folder.

PAL

A video standard used in Europe, Australia, and New Zealand. PAL video broadcasts 625 lines every 1/25 second.

PIN

Acronym for personal identification number, a number typically associated with an individual and used for access control

PTZ

Acronym for Pan-Tilt-Zoom. A feature on cameras that can pan, tilt, and zoom via computer control. PTZ allows for a larger viewing area for a camera by allowing it to rotate in different directions.

Request to Exit

Request to Exit (RTE) devices are used to allow passage through locked doors from the protected side of controlled entry points. An RTE contact is typically a button located near the associated door. When a cardholder pushes the button, an RTE is sent to the panel.

Router

An intelligent 'hub' that allows multiple sub-nets to be connected together to share resources and data

SMTP

Acronym for Simple Network Management Protocol. A standard for transmitting email across IP networks.

SNMP

Acronym for Simple Mail Transfer Protocol. A method of managing various pieces of hardware, for example a printer, connected to a network.

SSL

Acronym for Secure Sockets Layer, a common protocol for authentication and encrypted communication on the Internet. SSL is used in communication with both web servers (HTTPS) and LDAP servers.

Subnet

A group of computers sharing the same network properties and network resources

Supervised

A door or enclosure wired with a continuity circuit so as to detect tampering.

TCP/IP

Acronym for Transmission Control Protocol/ Internet Protocol. A suite of communication protocols used to connect hosts on the Internet.

TCP/IP Port

Each process that wants to communicate with another process identifies itself to the TCP/IP protocol suite by one or more ports. A port is a 16-bit number, used by the host-to-host protocol to identify to which higher level protocol or application program (process) it must deliver incoming messages.

Unsupervised

A door or enclosure which is not wired with a continuity circuit so as to detect tampering.

URL

Acronym for Uniform Resource Locator. A URL is the address of a resource, or file, available on a TCP/IP network such as the Internet.

UTC Time

An acronym for Coordinated Universal Time, a time scale that joins Greenwich Mean Time (GMT) which is based on the Earth's inconsistent rotation rate, with highly accurate atomic time. When atomic time and Earth time approach a one second difference, a leap second is added to UTC time.

Wiegand

An access control technology that uses cards containing magnetically charged tungsten wires cut into strips and mounted vertically in columns.

Wizard

A program utility that is used, as a guide, to work step-by-step through a process.

Index