TruPortal™

SOFTWARE USER GUIDE

P/N 460808001C • REV 02.00 • ISS 02JAN13

Trademarks and patents

Interlogix, TruPortal, TruVision, and logos are trademarks of United Technologies.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

UTC Fire & Security Americas Corporation, Inc.
791 Park of Commerce Blvd, Suite 100, Boca Raton, FL 33487 3630, USA

Authorized EU manufacturing representative:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Version

This document applies to TruPortal version 1.0, Service Pack (SP) 1.

Certification

CE 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, UTC Fire & Security 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/customer-support

GNU Public Licenses

Linux Kernel 2.6.25, 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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

You may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Flex-IFrame

Permission is hereby granted, free of charge, to any person obtaining a copy of this Flex-IFrame software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so.

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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Copyright © 2001-2009 Robert A. van Engelen, Genivia Inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

mini_httpd is licensed under the Acme Labs Freeware License.

Redistribution and use in source and binary forms of mini_httpd, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache log4Net is licensed under the Apache License version 2.0.

A copy of the license can be retrieved at http://logging.apache.org/log4net/license.html.

Non-English versions of Interlogix documents are offered as a service to our global audiences. We have attempted to provide an accurate translation of the text, but the official text is the English text, and any differences in the translation are not binding and have no legal effect.

The software included in this product contains copyrighted software that is licensed under the GPL. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product, which will be no earlier than 2013-08-30, by sending a money order or check for $5 to the following address:

Interlogix
1212 Pittsford-Victor Road
Pittsford, NY 14534-3820

Please write “source for TruPortal” in the memo line of your payment. You may also find a copy of the source at http://www.interlogix.com. This offer is valid to anyone in receipt of this information.

CHAPTER 1 *Introduction* *1*

Conventions Used in this Documentation **1**

CHAPTER 2 *Configuring TruPortal Hardware* *3*

TruPortal System Architecture **4**

Document the Physical Location of Each Device by Serial Number **5**

Connect the TruPortal System Controller to a LAN or Local Workstation **6**

Configuring Your Local Client Workstation to Operate TruPortal. **6**

Install Microsoft .NET 4.0 Framework *7*

Install Bonjour Print Services *7*

Discovering, Configuring and Testing TruPortal Hardware **7**

Discover and Configure TruPortal Hardware *7*

CHAPTER 3 *Configuring TruPortal Software* *9*

Update the TruPortal System Controller Firmware **10**

Set the Date and Time **11**

Configuring Network Security **11**

Create a Security Certificate *11*

Upload a Security Certificate *12*

Enable SSL/HTTPS *12*

Configuring Security **13**

Configure Site Security *13*

Configuring Card Formats **14**

Add a Card Format *14*

Remove a Card Format *14*

Default Card Formats *14*

Configuring Devices **15**

Assign Meaningful Names to Discovered Hardware *15*

Configure TruPortal *15*

TruPortal Inputs and Outputs *16*

Configure Door Controllers *16*

Configuring Doors *16*

Configure Readers *21*

Reader Options *22*

Configure I/O Expansion Modules *22*

Configuring Video Devices **22**

Add a DVR *23*

Add a Video Camera *23*

Add Video Layouts *24*

Link Cameras to Devices to Track Video of Events *24*

Configuring Areas **24**

Add an Area *25*

Assign Readers to Areas *25*

Remove an Area *25*

Configuring Anti-Passback **26**

Configure Anti-Passback *26*
Creating Holiday Groups **26**
Add a Holiday Group *27*
Add a Holiday to a Holiday Group *27*
Copy Holiday Group *27*
Remove Holiday Group *27*
Creating Schedules **28**
Add a Schedule *28*
Add an Interval to a Schedule *29*
Remove an Interval from a Schedule *29*
Copy a Schedule *29*
Remove a Schedule *29*
Creating Reader Groups **30**
Add a Reader Group *30*
Copy a Reader Group *30*
Remove a Reader Group *30*
Configuring Access Levels **31**
Add an Access Level *31*
Copy an Access Level *31*
Remove an Access Level *31*
Configuring Operator Roles **31**
Add an Operator Role *32*
Modify an Operator Role *32*
Copy an Operator Role *32*
Remove an Operator Role *33*
Configuring User-Defined Fields **33**
Add User-Defined Fields *34*
Re-arrange User-Defined Fields *34*
Remove a User-Defined Field *34*
Schedule Door and Reader Behavior **34**
Import Persons and Credentials from a CSV File **35**
Create a Backup and a Restore Point **35**

CHAPTER 4 *Managing Access* *37*

Managing Persons **37**
Add a Person *38*
Remove a Person *38*
Upload Person ID Photos *38*
Managing Credentials **39**
Add a Credential *39*
USB Credential Readers *39*
Remove a Credential *40*
Managing Lost or Stolen Credentials **40**
Prevent Use of a Lost or Stolen Credential *40*
Restore a Found Credential *41*
Managing User Accounts **41**
Add a User Account *41*
Change a User Name and Password *42*
Deactivate a User Account *42*
Reports **42**
Searching for Persons **43**

Search Persons *43*
Cancel a Search *43*

CHAPTER 5 *Monitoring Access* *45*

Events and Alarms **45**
View Latest Events *46*
Load More Events *46*
Load All Events *46*
Search for Events *46*
Export Events *46*
Video of Events **47**
Replay Event Video *47*
Monitor Video *47*
Video Controls Reference *48*
Controlling Doors **49**
Open a Door *49*
Reinstate a Door *50*
Lock Out a Door *50*
Unlock a Door *50*
Reinstate all Doors *50*
Lock Out all Doors *50*
Unlock all Doors *51*
Door Commands Menus *51*
Event View Tab *52*
Schedule View Tab *52*
Door Degraded Mode *52*
Monitoring Inputs and Outputs **53**
Activate or Deactivate an Output *53*
Reset Anti-Passback **53**

CHAPTER 6 *Maintenance* *55*

Log Into TruPortal **55**
Preventing Data Loss **55**
Create a Backup *56*
Restore from a Backup *56*
Saving and Restoring Custom Settings **56**
Save Custom Settings *56*
Restore Custom Settings *56*
Reset Factory Settings *57*
Firmware Updates **57**
Reboot the TruPortal System Controller **58**
System Settings Page **58**
System Information Tab *58*
Date and Time Tab *58*
Network Configuration Tab *58*
Security Tab *59*
User-Defined Fields Tab *59*
Card Formats Overview **59**
Raw Formats *59*

CHAPTER 7 *Troubleshooting* ***61***

Clear the Internet Browser Cache **61**
Display Requirements **61**
System Capabilities and Limitations **62**
Summary of Pre-defined Operator Roles ***63***
Diagnostics **64**
Fuses ***67***
Hardware Problem States ***67***
Error, Warning and Event Messages **68**
Tamper States ***68***
Power and Battery Events ***68***
Backup Battery Events ***68***
Device Events ***69***
Door Tamper Events ***70***
Auxiliary Input Events ***70***
Auxiliary Output Events ***70***
"Objects Have Changed" Warning ***70***
"NTP Sync Failed" Event ***70***
Video Player Active X Errors **71**
No Active Video Connections ***71***
Internet Browser Fails to Load Login Page **71**

CHAPTER 1 *Introduction*

The TruPortal™ User Interface software is embedded on the TruPortal System Controller. TruPortal allows you to:

- Control access for up to 64 doors based on user-defined access schedules
- Configure schedules to include recurring holidays
- Add up to 10,000 users and badges to the system
- Monitor events remotely and automate linking of events to corresponding video on TruVision DVRs
- Open, lock, lock out and reinstate doors remotely
- Add reader schedules to help automate the system
- Enforce anti-passback
- Create reader groups

Conventions Used in this Documentation

The text in this manual is formatted to make it easy for you 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, which enable you 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].

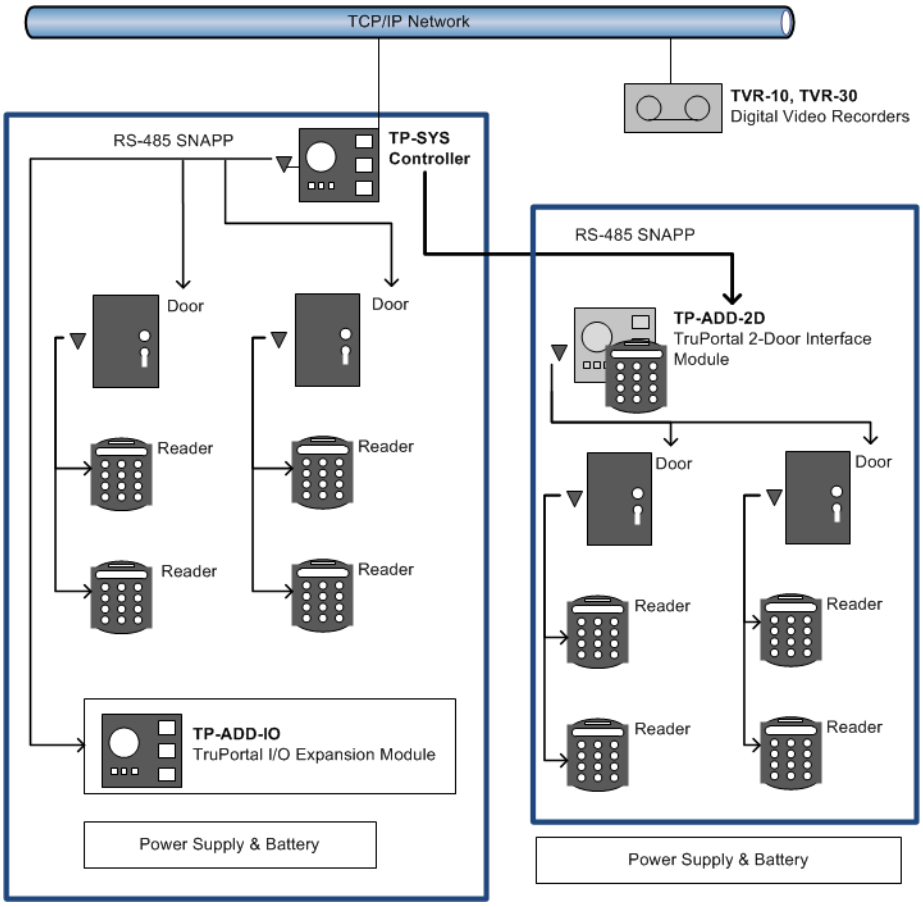
CHAPTER 2

Configuring TruPortal Hardware

Once the hardware devices for TruPortal are installed, you will need to configure the TruPortal System Controller.

Detailed configuration of optional functions is performed from the TruPortal User Interface. Before you can run that application, the TruPortal System Controller must be connected to the network, and must discover and test the inputs, outputs, doors and readers connected to it for proper wiring and installation.

TruPortal System Architecture



Document the Physical Location of Each Device by Serial Number

As each door configuration (locks, sensors, readers) is installed, provide a description for each, and list the serial numbers of devices associated with each door. This will assist you later in naming the devices, reader groups and areas when you configure the devices in the TruPortal User Interface.

Door Description	Reader Serial Numbers	Door controller Serial Numbers	I/O Expander 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:			

Door Description	Reader Serial Numbers	Door controller Serial Numbers	I/O Expander Serial Number	Linked Camera
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			
	In:			
	Out:			

See **Configuring TruPortal Software on page 9.**

Connect the TruPortal System Controller to a LAN or Local Workstation

There are two RJ-45 100BaseT ethernet jacks on the TruPortal System Controller. One is configurable, the other has a fixed IP (Internet Protocol) address. Please see the *TruPortal System Controller Quick Reference Guide* to identify the jacks.

If you are connecting directly from a local client workstation to the controller, use the static ethernet jack and a CAT-6 ethernet cable to connect it to the workstation.

If you are connecting the controller to a Local Area Network (LAN), use the configurable ethernet jack. Consult the site network administrator to connect the controller to the LAN.

Note: If you have multiple network appliances using 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 controller and the network drop.

Configuring Your Local Client Workstation to Operate TruPortal

The TruPortal User Interface resides on the TruPortal System Controller, so all that is needed to run the application is an Internet browser on the local client workstation.

However, the Discovery and Installation Wizard and the Import/Export Wizard are installed from a disc to a local workstation for purposes of configuring and testing the newly installed hardware, and uploading an existing personnel database (if any) to the controller.

Install Microsoft .NET 4.0 Framework

The TruPortal Utilities software will detect automatically if the .NET software is installed and display the word “Installed” next to the link if it is found.

1. Insert the TruPortal disc in your computer’s CD/DVD drive.

   Alternately, if you downloaded the disc image and extracted it to your computer’s hard disk drive, double-click on the **start.hta** application to launch the installer.
2. Click **.NET 4 Framework**.
3. Follow the instructions in the Microsoft .NET installer to complete the installation.

Install Bonjour Print Services

The TruPortal Utilities software will detect automatically if the Bonjour software is installed and display the word “Installed” next to the link if it is found.

1. Insert the TruPortal disc in your computer’s CD/DVD drive.

   Alternately, if you downloaded the disc image and extracted it to your computer’s hard disk drive, double-click on the **start.hta** application to launch the installer.
2. Click **Bonjour**.

   The Bonjour Services installation commences and finishes automatically.

Discovering, Configuring and Testing TruPortal Hardware

Note: Before TruPortal System Controller can be discovered using the Discovery and Installation Wizard, it needs to be connected to the local area network.

Discover and Configure TruPortal Hardware

1. Insert the TruPortal disc in your computer’s CD/DVD drive.

   Alternately, if you downloaded the disc image and extracted it to your computer’s hard disk drive, double-click on the **start.hta** application to launch the installer.
2. Click **Discovery and Installation Wizard**.
3. Select a **Language** and click [Next].

   The wizard will search the network for all TruPortal System Controllers.
4. Select the controller to configure from the list and click [Next].
5. Type the Administrator’s current **Password**.

   The default administrator **User Name** is “admin”

   The default administrator **Password** is “demo”
6. Choose a new password for the administrator.

IMPORTANT: The Administrator account has access to all aspects of the TruPortal configuration. Leaving default user names and passwords in place is dangerous. Anyone familiar with the product will know the defaults.

7. Type the password in the **New Password** and **Confirm Password** fields and click [Next].
8. Change the settings on the **Network Configuration** tab as directed by the site's network administrator.

   IMPORTANT: Operators will access the TruPortal User Interface by typing the TruPortal System Controller's IP address into their web browser address field. If the IP address of the controller is dynamic, then TruPortal operators must use a virtual URL or other alias to access the controller, for if the actual IP address assignment is changed by the network, the operators will not be able to find it.

   IMPORTANT: HTTPS is highly recommended. This secure hypertext protocol encrypts the packets between the users' browsers and the controller, preventing someone from gathering user information by spying on network traffic. There may be circumstances that require non-secured hypertext protocol (HTTP). For instance, if the TruPortal System Controller is accessed through a Web proxy server that does not support HTTPS (SSL) then the only option is to disable HTTPS/SSL.

9. Click [Next].

   The wizard will discover door controllers and I/O expansion modules connected to the TruPortal System Controller.
10. Click [Sync with PC] to set the correct time on the controller.
11. Select the appropriate **Global Input EOL Terminations** to indicate how the tamper circuits and sensors on the doors and readers are wired.
12. For each general purpose auxiliary input that is connected:
    a. Select a **Mode**.
    b. Observe the inputs to determine they are working and communicating with the controller.
13. For each general purpose auxiliary output that is connected:
    a. Click the icon next to the **State** to change state.
    b. Observe the outputs to determine they are working and being activated by the controller.
14. For each door controller, select the **Number of Doors** controlled.
15. For each door:
    a. Select the appropriate **Mode** for contact, request to exit and tamper circuits.
    b. Select commands from the **Door Control** list to test each door for proper installation and electrical wiring.
16. When you have tested all devices, click [Finish].

CHAPTER 3

Configuring TruPortal Software

TruPortal is designed so that, once configured, you can quickly add and remove persons and credentials, and manage access to your facility. During configuration, you will define the following:

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

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

1. **Update the TruPortal System Controller Firmware**.
2. **Check Diagnostics**.
3. **Set the Date and Time**.
4. **Create a Security Certificate**.
5. **Upload a Security Certificate**.
6. **Enable SSL/HTTPS**.
7. **Configure Site Security**.
8. **Add a Card Format**.
9. **Assign Meaningful Names to Discovered Hardware**.
10. **Configure TruPortal**.
11. Optional: **Configure I/O Expansion Modules**.
12. **Configure Door Controllers**.
13. **Configure Doors**.
14. **Configure Readers**.
15. Optional: **Add a DVR**.
16. Optional: **Add a Video Camera**.
17. Optional: **Link Cameras to Devices to Track Video of Events**.
18. Optional: **Add an Area**.
19. Optional: **Configure Anti-Passback**.
20. Optional: **Assign Readers to Areas**.
21. Optional: **Add a Holiday Group**.
22. Optional: **Add a Schedule**.
23. Optional: **Add a Reader Group**.
24. **Add an Access Level**.
25. Optional: **Add an Operator Role**.
26. Optional: **Add User-Defined Fields**.
27. Optional: **Schedule Door and Reader Behavior**.
28. **Import Persons and Credentials from a CSV File**.
29. **Create a Backup and a Restore Point**.

Update the TruPortal System Controller Firmware

1. Launch your Internet browser.
2. Download the latest TruPortal firmware update.
3. Log into TruPortal.
   a. Type the IP Address for TruPortal in the browser address bar.
   b. If you are using Internet Explorer and receive a warning about the security certificate, select **Continue to this website (not recommended)**.
   c. Type your **Username**.
   d. Type your **Password**.
   e. Select a **Language**.

f. Click [Log In].

4. Select ***System Administration > Firmware Updates***.
5. Click [Browse].
6. Navigate to and select the firmware update file.
7. Click [Update].
8. Check Diagnostics

Make certain there are no problems with the doors, controllers and other newly installed hardware by checking the TruPortal diagnostics screen.

See **Diagnostics on page 64.**

Set the Date and Time

TruPortal supports time synchronization with an NTP server. This option, if enabled in both TruPortal and your DVR, keeps your DVR(s) and TruPortal synchronized in time.Without this, TruPortal time may drift relative to DVR time and cause difficulty or inability to retrieve video related to an access event. The NTP client will attempt synchronization every hour.

Note: TVR10 does not support time synchronization with an NTP server.

Note: If the TruPortal 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.

1. Select System ***Administration > System Settings***.
2. Click the **Date and Time** tab.
3. Select your **Time Zone**.
4. Select your local **Date and Time**.
5. Optional: Synchronize time:
   a. Select [Synchronize with NTP server].

      NTP time synchronization requires access from the panel to the NTP server via UDP port 123. If this port is not accessible, the panel time will not synchronize with the NTP server, and “NTP Sync Failed” events will be logged.

   b. Type the IP address of the NTP server.
   c. Click [Sync now].

Configuring Network Security

The Network Configuration tab of the System Settings page allows you to assign a security certificate and configure the network properties, including secure browsing, for TruPortal.

Create a Security Certificate

1. Select ***System Administration > System Settings.***
2. Click the **Network Configuration** tab.
3. Click the [Create Certificate Signing Request] button.

The Certificate Signing Request dialog box appears.

4. Type the requested information and click [Generate].
   The CSR text appears in the text box on the right side of the dialog box.
5. To use a self-signed certificate:
   a. Click [Install Self-Signed Certificate].
   b. Reboot the controller when prompted.
6. To use a signed certificate:
   a. Copy CSR text and save to local file to send to a certificate authority of your choice.
   b. Close the Certificate Signing Request dialog box.
   c. See **Upload a Security Certificate on page 12.**

Upload a Security Certificate

1. Select ***System Administration > System Settings***.
2. Click the **Network Configuration** tab.
3. Click the [Import Certificate] button. The Upload Certificate dialog box appears.
4. Click [Select File].
5. Browse to and select the certificate file.
6. Click [Open].
7. Click [Upload].
8. Reboot the controller when prompted.

Enable SSL/HTTPS

IMPORTANT: Operating TruPortal without HTTPS security is not recommended. HTTPS encrypts communication between TruPortal and your client browser to ensure that intruders cannot intercept your communications and gain access to the server.

1. Select ***System Administration > System Settings***.
2. Click the **Network Configuration** tab.
3. Click the [Configure] button.
   The Network Properties property sheet appears.
4. Select **Enable HTTPS Connection**.

Note: There may be circumstances that require non-secured hypertext protocol (HTTP). For instance, if the TruPortal System Controller is accessed through a Web proxy server that does not support HTTPS (SSL) then the only option is to disable HTTPS/SSL.

Note: After enabling or disabling HTTPS/SSL, be sure to clear the browser cache, especially if using Firefox or Chrome.

Configuring Security

The Security tab of the System Settings page allows you to configure certain aspects pertaining to the physical security of your facility. Network security is addressed on the Network Configuration tab.

PIN Codes

TruPortal can be configured for access with a credential only, or with a credential and Personal Identification Number (PIN). Requiring people to present both 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 or Credential and PIN based on schedules. (See **Schedule Door and Reader Behavior on page 34.**)

Maximum PIN Length

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

PIN Retries

Allows persons a set number of chances to input their PINs correctly.

PIN Lock Out Time

If a person inputs 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 Degraded Mode

Credential information is stored on the TruPortal System Controller. If a door controller loses communication with the controller, it cannot verify credentials scanned at the readers against the database stored on the controller. In such a case the door controller must validate access requests if anyone is to enter the facility.

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 by TruPortal: 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.

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 be displayed telling the you that existing PIN numbers will be truncated to the new length. The prompt will allow you to continue or cancel the save operation.

4. Select the number of **PIN Retries**.
5. Select a **PIN Lock Out Time**.
6. Select a **Door Degraded Mode**:

- **Restricted**: No access is granted whatsoever
- **Site Code**: Access is granted if the card matches one of the formats defined on the Card Formats page, and the site code on the card matches the site code defined for the format
- **All**: Access is granted if the card matches any of the formats defined on the Card Formats page

7. Select an option for **Input EOL Terminations**.
8. 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 your configuration. The credential ID stored on the card includes a card number, a facility code, and an issue 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 you wish to remove.
3. Click [Remove].

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

Default Card Formats

TruPortal has the following credential formats installed by default:

- 37 Bit HID with Facility 40 (I10304)
- 37 Bit HID with Facility 50 (I10304)
- 37 Bit HID with Facility 60 (I10304)
- 4002 40 Bit (40 Bit CASI 4002)
- Raw 26 Bit (26 Bit Raw)

These formats can be removed if you need to add other formats. TruPortal can support up to eight active card formats.

Configuring Devices

After installing and connecting the hardware, the TruPortal System Controller will automatically discover all downstream devices and present these in a tree hierarchy on the Devices page. TruPortal will assign generic, sequential names to the devices it detects. These names should be replaced with meaningful names, to aid monitoring of access events. For example, “Door Controller (3)” might be renamed “Main Lobby, East Wall Doors.” To rename devices in this manner, you will need a record of each device’s serial number and installation location.

Device configuration involves more than just changing the names. Optional inputs and outputs, alarm timers, video monitoring, and extended timers for access by persons with disabilities are also from this page.

Note: To connect to a video camera or DVR, see **Configuring Video Devices on page 22**.

Assign Meaningful Names to Discovered Hardware

For a system of more than a few devices, it is recommended that you complete this task for all devices before proceeding with detailed device configuration. This will help you to keep track of where the devices are located in the facility as you proceed with detailed requirements.

Before beginning this task, obtain the site configuration chart showing where each device is physically located. See **Document the Physical Location of Each Device by Serial Number on page 5.**

1. Select ***System Administration > Devices***.
2. Select the TruPortal 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.
7. Type a descriptive **Device Name**.
8. Click [Accept Changes].
9. Repeat for each of the devices in the hierarchy.

Configure TruPortal

TruPortal 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 TruPortal System Controller.
3. Click the **General** tab.
4. Select a **Linked Camera** if one is configured to monitor the 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].

TruPortal Inputs and Outputs

Inputs and Outputs are general purpose options that allow you to tailor TruPortal to your needs. An input might be a signal from a motion detector, for example. An output is an electrical pulse from the TP controller to some device. Inputs and outputs are monitored from the ***Monitoring > Inputs/ Outputs*** page, and outputs can be activated manually from that page.

Configure Door Controllers

Door controllers can be connected to as many as four readers on two doors. 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 TruPortal 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.

Configuring 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 configured for an automatic opener and extended request to exit (RTE) to facilitate access by the disabled.

Configure Doors

1. Select ***System Administration > Devices***.
2. Expand the tree below the TP-Controller.
3. Expand the tree below the Door Controller.
4. Select the Door to configure.
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: Select any alarms the door is wired for:
    - **Door Held Open**
    - **Door Forced Open**
    - **Tamper**
14. Optional: If you have an alarm light or klaxon wired to the door, select “Door Held/Forced” from the **Aux Relay** list.
15. 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
16. Click [Accept Changes].
17. Repeat for each door.

Configure a Door for Disabled Access

TruPortal records events 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, TruPortal 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, TruPortal allows you to identify which credentials are granted this permission, and allows you 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 39.**

1. Select ***System Administration > Devices***.
2. Expand the tree below the TP-Controller.

3. Expand the tree below the Door Controller.
4. Select the Door to configure.
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: select any alarms the door is wired for:
    - **Door Held Open**
    - **Door Forced Open**
    - **Tamper**
14. 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**.
15. 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
16. Click [Accept Changes].
17. 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 TP-Controller.
3. Expand the tree below the Door Controller.
4. Select the Door to configure.
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: Select any alarms the door is wired for:
    - **Door Held Open**
    - **Door Forced Open**
    - **Tamper**
14. Select "**Mag Lock Bond Sense**" from the **Aux Input** list.
15. Optional: If you have an alarm light or klaxon 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
17. Click [Accept Changes].
18. 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.

Extended Grant Access Time
When a valid credential with the **extended strike/held times** option selected is scanned by the reader, the door will be unlocked for this length of time. This allows you to configure your system to comply with legislation and regulations governing access by individuals with disabilities.

See **Add a Credential on page 39.**

Door Held Time
When a valid credential is scanned by the reader, the door can be held open for this length of time. An event is recorded if a door is held open longer than that and the **Door Held Open** option is selected.

Extended Door Held Time
When a valid credential with the **extended strike/held times** option selected is scanned by the reader, the door can be held open for this length of time. An event is recorded if a door is held open longer than that and the **Door Held Open** option is selected. This allows you to configure your system to comply with legislation and regulations governing access by individuals with disabilities.

See **Add a Credential on page 39.**

Request to Exit Enabled

If the door is alarmed for being forced open, held open too long, and tampering, then Request to Exit 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.

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.

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.

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 you wish a physical alarm to occur if the door is forced.

Tamper

Select this option if the door is wired to detect tampering. If tampered with, an event will be recorded on the Events page.

Aux Input

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. TruPortal 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

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 Request To Exit (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.

Configure Readers

1. Select ***System Administration > Devices***.
2. Expand the tree below the TruPortal 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**

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 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 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.

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 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

TruPortal allows you to review video records of access events, by accessing the video recorded on a TVR10 or TVR30 from the cameras associated with the devices connected to the TruPortal System Controller. When an event happens at a device, TruPortal keeps a record of the date and time of the

event. If you have a camera linked to that device, TruPortal uses the event date and time to create a hyper link to the recorded video on the DVR the camera is attached to.

Note: TVR10 is available in the United States and Europe, TVR30 is available in the United States only.

Linking a camera to a device enables TruPortal to associate an event at that device with the video recorded from the camera during the time of the event. TruPortal does not control the camera or DVR directly, but it uses the information to tell the DVR 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). TruPortal allows you to control PTZ cameras if:

- You are using Internet Explorer as your browser
- You have ActiveX and.NET 4.0 installed or enabled in your browser
- The camera is connected to a TVR10 or TVR30

Add a DVR

TruPortal can connect to UTC Fire and Security TVR-10 and TVR-30 brand DVRs. These must be at the following firmware levels in order to work with TruPortal:

- TVR 30: 0617-0380-0625-6300 (or later)
- TVR 10: v2.3 build 100916 (or later)

Consult the TVR documentation for instructions to check and update firmware versions.

1. Select ***System Administration > Devices > Video Devices***.
2. Click [Add] and choose the appropriate DVR model.
3. Type a descriptive name for the DVR in the **Device Name** field.
4. Type the **IP Address** of the DVR.
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 DVR.

Add a Video Camera

Before performing this task, you must have added a TVR10 or TVR30 device to TruPortal.

Note: TVR10 is available in the United States and Europe, TVR30 is available in the United States only.

1. Select ***System Administration > Devices > Video Devices***.
2. Select the DVR 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 to which the camera is physically connected.

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

   If you are uncertain of the bandwidth, log into the DVR's Web-based interface 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 you wish to see 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.

Add Video Layouts

Video layouts determine how many camera inputs you can monitor from your 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 you have four cameras watching the loading dock area, you might 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 you link a camera to a reader, you 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 you link a camera to a door you will have a record of each access security incident.

Auxiliary inputs and outputs are optional devices connected to either the TruPortal System Controller or a TruPortal I/O Expansion Module. To link a camera to these devices, you must do so through the Input or Output tab of the appropriate controller.

1. Connect TruPortal (via your TCP/IP network) to the DVR and Camera.
   a. See **Add a DVR on page 23.**
   b. See **Add a Video Camera on page 23.**
2. Select ***System Administration > Devices***.
3. Select the device from the tree on the Devices page
4. Select the appropriate camera from the **Linked Camera** list.

Configuring Areas

Areas represent the spaces in the physical floor plan of your facility, specifically the entrances and exits to those spaces. Defining areas allows you 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 tracking of credentials.

Add an Area

Before you can assign readers to an area, you first must create the area.

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 you select "Never," you will have to reset an APB violation manually.
5. Click [Accept Changes].

Assign Readers to Areas

Assigning readers to areas is what defines areas in TruPortal. TruPortal records what reader a credential is scanned at, and based on area assignment, notes what 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 TruPortal detects a credential 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 you mistakenly assign 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. In this way TruPortal tracks what 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 (through a door held open by another person, for example), the TruPortal NGP-Controller will not know the person has left the specific area. As a result, if TruPortal 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.

Hard
The credential violating anti-passback 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, you have to add areas to TruPortal that match the areas in your site or floor plan, assign readers to those areas, and add credentials to TruPortal.

1. See **Add an Area on page 25.**
2. See **Assign Readers to Areas on page 25.**
3. See **Add a Credential on page 39.**

Note: The Credential pane of the Persons page (***Access Management > Persons***) allows you 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 TruPortal to override the regular schedule on those days. If you do not wish a holiday to override a certain schedule, then you need to include the holiday group in that schedule.

For example, your 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 office

staff and one for support staff (housekeepers and network administrators). Include the holiday group in the support staff schedule, but not in the office staff schedule. When configuring the support staff access level, assign the support staff schedule to the readers and reader groups that the support staff will use. When configuring the office staff access level, assign the office staff schedule to the readers and reader groups that the office staff will use.

Add a Holiday Group

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.
4. To add a holiday to the group, click [Add] in the holiday list pane and repeat step a.
5. Click [Accept Changes].

Add a Holiday to a Holiday Group

1. Select ***Access Management > Holidays***.
2. Select the holiday group you wish to modify from the list of holiday groups.
3. Add a holiday to the group:
   a. Click [Add] in the holiday list pane.
   b. 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.
4. Click [Accept Changes].

Copy Holiday Group

1. Select ***Access Management > Holidays***.
2. Select the holiday group you wish to copy from the list of holiday groups.
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 Holiday Group

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

1. Select ***Access Management > Holidays***.
2. Select the holiday group you wish to remove from the list of holiday groups.
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. 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.

TruPortal allows you to create up to 64 schedules and includes the following pre-defined schedules:

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

Note: 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). If you look at the pre-defined 24/7 schedule you will 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 you entered 12:00 AM as the start and end time, the schedule would be active for only59 seconds (from 12:00:00 to 12:00:59).

Time Intervals

An interval is the period of time during which a schedule is active. TruPortal schedules can be assigned multiple intervals.

For example, if your office cleaning staff washes and 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, you would create one interval for Wednesday and another for the other days of the week.

Add a Schedule

1. Select ***Access Management > Schedules.***
2. Click [Add].
3. Type a descriptive name in the **Schedule Name** field.
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 you wish to add to the interval.

c. Type values for the start and end times.

5. Click **Holiday Groups**.
6. 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 you created a holiday group for bank holidays and your business office is closed on those days, you would not select that holiday group for the schedule for your office workers access level. However, if your shipping department works on holidays, you would select the bank holiday group for the schedule for the shipping workers access level, thus preventing the bank holiday group from overriding the shipping schedule.
7. 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 you wish to add 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 you have a large number of readers and doors in your facility. Reader groups allow you 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 Levels page, allowing you 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 what doors a credential has access to and when. For example, if your facility has an office and a warehouse, and office workers are not allowed in the warehouse, then you would create an Access level for office workers which includes only those doors in the office area.

The 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.

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

If you have a great number of readers, creating a new access level can be time consuming. Copying an existing access level allows you 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 you wish to copy.
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 you do not want included in this access level.
7. Click [Accept Changes].

Remove an Access Level

1. Select ***Access Management*** > ***Access Levels***.
2. Click the access level you wish to remove.
3. Click [Remove].

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

Configuring Operator Roles

An operator role is a group permissions policy. When you add a person and grant that person the ability to login to and operate TruPortal, you will grant that operator 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 you to assign access privileges common to each type of operator based on their respective job roles. TruPortal includes five pre-defined roles:

- **View Only**
- **Guard**
- **Operator**
- **Dealer**
- **Administrator**

The five pre-defined roles cannot be deleted, but four can be modified. You can create custom roles as well. Custom roles can be deleted, but not if they are assigned to any users.

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 you 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 you wish to copy.
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: The five pre-defined roles cannot be deleted.

1. Select ***System Administration > Operator Roles***.
2. Select the role you wish to remove.
3. Click [Remove].
   The Remove Item dialog box appears.
4. Click {Remove].

Configuring User-Defined Fields

Person records in the TruPortal database can have user-defined fields associated with them. This allows you 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 Persons page. If you disable a field, 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 with TruPortal, you should have a person record identifier, such as an employee number, that is unique to each person in your 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 you create user-defined fields, you can designate them 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 you want users with the Operator role to view all personal information and users with the Guard role to view only non-protected personal information, you would 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 TruPortal database. A field must be enabled to appear on the 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].

Re-arrange User-Defined Fields

The user-defined fields are part of the Person records in the TruPortal database. A field must be enabled to appear on the Persons page. If you disable a field, 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 Persons page.

Remove a User-Defined Field

A field must be enabled to appear on the Persons page. If you disable a field, 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 you wish to delete.
4. Click [Accept Changes].

Schedule Door and Reader Behavior

The Schedule View tab on the Doors page is used to override default door and reader behavior according to a schedule. For example, during business hours you may want a public door, such as to a showroom or retail area, to be unlocked. After normal business hours, you may want certain readers to require both a credential and a PIN (useful to prevent access with lost or stolen credential cards) so you configure the reader 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 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 13.**)

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**

Import Persons and Credentials from a CSV File

The Import/Export Wizard allows you to map the fields of a comma-separated-values (CSV) file to the TruPortal database table, and import the persons and credentials.

Note: A TruPortal 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 TruPortal. Import and Export of TruPortal user account data is not supported. Only user-defined personal data and credential data can be imported and exported.

See “Import Persons and Credentials from a CSV File” in the *TruPortal Import/Export Wizard User Guide*.

Create a Backup and a Restore Point

After you have completed the configuration of TruPortal, it is important to create both a backup file, stored on your local PC and a restore point (saving your custom settings) stored on the controller, in case you need to restore the system to its initial operating state.

See **Preventing Data Loss on page 55.**

CHAPTER 4 *Managing Access*

You manage who has access to your facility and TruPortal by:

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

Managing Persons

Each individual in your organization can have access to the building and access to TruPortal. Access to the physical facility is controlled by means of a credential (commonly called an ID badge). Access to TruPortal is controlled by means of a user account to log into the controller. To keep the user accounts and credentials organized, TruPortal associates both with one record for each individual in your 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 your facility will need a credential (an ID badge with an encoded number that is recognized by TruPortal). However, not everyone who needs access to the facility will also need access to TruPortal with a user account. Second, only those who operate and manage TruPortal will need user accounts. Third, in some cases, TruPortal 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,” in TruPortal allow you 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

Be sure to assign each person record a unique identification number of some kind. This may be an employee number, for example.

Before adding persons, be sure to configure any user-defined fields which you may require. See **Add User-Defined Fields on page 34.**

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 TruPortal software, click the **User Account** tab and create the account. See **Add a User Account on page 41.**
7. Click [Accept Changes].
8. If the person requires a credential for access to the physical facility, see **Add a Credential on page 39**.

Remove a Person

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

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

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 Person ID Photos

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.

Photos are limited to 10KB or less in size.

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: You can replace a user ID photo with an updated photo by clicking the existing photo and following these steps.

Managing Credentials

Everyone who needs to enter your facility will need a credential (an ID badge with an encoded number that is recognized by TruPortal). Before you can assign a credential, you must first add the person to the database. See **Add a Person on page 38.**

Add a Credential

Before you can add a credential to a person, you must first create a record for that person. See **Add a Person on page 38.**

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**.
7. Optional: type the **PIN** code.
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 you are 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].

USB Credential Readers

RF IDeas manufactures credential card readers that can connect with a computer via USB. These devices can be used to read the data stored on an ID badge and automatically insert the credential into the **Credential ID** field. This can be a considerable time saver if you have many credentials to add to TruPortal.

These devices must be installed and configured according to the manufacturer's instructions, and if you are using credentials with a facility code, the RF readers must be configured to separate the facility code from the credential code on the card.

Remove a Credential

You need not remove a credential to prevent its use. For example, if an individual reports a lost credential, rather than delete the credential right away, you can deactivate it 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, you can remove the lost credential. See **Prevent Use of a Lost or Stolen Credential on page 40.**

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].

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

Managing Lost or Stolen Credentials

If an individual reports a lost credential, rather than delete the credential right away, you can deactivate it 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, you can remove the lost credential.

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 you have video cameras monitoring door and reader events, you will have an image of the person who attempted to use the credential after it was reported stolen. 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. In this way you may be able to help 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 TruPortal. 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

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. Select **Can log on**.
6. Type a **User Name**.
7. Click [Change 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. 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. Type a new **User Name**.
6. Click [Change 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].

Reports

TruPortal has five pre-defined reports to allow you to view information stored in the server database:

Access History
Allows you to view a summary of access attempts by person, filtered by Date Range, Person Name (wildcard), Reader, Area and Grant or Deny.

Credential
Allows you to view a list of credentials assigned, filtered by Person Name (wildcard), Credential ID (wildcard), Access Levels, Active or Inactive.

Reader Access
Allows you to view a list of Persons with access to each reader, filtered by Person Name (wildcard), Reader.

Roll Call
Allows you to view a list of Persons by current area or last reader, filtered by Person Name (wildcard), Area, Reader.

Roster
Allows you to view a list of all Persons in the database, filtered by Person Name (wildcard) and Login privileges.

Note: Reports are displayed in HTML format, in an internet browser window. The TruPortal product logo appears in the upper right corner. If you are using Internet Explorer 7 or earlier, this image will not display properly. This is a limitation of older versions of Internet Explorer.

Searching for Persons

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

Search Persons

1. Select ***Access Management > Persons***.
2. Click the **Search** button to select which field to search.
3. Type your search term.
4. Press <Enter>.

Cancel a Search

The Search results will continue to filter the database, even if you navigate to another page and return to the Persons page, until you cancel the search.

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

CHAPTER 5 *Monitoring Access*

During day to day operations you will monitor and control facility access by:

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

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 TruPortal
- System and device status messages
  - Changes in system state, such as updates to the Time and Date
  - Mode changes for attached devices
- Alarms
  - Door tampering
  - Doors forced open
  - System failures or problems

Any event associated with a device linked to a camera will have a video record of the event.

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, you can view a summary of the event, including a thumbnail photo of the person associated with the event by moving your 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 display is limited to the most recent events. To view older events than those displayed, you must first load them to your browser from the TruPortal. 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 **Events** action button.
3. Select **Load More Events**.
4. Optional: to stop the operation, click **Cancel** when it appears.

Load All Events

The Events display is limited to the most recent events. To view older events than those displayed, you must first load them to your browser from the TruPortal. The Load All Events command will load all of the events on the Controller to your browser, and may take several minutes to complete.

1. Select ***Events***.
2. Click the **Events** action button.
3. Select **Load More Events**.
4. Optional: to stop the operation, click **Cancel** when it appears.

Search for Events

The search feature allows you 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 screen.
3. Type search criteria in the appropriate fields.

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

Export Events

TruPortal 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 **Events** action button.
3. Select **Export Events**.
4. Choose the location on your computer where you wish the file saved.

5. Type a descriptive filename with the extension **.csv**.
6. Click **Save**.

Video of Events

TruPortal 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 22.**

Links to event-specific video are found on the Events page. The Video page allows you to monitor the video feed from one or more cameras.

Replay Event Video

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

FIGURE 1. Event Video Camera Icon

1. Select ***Events***.
2. Scroll to or search for the event.
3. Click the Camera icon.
   The Event Detail pane appears at the bottom of the page.
4. Click [Play Event Video].

Monitor Video

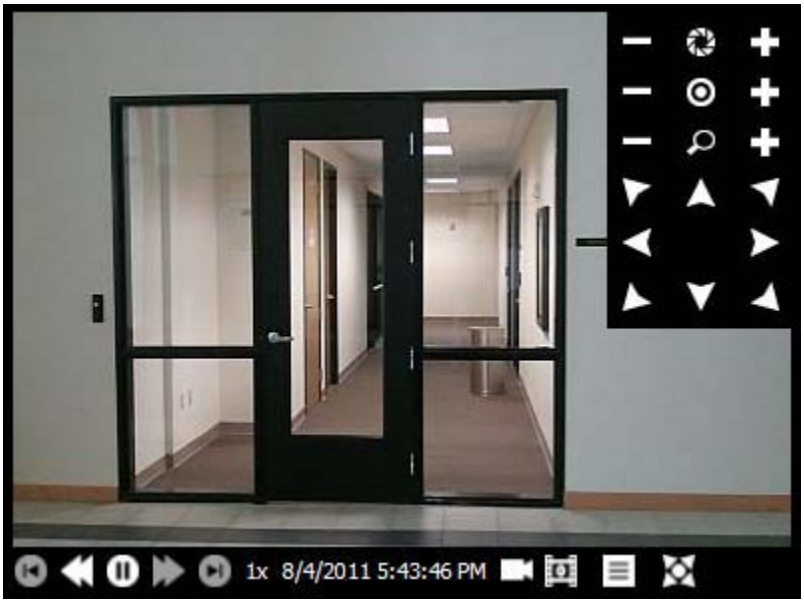
While the Events screen lets you view recorded video of events linked to specific devices, the Video page lets you monitor overall site security. For example, if a suspicious person were lurking in your parking lot, this would not trigger a door or reader event, but if you have a camera watching the parking lot you would detect the person by watching that camera.

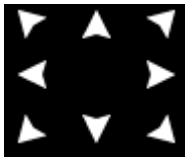
Before you can monitor live or recorded video, you must add at least one video layout. See **Add Video Layouts on page 24.**

1. Select ***Monitoring > Video***.
2. Select a **Layout**.
3. To view live video, click the **Live** button.
4. To view recorded video, click the **Playback** list and select an option.
5. Optional: To reposition a Pan-Tilt-Zoom camera, click the **PTZ** button to open and adjust the PTZ controls.

Video Controls Reference

FIGURE 2. TruPortal Video Monitoring Controls



Icon	Feature	Function
	Iris control	opens or closes the camera iris to adjust for the amount of light available
	Focus control	adjusts the image focus
	Zoom control	adjusts the camera's zoom
	Pan and Tilt controls	Moves the camera in the direction(s) indicated by the respective arrow
	Single Step Backward control	Moves the recorded video back one frame

Icon	Feature	Function
	Reverse control	Moves the video backward
	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 video control	Switches from playback of recorded video to viewing live video
	Playback control	Menu selection of playback options, from live to several minutes in the past
	Presets control	Quickly moves the camera to preset location
	PTZ control	Opens the Pan, Tilt, Zoom controls (only works with PTZ cameras)

Controlling Doors

The **Doors** page shows the status of the doors, the assigned readers, recent events at those doors, and the assigned schedules. The **Doors** 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 you wish to open.
4. Select **Open 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 you wish to reinstate.
4. Select **Reinstate Door**.

Lock Out a Door

Use the Lock Out Door command 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 you wish to lock out.
4. Select **Lock Out 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 you wish to unlock.
4. Select **Unlock Door**.

Reinstate all Doors

Use the Reinstate All Doors command to return all doors to their normal mode of operation after unlocking all doors or locking out all doors.

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

Lock Out all Doors

Use the Lock Out All Doors command to prevent any credentials from being granted access at any door.

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

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.

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

Door Commands Menus

Sometimes it is necessary to override normal scheduled behavior for a specific door, or for the entire site. For example, you might need to open a door for a package delivery person. During a fire drill you would unlock all doors to facilitate the drill. If some disaster or emergency situation occurred near your facility you might need to lock out all doors. You can control individual doors from the **Event View** tab of the ***Monitoring > Doors*** page. The global door commands allow you with one click to change the state of all doors on the site.

Global Door Commands Menu

Note: After unlocking all doors or locking out all doors, you must 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, you must reinstate all doors before you can control an individual door directly.

Lock Out 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, you must reinstate all doors before you can control an individual door 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.

Reinstate Door
Restores the door to default behavior based on the schedule.

Lock Out Door
Locks the doors and ignores credentials, so that no one can enter or exit.

Unlock Door
Releases the lock on the door, allowing free access and egress, until you change the door state, a reader schedule changes the door state, or you execute a global (“all doors”) command.

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. You can control individual doors from the **Event View** tab of the ***Monitoring > Doors*** page.

Schedule View Tab

The **Schedule View** tab on the ***Monitoring > Doors*** page allows you to modify door and reader behavior according to schedules, rather than manually as you would do on the **Event View** tab.

For example, if you have a customer showroom, you would want the door from the parking lot to the showroom locked when the business was closed, but unlocked during business hours when a salesman was in the showroom, so customers can easily enter the building. In this case you might select a door schedule for 9:00 AM to 5:00 PM and choose "First Card In" for the **Schedule Mode**, if you wanted the showroom 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.

Door Degraded Mode

Credential information is stored on the TruPortal 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 degraded 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.

Monitoring Inputs and Outputs

Inputs and Outputs are general purpose options that allow you to tailor TruPortal to your needs. An input might be a signal from a motion detector, for example. An output is an electrical pulse from the TP controller to some device. Inputs and outputs are monitored from the ***Monitoring > Inputs/Outputs*** page, and outputs can be activated manually from that page.

Activate or Deactivate an Output

1. Select ***Monitoring > Inputs/Outputs***.
2. Click the Activate/Deactivate button for the Output.
   The State changes from “Off” to “On,” or “On” to “Off.”

Reset Anti-Passback

Anti-Passback requires a credential be used to enter and exit an area. In this way the system tracks what 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), TruPortal will not record that the person has left the specific area. As a result, if TruPortal 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 6 *Maintenance*

A few simple maintenance activities will help make sure your TruPortal system runs efficiently with minimal trouble or disruption to service. These include making backups of the database and controller configuration settings and updating the firmware (the TruPortal User Interface software installed on the TruPortal System Controller).

Log Into TruPortal

1. Launch your Internet Browser.
2. Log into TruPortal.
   a. Type the IP Address for TruPortal in the browser address bar.
   b. If you are using Internet Explorer and receive a warning about the security certificate, select **Continue to this website (not recommended)**.
   c. Type your **Username**.
   d. Type your **Password**.
   e. Select a **Language**.
   f. Click [Log In].

Preventing Data Loss

Periodic backup of your TruPortal database is highly recommended to ensure quick recovery of your security needs following a disaster. TruPortal saves backups to your local computer, so you have a copy that is not on the controller. The backup file is encrypted. The backup file includes all records and settings that you can configure in TruPortal with the exception of:

- Network configuration settings
- Door/reader states set manually via the Door page

Create a Backup

1. Log into TruPortal.
2. Select ***System Administration > Backup/Restore Database***.
3. Click [Download Backup File].
   The Backup Database dialog box appears.
4. Click [Download Backup File].
5. Select a location for the file.
6. Click [Save].

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 TruPortal.
2. Select ***System Administration > Backup/Restore Database***.
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

Unlike a backup, custom settings are stored on the TruPortal System Controller. The custom settings file includes all settings and data. This is like a custom default state. Instead of resetting the controller to a factory default state, which would then have to be reconfigured to your specific requirements, you can save your basic site configuration as a custom setting and reset to that, should the need ever arise.

Save Custom Settings

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

1. Select ***System Administration > Save/Reset Settings.***
2. Select **Save Custom Settings**.
3. Type your **Username**.
4. Type your **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 in TruPortal and reset it to the settings stored in the custom settings file. Be sure you have a current backup before restoring custom settings.

IMPORTANT: After restoring custom settings, the 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 you have not configured a **Door Degraded Mode** that allows access when the controller is offline.

1. Select ***System Administration > Save/Reset Settings.***
2. Select **Restore Custom Settings**.
3. Type your **Username**.
4. Type your **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 your browser will display its default page when it cannot connect to a web address.
7. Clear your browser cache. (In Internet Explorer 8+, press <Ctrl>+<Shift>+<Delete>.)

Reset Factory Settings

IMPORTANT: Using this feature will erase all settings and data in TruPortal and reset it to factory defaults. Be sure you have a current backup before resetting the system.

1. Select ***System Administration > Save/Reset Settings***.
2. Select **Reset Factory Settings**.
3. Type your **Username**.
4. Type your **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 your browser will display its default page when it cannot connect to a web address.
7. Clear your browser cache. (In Internet Explorer 8+, press <Ctrl>+<Shift>+<Delete>.)

   When the server comes back online, the End User Software License Acceptance Form will be displayed.
8. Click **Accept**.

Firmware Updates

The TruPortal software resides on the controller circuit board itself. Periodic software updates are applied to the controller using the Firmware Updates feature.

1. Launch your Internet browser.
2. Download the latest TruPortal firmware update.
3. Log into TruPortal.
   a. Type the IP Address for TruPortal in the browser address bar.

b. If you are using Internet Explorer and receive a warning about the security certificate, select **Continue to this website (not recommended)**.
c. Type your **Username**.
d. Type your **Password**.
e. Select a **Language**.
f. Click [Log In].

4. Select ***System Administration > Firmware Updates***.
5. Click [Browse].
6. Navigate to and select the firmware update file.
7. Click [Update].

Reboot the TruPortal System Controller

1. Select ***System Administration > Devices***.
2. Select the controller from the device list.
3. Click [Reboot Controller].

System Settings Page

The System Settings page is divided into five tabs. The System Information tab is displayed by default.

System Information Tab

This tab is informational only, and displays the application firmware revision; UI firmware revision and Kernel firmware revision. The Application and UI firmware revisions should be the same.

Use this version information for technical support, and to determine when to upgrade to a newer version of the firmware.

Date and Time Tab

The date and time are used to synchronize the events with video of the same, and to implement scheduled door and reader behavior.

Note: If you manually change the time to within one minute of a schedule period, or the NTP feature does so automatically, then the schedule will take effect immediately instead of at the designated minute.

See **Set the Date and Time on page 11.**

Network Configuration Tab

This tab shows the network settings for TruPortal. From this tab you can create a secure certificate for secure hypertext transfer protocol (https), import a security certificate, and configure the Internet protocol (IP) address, subnet mask, default gateway and domain name server (DNS), as needed by the specific site network settings.

See **Configuring Network Security on page 11.**

Security Tab

The Security tab of the System Settings page allows you to configure certain aspects pertaining to the physical security of your facility. Network security is addressed on the Network Configuration tab.

See **Configuring Security on page 13.**

User-Defined Fields Tab

This tab allows you to create custom fields for person records, to arrange their order on the display, and protect fields containing sensitive information.

Person records in the TruPortal database can have user-defined fields associated with them. This allows you 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 Persons page. If you disable a field, it will be removed from the database, and all data contained in that field for each Person record will be lost.

See **Configuring User-Defined Fields on page 33.**

Card Formats Overview

Before a credential can be recognized, TruPortal must be configured to recognize the card format—the way the data is formatted on the ID badge.

TruPortal is pre-configured for 16 popular commercial card formats, and supports up to eight card formats active simultaneously. If the card format you use is not listed, you can add it as a custom type.

Raw Formats

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 you use a facility code and a door goes into degraded mode because it cannot communicate with TruPortal, 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.

CHAPTER 7 *Troubleshooting*

Clear the Internet Browser Cache

Clearing the cache and restarting your browser can solve many apparent problems, such as sudden strange behavior in the TruPortal software. Specific steps vary by browser make and version.

1. Log out of TruPortal and return to your home page.
2. Clear your browser history and cache.
3. Close your browser and reopen.
4. Log into TruPortal.

Note: After enabling or disabling HTTPS/SSL, be sure to clear the browser cache, especially if using Firefox or Chrome.

Display Requirements

The TruPortal application runs in an Internet browser. For optimum viewing, you should:

- Use Internet Explorer 8+
- Open the browser window to full screen (a minimum width of at least 1024 pixels is necessary to avoid scrolling)
- Set your display resolution to a minimum of 1024 pixels wide

System Capabilities and Limitations

Attribute	TP-
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
Number of retained events in event log	65,000
Doors/Readers	
Number of doors (base board and dual door controllers) with readers in / Number of doors with readers in and out	64 / 32
TP-ADD-2D-BRD Dual Door Control Modules (including built in)	32
Readers (total)	64
Inputs/Outputs	
Total number of system inputs (including TruPortal System Controller)	132
Total number of system outputs (including TruPortal System Controller)	66
Total number of TP-ADD-IO or TP-ADD-IO-BRD Input/Output Expansion Add-Ons	8
DVR/Cameras	
DVRs	4
Cameras per DVR	
TVR10 (EMEA & US)	4
TVR30 (US Only)	16
Cameras (maximum)	64

Attribute	TP-
Ethernet ports (total/supported)	2/1
RS-485 SNAPP bus ports	4

Note: TVR10 is available in the United States and Europe, TVR30 is available in the United States only.

Summary of Pre-defined Operator Roles

Permission Levels:

- **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 / Execute**: The operator can modify settings or execute command

Permission	Permission Levels	Administrator	Operator	Guard	View Only	Dealer
Access Levels	None, View, Modification	Modification	Modification	View	View	Modification
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	None, View, Execute	Execute	Execute	Execute	View	Execute
Events	None, View	View	View	View	View	View
Firmware Updates	None, Execute	Execute	None	None	None	Execute

Permission	Permission Levels	Administrator	Operator	Guard	View Only	Dealer
Holidays	None, View, Modification	Modification	Modification	View	View	Modification
Input/Output	None, View, Execute	Execute	Execute	Execute	View	Execute
Network Configuration	None, View, Modification	Modification	View	View	View	Modification
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
Reset Settings	None, Execute	Execute	None	None	None	Execute
Restore Database	None, Execute	Execute	None	None	None	Execute
Schedules	None, View, Modification	Modification	Modification	View	View	Modification
Security	None, View, Modification	Modification	View	View	View	Modification
System Information	None, View	View	View	View	View	View
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

Diagnostics

TruPortal provides informational diagnostics; there are no actions you can perform to run specific diagnostic tests. The Diagnostics page has visual indicators for common failure modes that help you to identify and solve problems. All information will be queried at login time and every minute

thereafter. You can manually refresh the data by clicking [Refresh].The page displays the last time the screen was updated.

Note: The TruPortal System Controller cannot display an accurate reading for DC current when the system is powered by a DC source. The DC current information will only be displayed when the TruPortal 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 TruPortal System Controller board for use by external peripherals.

Fuse	+V	0V
Aux 1	CN3.1	CN3.2
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

Error, Warning and Event Messages

Tamper States

The TruPortal 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 Diagnostics page or by using the Installation Wizard.

Power and Battery Events

TruPortal System Controller Shuts Down on Battery Power

If the controller is operating on battery power only and the battery voltage drops below 10.2 volts, the controller will shut down until AC power is restored.

See **Backup Battery Events on page 68.**

AC Power Events

Event Code	Event Description
Event 14626	AC Power Failed
Event 14627	AC Power Restored

Note: The TruPortal System Controller cannot display an accurate reading for DC current when the system is powered by a DC source. The DC current information will only be displayed when the TruPortal System Controller has AC power.

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 is powered exclusively off backup battery, the system 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 SNAPP bus communications with a configured downstream device is 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 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 you local browser cache may become out of synchronization with TruPortal. When this happens, the interface will be disabled, and the warning message will appear.

Click the text of the warning to reload the page.

“NTP Sync Failed” Event

NTP time sync requires access from the panel to the NTP server via UDP port 123. If this port is not accessible, the panel time will not sync with the NTP server, and “NTP Sync Failed” events will be logged.

Video Player Active X Errors

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 has not been configured
- the TruPortal application has lost communication with a connected DVR
- the ActiveX control needed to view video has not been installed or is out of date

Note: Video can only be viewed on Internet Explorer.

If the error message is displayed when you click a camera icon next to an event:

1. Click [Play Event Video].
2. Either the video is displayed or the ActiveX control is installed.
3. If neither happens and the message persists, verify the DVR and camera are operating:
   a. See **Configuring Video Devices on page 22.**
   b. See **Link Cameras to Devices to Track Video of Events on page 24.**.

If the error message is displayed when you select *Monitoring* > *Video*:

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 you were viewing.
   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 the camera is added to the Devices page and operating:
   a. See **Configuring Video Devices on page 22.**
   b. See **Add a Video Camera on page 23.**
   c. See **Add Video Layouts on page 24.**

Internet Browser Fails to Load Login Page

After changing between secured (HTTPS) and normal hypertext protocol (HTTP), you may notice that Firefox or Chrome will not load the TruPortal System Controller login page.

See **Clear the Internet Browser Cache on page 61.**

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
Short 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.

Area APB
Areas are defined by the Readers that enter and leave them. The current Area a Badge is located in 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.

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)

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.

LAN

Acronym for Local Area Network. Linkage of personal computers within a limited area by high-performance cables so that users can exchange information, share peripherals and draw on the resources of a massive 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.

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.

Router
An intelligent 'hub' that allows multiple sub-nets to be connected together to share resources and data

SNMP
Acronym for Simple Network Management 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.

Sub-net
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.

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

Symbols

.NET 7
.NET 4.0 23

Numerics

1 Gbps 74
10 Mbps 74
100 Mbps 74
100BaseT 6

A

AC Power Events
  Event 14626 68
  Event 14627 68
Access History report 42
Access Level 35, 73
Access Levels page 28, 30, 31, 35
Activate
  credential 40
Active From 39
Active On/Off 22
Active To 39
Active X Errors 71
ActiveX 23
Add
  access levels 31
  area 25
  card formats 14
  credential 37
  digital video recorder 23
  holiday groups 26
  ID photos 38
  operator roles 31
  persons 37
  reader groups 30
  schedules 28
  user accounts 37
  user-defined fields 33
  video camera 23
  video layouts 24
Admin 63
Administrator 32
  change password of 7
  user account 7
ANSI 73
Anti-passback 20, 25, 45, 53
  configuring 26
Anti-Passback Exempt 39
Anti-Passback Reset 53
APB 73
Application firmware revision 58
Area APB 73
Area Definition page 25
Aux Input 20
Aux Relay 17, 20
Aux Relay On Time 18, 21
Auxiliary Input Events
  14640 70
  14641 70
  14642 70
  4170 70
Auxiliary Output Events
  10240 70
  11264 70

B

Backup 35
Backup Battery Events 68
  14612 68
  14613 68
  14624 68
  14625 68
  14649 68
Backup Database dialog box 56
Badge ID 35
Bonjour Print Services 7
Browser cache 61

C

Can log on check box 42
Card formats
  configure 14
Card Formats page 14, 53
Card Type 73
CD/DVD drive 7
Certificate Signing Request dialog box 12
Change
  passwords 41
Comma Separated Values 35, 46
Configure
  access levels 31
  anti-passback 26
  area 25
  areas 24, 25
  card formats 14
  credential 37
  date and time 11, 70
  devices 24
  door 17
  door options 19
  doors 16
  DVR 22, 23
  event video 24
  NTP server time synchronization . 11, 70
  operator roles 31
  persons 37
  Persons page 33
  reader groups 30
  readers 21, 22
  schedules 28

TruPortal controller 7
user accounts 37
user-defined fields 33
video camera 22, 23
video layouts 24
Conventions 1
Credential
activate 40
deactivate 40
limited duration 40
lost or stolen 40
report 42
Credential and PIN 22, 52
Credential Only 22, 52
Credential pane 26
Credentials 35
managing 37
CSV 35

D

Database record number 33
Date 11
Date and Time tab 58
DC power 67
Deactivate
credential 40
Dealer 32, 63
Default 25
Default Area 25
Default gateway 58
Device Events
Event 14622 69
Event 14623 69
Event 14628 69
Event 14629 69
Event 14643 69
Event 4105 69
Event 4106 69
Event 4107 69
Device Name 15
Devices page 15, 17, 18, 34, 58
Door 51
DHCP 73
Diagnostics page 64
Disabled access 17
Discovery and Installation Wizard 7
Domain Name Server (DNS) 58
Door
supervised 75
unsupervised 75
Door Contact 18, 19, 73
Door Degraded Mode 13
All 13
Restricted 13
Site Code 13
Door Held Open 19
Door Held/Forced 17, 19, 21
Door Holder 73
Door Opener 20
Door Strike 74
Door Strike Mode 17, 18, 21
Door Tamper Alarm 70
Door Tamper Events
Event 14632 70
Event 14633 70
Door Tamper Restored 70
Doors
commands menus 51
Event View tab 52
monitoring 34
Schedule View tab 52
Doors page 28
Schedule View tab 34
DVR 11

E

Employee number 33
Enable HTTPS Connection 12
End User Software License Acceptance Form 57
Enter new password field 41
Ethernet 6, 74
Event 10240 70
Event 11264 70
Event 14612 68
Event 14613 68
Event 14618 69
Event 14624 68

Event 14625 68
Event 14640 70
Event 14641 70
Event 14642 70
Event 14644 51
Event 14646 51
Event 14649 68
Event 14651 69
Event 14652 69
Event 4170 70
Events
exporting 46
lost or stolen credentials 40
NTP Sync Failed 11, 70
video 47
video of 24
viewing 46
Events page 45, 47, 71
Export
events 46
Extended Request to Exit
(RTE) 17, 18, 19, 20
extended strike/held times 19

F

Facility Code 74
Facility code 14
Field 34
Filter
persons list 43
Firmware Updates page 57
First Access 73
From Area 25
Fuses 67

G

General purpose
inputs 8, 15, 16
outputs 8, 15, 16
General tab 15
Global Input EOL Terminations 8
Group permissions
operator roles, example of 33
Guard 32, 63

H

Holidays
custom 27
repeats yearly 27
single 27
Holidays page 26
HTTP 74
HTTPS 8, 12, 58, 75

I

ID badge 35
ID number 33
ID Photos 38
IEEE 802.3 74
Import Certificate button 12
Import/Export Wizard 7
Input EOL Terminations 13
Input Types
normally closed 21
normally open 21
supervised 21
unsupervised 21
Inputs
auxiliary 53
monitoring 53
Inputs tab 22
Inputs/Outputs page 53
Internet Explorer 57, 71
versions earlier than 8.0 43
internet protocol 58
Introduction 1
IP 6
IP address 8, 11
IP Camera 74
Issue code 14

K

Kernel firmware revision 58

L

LAN 6, 74
LDAP 74, 75
Linked Camera 15, 16, 18, 19, 22, 24
Live video 47
Local Area Network 6
Lock On Close 20

M

Mag Lock Bond Sense 19, 20
Magnetic 73
Magnetic lock 13, 18
Maximum PIN Length 13
Messages
AC Power Failed 68
AC Power Restored 68
Backup Battery Critical 68
Backup Battery Cutoff 68
Backup Battery Low 68
Backup Battery Not Detected 68
Backup Battery Restored 68
Device Communications Failed 69
Device Communications Restored 69
Device Failed 69
Device Restored 69
Fuse Restored 69
Fuse Tripped 69
Input Active 70
Input Disabled 70
Input Inactive 70

Input Tamper Alarm 70
Memory Backup Battery Low 69
No active video connections 71
NTP Sync Failed 11, 70
Objects Have Changed 70
Output Off 70
Output On 70
System Restored 69
System Trouble 69
Tamper Alarm 69
Tamper Restored 69
The Device is rebooting 57
Microsoft .NET 4.0 Framework 7
Monitor
doors 35
inputs 53
outputs 53

N

National Television Standards Committee . 74
Network
router 6
switch 6
Network Configuration tab 11, 12, 58
Network Properties property sheet 12
Normal Grant Access Time 17, 18, 20
Normally Closed 21
Normally Open 21
NTP 58
NTP server 11
NTP Sync Failed 11, 70
NTSC 74

O

Operator 32, 63
Operator Roles page 31, 33
Outputs
auxilliary 53
monitoring 53

P

PAL 75
Passwords
changing 41
Permission Levels 63
Person ID 33
Person Records
unique ID 33
Personal Identification Number (PIN) 13
Persons
credential 37
managing 37
photos 38
removing 38
search for 43
user account 37
Persons page 33, 37, 38, 41, 42, 43, 59
configure user-defined fields 33
Credential pane 26
Persons with disabilities 39
PIN 35, 75
PIN Lock Out Time 13
PIN Retries 13
Pre-Event Playback Duration 24
Protect sensitive data 33
Protected check box 33
PTZ 75
PTZ cameras 23

R

Reader Access report 42
Reader Assignments page 25
Reader Groups page 30
Reader In Only 20
Reader In Reader Out 20
Reader Options 22
credential and PIN 22
credential only 22
Reboot
TruPortal controller 12
Reboot Controller 58
Recorded video 47
Remove
access levels 31
area 25
card formats 14
credential 40
holiday group 27

operator roles ... 33
person ... 38
reader groups ... 30
schedules ... 29
Remove Item dialog box ... 14, 25, 28, 29, 30, 31, 38, 40
Reports
Access History ... 42
Credential ... 42
Reader Access ... 42
Roll Call ... 42
Roster ... 42
Request to Exit (RTE) ... 17, 18, 19, 20
Restore ... 35
Restore Custom Settings ... 57
RF IDeas ... 39
RFID ... 39
RJ-45 ... 6
Roll Call report ... 42
Roster Report ... 25
Roster report ... 42
Router ... 75

S

Save/Reset Settings page ... 57
Schedule Mode ... 35
Credential and PIN ... 35
Credential Only ... 35
door ... 52
First Card In ... 35
Locked ... 35
reader ... 52
Unlocked ... 35
Schedule View tab ... 34
Schedules
time intervals ... 28
Schedules page ... 28, 29, 52
Search
persons ... 43
Security ... 13
Security tab ... 13, 59
Sensitive data
protect ... 33
Serial Number ... 5, 15
Smart Card ... 73
SNMP ... 75
SSL ... 75
start.hta ... 7
Sub-net ... 75
Subnet mask ... 58
Supervised ... 21, 75
System Information tab ... 58
System Settings page ... 11, 12, 13, 33
System Settings tab ... 12

T

Tamper ... 8, 18, 19
Tamper Alarm Enabled ... 22
TCP/IP ... 75
TCP/IP Port ... 75
Time ... 11
Time intervals ... 28
Timed Unlock ... 21
To Area ... 25
TVR10 ... 22, 23
TVR30 ... 22, 23

U

UDP ... 11, 70
UI firmware revision ... 58
Unique Field ... 33
Unique identification number ... 33
Unlock All Doors check box ... 16, 22
Unsupervised ... 21, 75
Upload
photos ... 38
Upload Certificate dialog box ... 12
URL ... 75
USB ... 39
USB credential readers ... 39
Use extended strike/held times checkbox ... 39
User Account Data ... 35
User Account tab ... 41, 42
User accounts
group permissions ... 33
managing ... 37
User-Defined Fields
protected ... 33
User-Defined Fields tab ... 33, 59

V

Video
playback ... 47
player controls ... 48
viewing events ... 47
Video Devices ... 23
Video Layouts page ... 24
Video page ... 47, 48, 71
Video Stream Bandwidth ... 24
View Only ... 32, 63
Voltage ... 68

W

Warning
Objects Have Changed ... 70
Warnings
The Device is rebooting ... 57
Web Browser Configuration and Control ... 23
Wiegand ... 73, 75
Wizard ... 75