



# TruPortal™

MIGRATION TO ONGUARD USER GUIDE

Interlogix<sup>®</sup> TruPortal™ Migration to OnGuard User Guide, product version 1.72.xxx. This guide is item number 460871002C, March 7, 2016.

**Copyright**

© 2016 United Technologies Corporation.

Interlogix is part of UTC Climate, Controls & Security, a unit of United Technologies Corporation. All rights reserved.

**Trademarks and patents**

Interlogix, TruPortal, TruVision, and logos are trademarks of United Technologies. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

**Manufacturer**

Interlogix  
3211 Progress Drive, Lincolnton, NC 28092  
Authorized EU manufacturing representative:  
UTC Climate, Controls & Security B.V.  
Kelvinstraat 7, 6003 DH Weert, Netherlands

**Version**

This document applies to TruPortal version 1.72.xxx or later.

**Certification**



**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**

**12004/108/EC (EMC directive):** Hereby, United Technologies declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.



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

**Contact information**

[www.interlogix.com](http://www.interlogix.com)

**Customer support**

[www.interlogix.com/support](http://www.interlogix.com/support)

**GNU Public Licenses**

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

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

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

**OpenSSL and AstraFlex Components are licensed under a Modified BSD License**

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

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

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.

## **nginx is licensed under the nginx License (Modified BSD License)**

Copyright © 2002-2012 Igor Sysoev

Copyright © 2011,2012 Nginx, Inc.

Redistribution and use in source and binary forms, 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 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 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.

## **CMockery, Google Protocol Buffers (C), and Swagger-js are licensed under the Apache License, Version 2.0 (the "License")**

Copyright © 2006, Google Inc.

Copyright © 2008-2011, Dave Benson.

Copyright © 2015 SmartBear Software

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 2014-09-30, 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.

---

# Table of Contents

---

|                  |  |          |
|------------------|--|----------|
| <b>CHAPTER 1</b> | <b><i>Introduction</i></b> .....                     | <b>1</b> |
|                  | Terminology .....                                    | 1        |
|                  | Prerequisites .....                                  | 2        |
| <b>CHAPTER 2</b> | <b><i>Using the Migration Wizard</i></b> .....       | <b>3</b> |
|                  | Enclosure Labels .....                               | 5        |
| <b>CHAPTER 3</b> | <b><i>Restrictions and Limitations</i></b> .....     | <b>7</b> |
|                  | Access Panels .....                                  | 11       |
|                  | Alarm Panels .....                                   | 14       |
|                  | Areas .....  | 15       |
|                  | Readers and Doors .....                              | 16       |
|                  | Access Levels .....                                  | 20       |
|                  | Anti-passback Functionality and Area Mapping .....   | 20       |
|                  | Supervision Types .....                              | 21       |
|                  | <i>Parameter Mapping for Supervision Types</i> ..... | 21       |
|                  | Unlock All Doors .....                               | 22       |
|                  | PINs Longer than Four Digits .....                   | 22       |
|                  | Card Formats .....                                   | 22       |
|                  | Module Tamper Alarms .....                           | 23       |
|                  | Fallback Modes for IPSDC .....                       | 23       |
|                  | Holiday “Custom” Mode .....                          | 24       |
|                  | <i>Parameter Mapping for Holidays</i> .....          | 24       |
|                  | <i>Parameter Mapping for Schedules</i> .....         | 25       |
|                  | World Time Zone Setting .....                        | 25       |

---

**Table of Contents**

---

Name Lengths ..... 25  
Reader Groups in Access Levels ..... 25

---

This document describes how to use the OnGuard Migration Wizard to migrate person, credential, and access level data from TruPortal 1.6, 1.71, or 1.72 to OnGuard 7.0, 7.1, or 7.2.

After using the OnGuard Migration Wizard, additional OnGuard configuration is required. Reports will be generated containing instructions for this additional configuration.

**IMPORTANT:** This migration is intended only for access control and for the conversion of models TP-SYS-2D or TP-SYS-2D2R to NGP-2220UL, or TP-ADD\_1DIP to DirecDoor DDSDC.

See the Listed control unit’s installation manual as referenced on the product label, for complete details.

---

## Terminology

Some of the terminology in OnGuard differs from TruPortal. The following table lists the TruPortal term and its OnGuard equivalent.

| TruPortal Term  | OnGuard Term   |
|-----------------|--|
| Person          | Cardholder   |
| Credential      | Badge  |
| Operator roles  | Users  |
| Video Layout    | Matrix Layout  |
| Action Trigger  | Input Event  |
| Action          | Output Action  |
| System Settings | Many of the System Settings can be found in System Administration under Access Panels, Alarm Panels, or Readers and Doors. |

| TruPortal Term | OnGuard Term   |
|----------------|--|
| Devices        | A similar display of devices can be found in System Administration under the System Tree. (Select the menu option, <b>View &gt; System Tree.</b> ) |
| Backup/Restore | Archive/Restore  |

---

## Prerequisites

Before you begin, make sure the following requirements are met:

- You must have Administrator rights on the workstation.
- OnGuard must already be installed and functional.
- DataConduIT must be configured and enabled in OnGuard.
- Ensure that there are no devices configured in OnGuard with the same IP addresses as the TruPortal panel or IPSDC devices.
- The TruPortal panel and all IPSDC devices need to be online and accessible from this workstation.
- If the OnGuard Communication Server is running on another workstation, the TruPortal panel and IPSDC devices must also be accessible from that workstation.
- A suitable application for viewing RTF files is needed (for viewing the generated reports). Microsoft Word is recommended.
- If you do not have a recent backup of the OnGuard database, back up the database before proceeding.

---

To migrate data from TruPortal to OnGuard, obtain the TruPortal to OnGuard Migration Wizard and install it. Start the Migration Wizard and perform the following steps.

1. **Introduction** - Read the Introduction and make sure the requirements are met. Before you begin:
  - Make sure you have administrator rights on this workstation.
  - OnGuard should be installed and functional.
  - The DataConduIT interface should be configured and enabled in OnGuard.
  - Ensure that there are no devices configured in OnGuard with the same IP addresses as the TruPortal panel or IPSDC devices.
  - The TruPortal panel and all IPSDC devices need to be online and accessible from this workstation.
  - If the OnGuard Communication Server is running on another workstation, the TruPortal panel and IPSDC devices must also be accessible from that workstation.
  - Back up the OnGuard database.Click [Next].
2. **Login** - Type in the IP address, the user name, and password with which to log in (the administrative account should be used). Click [Next].
3. **Settings** -
  - a. If segmentation is enabled in OnGuard, select the segment to be used.
  - b. Select the badge type.
  - c. If you want to import pictures, select the **Import pictures** check box.Click [Next].
4. **Access Level Mapping** - The TruPortal access levels are listed. Configure the mapping to the OnGuard access level. The default setting creates a new access level in OnGuard with the same name as the access level in TruPortal. Alternatively, the TruPortal access level may be mapped to any access level already existing in OnGuard. If **Do not map** is chosen for any of the access levels, some data may be lost. Click [Next].
5. **Custom Field Mapping** - The TruPortal custom fields are listed. Configure the mapping to the OnGuard cardholder fields. If **Do not map** is chosen for any of the fields, some data may be lost. Click [Next].

6. **Initial OnGuard Settings** - After these mappings, the Initial OnGuard Settings need to be configured in OnGuard. These settings must be configured before proceeding. Scroll down to view Initial OnGuard Settings. An RTF file must be saved for later reference by clicking [Save to disk]. When configuration is completed, click [Next].
7. **Data Import** - Click [Import] to begin the migration of data. This process may take a long time (up to a few hours), depending on the number of persons or credentials to be transmitted and the computer/OnGuard load. When the import is done, you may view the log by clicking [View Report].
8. **IPSDC Conversion** - Under IP Single Door Controller Firmware Conversion, you must verify that devices configured in OnGuard do not have the same addresses as any of the IPSDC IP addresses. Select check boxes of the controllers that need OnGuard compatible firmware. Type in their IP addresses. Click [Convert Panels].  

IPSDC devices are converted in groups of four. This process may take a long time (up to 15 minutes per four devices).
9. **Panel Conversion** - Under TruPortal Panel Firmware Conversion, you must verify that devices configured in OnGuard do not have the same addresses as the TruPortal IP addresses. You may now choose to convert the panel.

**Note:** All TruPortal data will be removed from the panel. This is irreversible.

Click [Convert Panel]. A progress bar is shown indicating the status. When the conversion is done, you may view the log by clicking [View Report].

10. **System Configuration in OnGuard** - After the conversion is done, additional manual configuration is needed in OnGuard. The System Configuration Report provides the details of the configuration. An RTF file must be saved for later reference by clicking [Save to disk]. The saved RTF files may be opened (by applications such as Microsoft Word) and printed.  
Click [Finish].

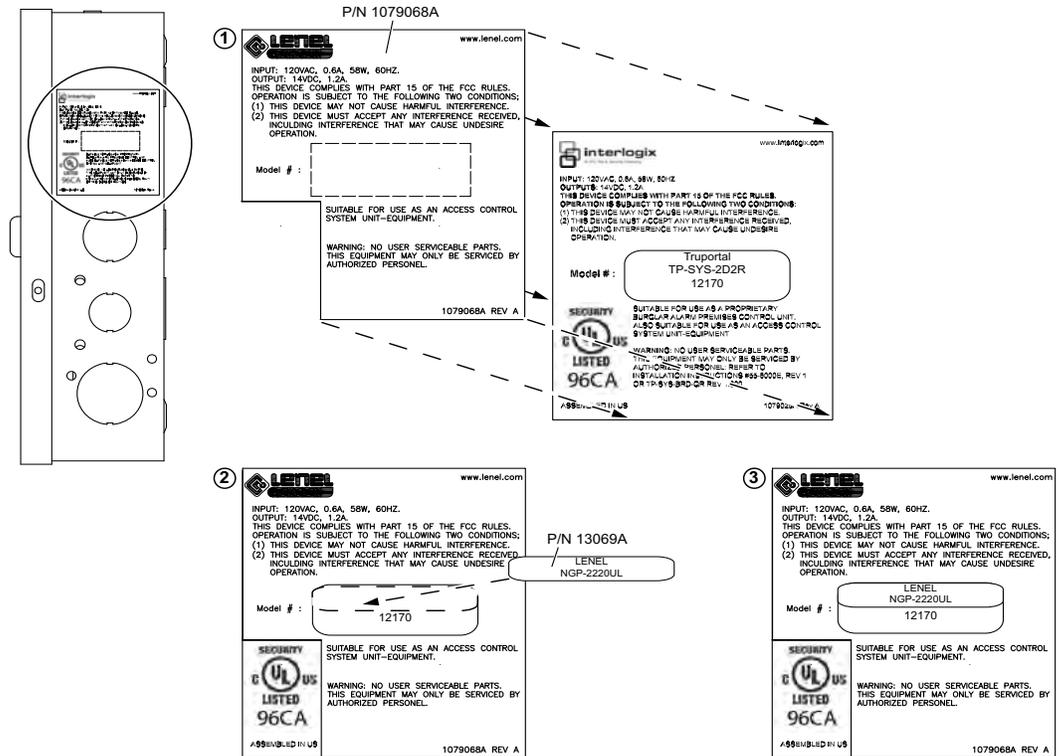
## Enclosure Labels

After migration is completed, new enclosure labels must be applied.

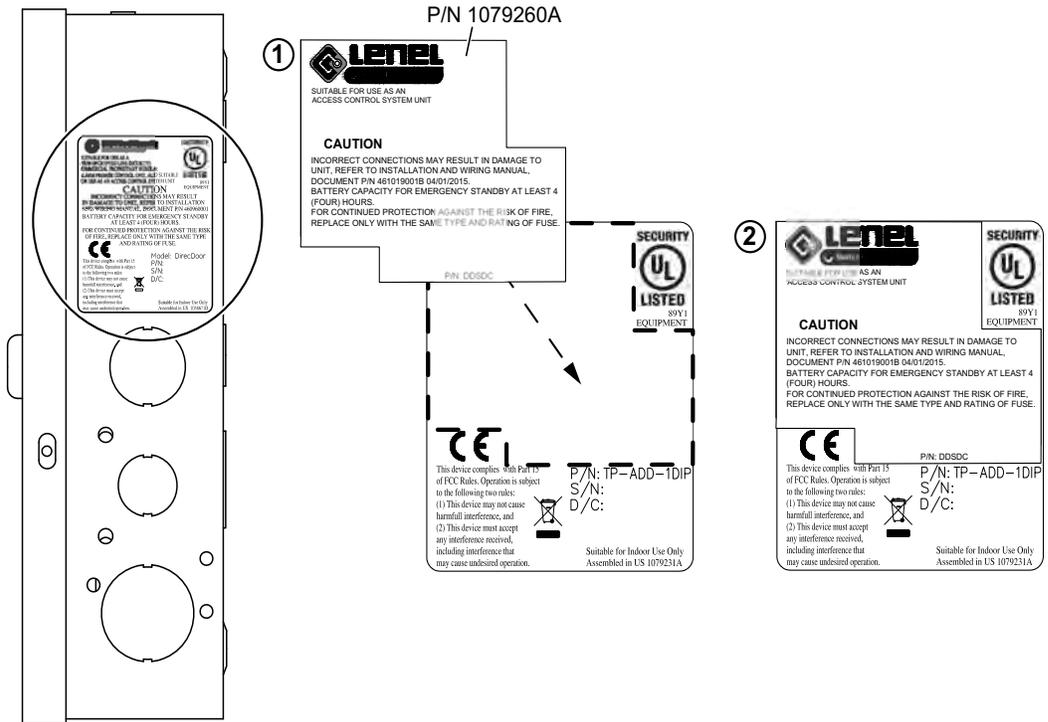
- Using the provided certification labels, replace the label on the outside of the enclosure.

For TruPortal-to-NGP-2220-UL, refer to the following diagram:

**IMPORTANT:** As shown in Steps 2 and 3 below, do not cover up the TruPortal date code (for example, “12170”) with the NGP-2220UL label (P/N 13069A).



For TruPortal IPSDC-to-DirecDoor DDSDC, refer to the following diagram:



2. Using the provided wiring diagram, replace the wiring diagram on the inside cover of the enclosure.

| Label                                       | Converting to NGP-2220UL         | Converting to DirecDoor DDSDC |
|---|----------------------------------|-------------------------------|
| Certification label on outside of enclosure | part numbers 1079068A and 13069A | part number 1079260A          |
| Wiring diagram on inside cover of enclosure | part number 28031C-0C            | part number 1979261A          |

3. Place the Lenel logo on the front of the enclosure.

**IMPORTANT:** Follow the procedures provided by both the configuration reports generated by the migration tool. The restrictions and limitations are listed here only for reference and should not be used directly for configuration of the system.

The restrictions and limitations are listed in the following table with detailed information following.

| TruPortal configuration    | Migration        | Notes   |
|----------------------------|------------------|---|
| Event history              | Not supported    | TruPortal event history can be backed up or exported prior to migration, but cannot be imported into OnGuard.   |
| Devices/Video Devices      | Not supported.   | OnGuard configuration is different. OnGuard video may be used, but some TruVision recorders may or may not be supported, depending on version compatibility.  |
| Devices/System Controller  | Manual migration | Follow the procedures in the generated report. See <a href="#">Access Panels on page 11</a> .   |
| Devices/Door Controller    | Manual migration | Follow the procedures in the generated report. See <a href="#">Readers and Doors on page 16</a> .   |
| Devices/IP Door Controller | Manual migration | Follow the procedures in the generated report. See <a href="#">Readers and Doors on page 16</a> .   |
| Devices/IO Expander        | Manual migration | Follow the procedures in the generated report. See <a href="#">Readers and Doors on page 16</a> .   |
| Doors                      | Manual migration | Follow the procedures in the generated report. Readers in OnGuard must be configured manually. Supervision types may be altered and wiring changes may be required for inputs. See <a href="#">Supervision Types on page 21</a> . |
| Readers                    | Manual migration | Follow the procedures in the generated report. See <a href="#">Readers and Doors on page 16</a> .   |

| TruPortal configuration           | Migration                              | Notes  |
|-----------------------------------|--|--|
| Inputs                            | Manual migration                       | Follow the procedures in the generated report. A Global I/O action may be defined in OnGuard for the “Unlock all doors” option. Note that only the unlock action is implemented. Doors may be reinstated manually.<br>Supervision types may be altered and wiring changes may be required for inputs. See <a href="#">Supervision Types on page 21</a> . |
| Outputs                           | Manual migration                       | Follow the procedures in the generated report. See <a href="#">Alarm Panels on page 14</a> .   |
| Person/First, Middle, Last Name   | Automatic migration, with limitations. | Text may be truncated depending on maximum field lengths in OnGuard. See <a href="#">Name Lengths on page 25</a> .   |
| Person/UDFs                       | Automatic migration, with limitations. | UDFs will map to specific OnGuard credential fields. Text may be truncated depending on maximum field lengths in OnGuard. See <a href="#">Name Lengths on page 25</a> .  |
| Person/User Account               |  | OnGuard concept and/or usage is different. For more information, refer to the System Administration User Guide in the OnGuard system.  |
| Person/Picture                    | Automatic migration                    |  |
| Person/List of Credentials        | Automatic migration                    | OnGuard settings may need to be manually configured to allow more than one card per person. This is covered by the Initial OnGuard Settings report.  |
| Credential/ID                     | Automatic migration, with limitations. | OnGuard does not support card numbers greater than 64 bits without splitting them into card ID and extended ID. These cards will not work on OnGuard.  |
| Credential/Other information      | Automatic migration                    |  |
| Credential/Assigned access levels | Automatic migration                    | In some cases, OnGuard settings may need to be manually configured to allow more than six access levels per card. This is covered by the Initial OnGuard Settings report.  |
| Access Levels                     | Automatic and manual migration         | Access levels will be automatically created in OnGuard or existing OnGuard access levels will be used, but some detailed configuration needs to be set up manually. See <a href="#">Access Levels on page 20</a> .   |
| Schedules                         | Manual migration                       | Follow the procedures in the generated report. See <a href="#">Parameter Mapping for Schedules on page 25</a> .  |

| TruPortal configuration                     | Migration                           | Notes   |
|---|-------------------------------------|---|
| Holidays                                    | Manual migration                    | Some custom holidays are not supported. See <a href="#">Holiday "Custom" Mode on page 24</a> .  |
| Areas                                       | Manual migration, with limitations. | Some physical area may be represented by multiple logical areas in OnGuard. See <a href="#">Areas on page 15</a> .  |
| APB Settings                                | Manual migration, with limitations. | Global APB mode may need to be used in the OnGuard system, if the TruPortal panel had IPSCD devices attached and APB was used in the system. Some configurations may not convert to OnGuard (the APB feature may be disabled for some readers). See <a href="#">Anti-passback Functionality and Area Mapping on page 20</a> . |
| Reader Groups                               | Not supported                       | Reader group assignments to Access Levels in TruPortal are not lost, but "flattened" to per-reader assignments. See <a href="#">Reader Groups in Access Levels on page 25</a> .   |
| Action Triggers                             |                                     | Can use OnGuard Local I/O or Global I/O, but the OnGuard concept and/or usage is different. For more information, refer to the System Administration User Guide in the OnGuard system.  |
| System Settings/Date and Time               | Manual migration, with limitations. | There is no one-to-one relationship between the TruPortal and OnGuard settings. See <a href="#">World Time Zone Setting on page 25</a> .  |
| System Settings/Security/Max PIN Length     | Manual migration                    | To be manually configured to global OnGuard option, and to per-controller options. See <a href="#">PINs Longer than Four Digits on page 22</a> .  |
| System Settings/Security/Max PIN Attempts   | Manual migration                    | To be manually configured in OnGuard as an access controller option.  |
| System Settings/Security/PIN Lockout Time   | Manual migration                    | To be manually configured in OnGuard as an access controller option.  |
| System Settings/Security/Door Fallback Mode | Manual migration                    | To be manually configured in OnGuard as an access controller option.  |

| TruPortal configuration                                | Migration                              | Notes  |
|--|--|--|
| System Settings/<br>Security/Input EOL<br>Termination  | Manual migration, with<br>limitations. | OnGuard does not allow for configuration of single resistor line supervisions for the NGP panel. Some of these can be replaced with non-supervised modes with limited functionality (no tampers reported). Some others cannot be replaced with any configuration in OnGuard — these cases require a physical change of input wiring. Both cases will appear in the configuration report if applicable. |
| System Settings/<br>Security/IPSDC Fallback<br>Mode    | Manual migration, with<br>limitations. | The DirecDoor device does not support cache-based fallback mode. See <a href="#">Fallback Modes for IPSDC on page 23</a> .   |
| System Settings/<br>Security/IPSDC<br>Encryption       | Manual migration                       | To be manually configured in OnGuard as an encryption option for all DirecDoor panels.   |
| System Settings/User<br>Defined Field<br>configuration |  | The configuration itself is lost (order, required, secure fields), but the relevant person data may be automatically transmitted to OnGuard, according to the mappings defined in Migration wizard. The OnGuard concept and/or usage is different. For more information, refer to the System Administration User Guide in the OnGuard system.  |
| System Settings/Card<br>Formats                        | Manual migration, with<br>limitations. | Some custom settings on card parity checking are not available in OnGuard. Card format will remain functional in this case, but parity checking will be dropped. OnGuard does not support card numbers greater than 64bits. Instances of these card formats will appear in the configuration report. See <a href="#">Card Formats on page 22</a> .   |
| System Settings/<br>Operator Roles                     | Not supported                          |  |
| System Settings/DB and<br>Event Backup Schedules       | Not supported                          |  |
| System Settings/Network<br>Configuration               | Not supported                          |  |
| System Settings/<br>Certificate                        | Not supported                          |  |
| System Settings/Network<br>Shares                      | Not supported                          |  |
| System Settings/Email                                  | Not supported                          |  |

## Access Panels

Access panel objects may be created from the main TruPortal panel, which converts to an NGP panel (firmware v1.4.2 or later), or on IPSDC devices (which converts to DirecDoor panels). These settings are found in the Administration/Access Panels menu.

### Parameters for Main TruPortal Panel

| OnGuard parameter              | TruPortal parameter  | Notes  |
|--------------------------------|--|--|
| <b>Options tab</b>             |  |  |
| Name                           | System Controller<br>Device name   | Maximum length - 32 characters (may be truncated)  |
| Online                         | –  | Always selected.   |
| Model                          | NGP-2220   |  |
| World region                   | –  | Set to North America.  |
| Serial number                  | –  | Value detected automatically from TP panel   |
| Panel code                     | –  | Set to 0   |
| Door fallback mode             | Door fallback mode<br>(System settings/<br>Security)                     | No Access (TruPortal) — None (OnGuard)<br>Site code access (TruPortal) — Valid facility<br>code (OnGuard)<br>All access (TruPortal) — Valid Card Format<br>(OnGuard) |
| Enable wall tamper             | –  | Always selected.   |
| <b>Primary connection tab</b>  |  |  |
| Connection type                | –  | Set to IPv4.   |
| IP Address                     | –  | Same as IP used to communicate with TP<br>panel  |
| Port                           | –  | Set to 3001.   |
| <b>Encryption tab</b>          |  |  |
| Use an encrypted<br>connection | Enable HTTPS<br>Connection (System<br>settings/Network<br>configuration) |  |
| <b>Invalid access tab</b>      |  |  |
| Number of invalid PINs         | Max PIN attempts<br>(System settings/<br>Security)                       |  |

**Parameters for Main TruPortal Panel (Continued)**

| OnGuard parameter                                       | TruPortal parameter                          | Notes  |
|---|--|--|
| Individual lockout duration                             | PIN lockout time (System settings/ Security) |  |
| <b>Log on/PIN tab</b>                                   |  |  |
| PIN type  | PIN max length (System settings/ Security)   |  |
| <b>Card formats tab</b>                                 |  |  |
| List of all card formats entered in Card format section |  |  |
| <b>Location tab</b>                                     |  |  |
| Workstation   | –  | Name of PC where communication server is working (to be found by the user).  |
| Timezone  | –  | World timezone to be used (to be determined by user). The name of original timezone from TP system is displayed in the configuration report. |
| Daylight savings  | –  | Daylight Saving Time to be used (determined by user)   |

**Parameters for IPSDC Devices**

| OnGuard parameter  | TruPortal parameter                       | Notes   |
|--------------------|---|---|
| <b>Options tab</b> |   |   |
| Name               | IP 1 Door 2 Reader Controller Device name | Maximum length - 32 characters (may be truncated) |
| Online             | –   | Always selected.                                  |
| Model              | DirecDoor                                 |   |
| World region       | –   | Set to North America.                             |
| Serial number      | Serial number                             | Value detected automatically from TP panel        |
| Panel code         | –   | Set to 0.   |

## Parameters for IPSDC Devices (Continued)

| OnGuard parameter                                       | TruPortal parameter                                       | Notes  |
|---|---|--|
| Door fallback mode                                      | IPSDCU fallback mode (System settings/ Security)          | No Access (TruPortal) — None (OnGuard)<br>Site code access (TruPortal) — Valid facility code (OnGuard)<br>All access (TruPortal) — Valid Card Format (OnGuard)<br>Use Local Cache Table (TruPortal) — Valid Card Format (OnGuard)<br><b>Note:</b> Cached mode is not supported by OnGuard, so Valid Card Format mode is recommended. A warning message is displayed. |
| Enable wall tamper                                      | Tamper Alarm Enabled                                      |  |
| <b>Primary connection tab</b>                           |   |  |
| Connection type   | –   | Set to IPv4.   |
| IP Address  | –   | User needs to enter IPSDC device IP address here, as the TruPortal panel is not aware of it. A message is displayed.   |
| Port  | –   | Set to 3001.   |
| <b>Encryption tab</b>                                   |   |  |
| Use an encrypted connection                             | Encrypt IPSDCU Communications (System settings/ Security) |  |
| <b>Invalid access tab</b>                               |   |  |
| Number of invalid PINs                                  | Max PIN attempts (System settings/ Security)              |  |
| Individual lockout duration                             | PIN lockout time (System settings/ Security)              |  |
| <b>Log on/PIN tab</b>                                   |   |  |
| PIN type  | PIN max length (System settings/ Security)                | This tab is not shown in OnGuard 7.0. A warning message is displayed if the PIN length is a value other than 4. Longer PINs may not work in DirecDoor controllers.   |
| <b>Card formats tab</b>                                 |   |  |
| List of all card formats entered in Card format section |   |  |

### Parameters for IPSDC Devices (Continued)

| OnGuard parameter   | TruPortal parameter | Notes  |
|---------------------|---------------------|--|
| <b>Location tab</b> |                     |  |
| Workstation         | –                   | Name of PC where communication server is working (to be found by the user).                                      |
| Timezone            | –                   | World timezone to be used (to be determined by user). The name of original timezone from TP system is displayed. |
| Daylight savings    | –                   | Daylight Saving Time to be used (determined by user)   |

### Alarm Panels

Alarm panel objects may be created from the main TruPortal panel baseboard or IO expander devices.

With the main panel baseboard, the board itself does not require any configuration and is created automatically by OnGuard, along with the NGP panel (Access Panel object).

The name of the Alarm Panel for the baseboard is “[Access Panel name] Baseboard I/O,” where [Access Panel name] is the name of NGP panel, with a maximum of 20 characters (may be truncated).

These settings are found in the Access Control/Alarm Panels menu.

The IO expander device must be created manually and configured as follows:

#### Parameter Mapping for Alarm Panels

| OnGuard parameter       | TruPortal parameter                | Notes                                    |
|-------------------------|------------------------------------|--|
| <b>Alarm Panels tab</b> |                                    |  |
| Name                    | IO Expander Controller Device name |  |
| Panel                   | –                                  | Set to the name of main TruPortal panel. |
| Serial Number           | Serial Number                      |  |
| Model                   | –                                  | Set to NGP-1100.                         |
| Number of outputs       | –                                  | 8  |

For both the baseboard and IO expander, inputs and outputs need to be created and configured.

**IMPORTANT:** Only enabled I/Os are included in report.

| OnGuard parameter       | TruPortal parameter | Notes |
|-------------------------|---------------------|-------|
| <b>Alarm Inputs tab</b> |                     |       |

| OnGuard parameter        | TruPortal parameter | Notes   |
|--------------------------|---------------------|---|
| Name                     | Input name          |   |
| Alarm Panel              | –                   | Set to the name of IO Expander Controller.  |
| Input Number             | –                   | Consecutive numbers 1-16, as listed in TruPortal  |
| Supervision              | –                   | Resolved OnGuard supervision. Limitations apply. See <a href="#">Supervision Types on page 21</a> . |
| Point Type               |                     | Standard  |
| <b>Alarm Outputs tab</b> |                     |   |
| Name                     | Output name         |   |
| Alarm Panel              | –                   | Set to the name of IO Expander Controller.  |
| Input Number             | –                   | Consecutive numbers 1-16, as listed in TruPortal  |

## Areas

The “Outside” area is never included in the report, as it is defined in OnGuard by default.

The “Default” area in TruPortal is mapped to the default area for the NGP panel, which is created automatically in OnGuard with the name, “Default Area [NGP panel name].” The Configuration Report recommends renaming this area to the name specified in TruPortal.

If the TruPortal system does not have IPSDCU devices configured, all other TruPortal areas are mapped directly to OnGuard areas belonging to the NGP panel (to be created manually in OnGuard).

If the TruPortal system has IPSDCU devices, areas may need to be attached either to the main NGP or DirecDoor panels. The migration wizard tries to analyze the area and reader relationships, resolving areas so that at least one side of a door is an area belonging to the panel which controls the door. The “Outside” area is always considered as not assigned to any panels.

If this is possible, all TruPortal areas are mapped to relevant OnGuard areas belonging to various panels (NGP/DirecDoors). This also causes Global APB mode to be enabled in OnGuard.

If this is not possible, then areas may be multiplied — a single physical area in TruPortal is represented by multiple areas in OnGuard, belonging to multiple panels. Names for these areas are created by concatenating of original TruPortal area name and the name of the relevant access panel. This configuration prevents use of any form of APB on the readers moving to or from such areas.

### Parameter Mapping for Areas

| OnGuard parameter      | TruPortal parameter | Notes  |
|------------------------|---------------------|--|
| <b>Add area window</b> |                     |  |
| Local area             | –                   | Always selected (disabled unless in Global APB mode) |

**Parameter Mapping for Areas (Continued)**

| OnGuard parameter                         | TruPortal parameter         | Notes   |
|---|-----------------------------|---|
| Panel                                     | NGP or DirecDoor panel name |   |
| <b>Area parameters</b>                    |                             |   |
| Name                                      | Area Name                   | May be converted/concatenated. Maximum length - 32 characters (may be truncated). |
| <b>General tab, Anti-passback section</b> |                             |   |
| Auto reset                                | Anti-Passback Auto Reset    |   |

**Readers and Doors**

Readers and doors have different options available for NGP and DirecDoor panels.

**NGP Readers and Doors**

| OnGuard parameter       | TruPortal parameter     | Notes  |
|-------------------------|-------------------------|--|
| <b>General tab</b>      |                         |  |
| Name                    | "Door" Device name      |  |
| Panel                   | NGP panel name          |  |
| Type                    | –                       | <b>Onboard Door 1/2 (Wiegand/Prox)</b> - for baseboard doors 1 and 2, respectively<br><b>Dual Interface Door 1/2 (Wiegand/Prox)</b> - for door controller doors 1 and 2, respectively.<br>Second door is defined if the <b>Number of Doors</b> in TruPortal is set to <b>Control Two Doors</b> |
| Serial number           | Serial Number           | Parameter of door controller   |
| Strike                  | Door Strike Mode        | Lock on Close (TruPortal) — Cut Off on Close (OnGuard)<br>Timed Unlock (TruPortal — Cut Off on Duration (OnGuard)  |
| <b>Settings tab</b>     |                         |  |
| Enable request to exit  | Request To Exit Enabled |  |
| Request to exit circuit | Request To Exit         | Resolved OnGuard supervision. Limitations apply. See <a href="#">Supervision Types on page 21</a> .  |

## NGP Readers and Doors (Continued)

| OnGuard parameter   | TruPortal parameter                            | Notes  |
|---|--|--|
| Main panel controls processing for request to exit instead of door controller | Do Not Activate Strike On RTE                  | This TruPortal parameter also affects the next OnGuard parameter   |
| Do not activate strike on request to exit                                     | Do Not Activate Strike On RTE                  | Selected only if <b>Do not Activate Strike On RTE</b> in TruPortal is selected.  |
| <b>Door tab</b>   |  |  |
| Reader configuration  | Access Mode                                    | Entry Reader Only (TruPortal) — In Reader Only (OnGuard)<br>Entry and Exit Readers (TruPortal — In and Out Readers (OnGuard)   |
| Schedule/Mode   | Door/Schedule                                  | If the parameter is set to <b>No schedule</b> in TruPortal (found under Monitoring > Schedule View), it will be set to <b>Always</b> in OnGuard. Otherwise, the relevant schedule name is used in OnGuard.   |
| During schedule/ Mode   | Door/Schedule Mode                             | If the Door/Schedule is set to <b>No schedule</b> in TruPortal (found under Monitoring > Schedule View), it will be set to <b>Credential Required</b> in OnGuard.<br>Otherwise, the following settings apply:<br>Unlocked (TruPortal) — Unlocked (OnGuard)<br>First Card In (TruPortal) — Pending First User (OnGuard)<br>Locked (TruPortal) — Credential Required (OnGuard) |
| Outside Schedule/ Mode  | –  | Always <b>Credential Required</b> .  |
| Reader tamper circuit   | Tamper (check box) and Tamper (drop-down list) | If the <b>Tamper</b> check box is not selected, the OnGuard parameter is <b>Disabled</b> .<br>Otherwise, the OnGuard setting is the supervision type, based on the TruPortal Tamper setting. Limitations apply. See <a href="#">Supervision Types on page 21</a> .   |
| Door circuit  | Door contact                                   | The OnGuard parameter is the name of the OnGuard supervision type. Limitations apply. See <a href="#">Supervision Types on page 21</a> .   |
| <b>In Reader tab</b>  |  |  |
| Area Entering   | To Area  | (Found in TruPortal under Access Management > Areas > Reader Assignments)<br>Area names may be changed, according to the rules specified in the Areas section.   |
| Area Leaving  | From Area                                      |  |

## NGP Readers and Doors (Continued)

| OnGuard parameter  | TruPortal parameter                   | Notes   |
|--|---------------------------------------|---|
| Schedule/Reader Mode   | Reader/Schedule                       | If the parameter is set to <b>No schedule</b> in TruPortal (found under Monitoring > Schedule View), it will be set to <b>Always</b> in OnGuard. Otherwise, the relevant schedule name is used in OnGuard.  |
| During schedule/Reader Mode  | Reader/Schedule Mode or Access Method | If the Reader/Schedule is set to <b>No schedule</b> in TruPortal, then the parameter for Access Method in TruPortal (found under System Administration > Devices > ... > Reader) will be used.<br>Otherwise, the setting for Reader/Schedule in TruPortal (found under Monitoring > Schedule View) will apply. Value mapping:<br>Credential Only (TruPortal) — Card Only (OnGuard)<br>Credential and PIN (TruPortal) — Card and PIN (OnGuard)<br>Credential or PIN (TruPortal) — PIN or Card (OnGuard)<br>PIN Only (TruPortal) — PIN Only (OnGuard) |
| Outside schedule/Reader Mode   | Access Method                         | The parameter for Access Method in TruPortal (found under System Administration > Devices > ... > Reader) will be used.<br>Value mapping:<br>Credential Only (TruPortal) — Card Only (OnGuard)<br>Credential and PIN (TruPortal) — Card and PIN (OnGuard)<br>Credential or PIN (TruPortal) — PIN or Card (OnGuard)<br>PIN Only (TruPortal) — PIN Only (OnGuard)   |
| Anti-passback mode   | Anti-Passback                         | The parameter for Anti-Passback in TruPortal (found under Access Management > Areas > Reader Assignments) will be used.<br>Limitations apply. See <a href="#">Areas on page 15</a> .  |
| Perform area leaving check   | –                                     | Selected only if Anti-Passback mode for this reader is enabled and Global APB is enabled.   |
| <p><b>Out Reader tab</b><br/>Settings are the same as those of the In Reader tab; however, Area entering/Area leaving fields are disabled. The Out Reader is enabled only if the reader configuration is set to <b>In and Out Readers</b> on the Door tab.</p> |                                       |   |
| <p><b>Timing and Alarms tab</b></p>  |                                       |   |
| Normal timing/Strike time  | Normal Grant Access Time              |   |

**NGP Readers and Doors (Continued)**

| <b>OnGuard parameter</b>       | <b>TruPortal parameter</b>   | <b>Notes</b>   |
|--------------------------------|------------------------------|--|
| Normal timing/Held open time   | Door Held Time               |  |
| Extended timing/Strike time    | Extended Grant Access Time   |  |
| Extended timing/Held open time | Extended Door Held Time      |  |
| Alarms/Forced open             | Alarm Enabled/Door Held Open |  |
| Alarms/Held open               | Alarm Enabled/Door Held Open |  |
| <b>Auxiliary Inputs tab</b>    |                              |  |
| Input 1/Mode                   | Aux Input                    | None (TruPortal) — None (OnGuard)<br>Mag Lock Bond Sense (TruPortal) —<br>Magnetic lock bond sense (OnGuard)<br>Extended RTE (TruPortal) — Extended<br>request to exit (OnGuard) |
| <b>Auxiliary Outputs tab</b>   |                              |  |
| Output 1/Mode                  | Aux Relay                    | None (TruPortal) — None (OnGuard)<br>Door Held/Forced (TruPortal) — Activate on<br>door held or forced open (OnGuard)<br>Door Opener (TruPortal) — Door opener<br>(OnGuard)      |
| Output 1/Time                  | Aux Relay On Time            |  |

**DirecDoor Readers and Doors**

| <b>OnGuard parameter</b> | <b>TruPortal parameter</b> | <b>Notes</b>  |
|--------------------------|----------------------------|---|
| <b>General tab</b>       |                            |   |
| Name                     | "Door" Device name         |   |
| Panel                    | DirecDoor panel name       |   |
| Type                     | –                          | Always Wiegand/Prox   |
| Reader number            | –                          | Always 1  |
| Strike                   | Door Strike Mode           | Lock on Close (TruPortal) — Cut Off on Close<br>(OnGuard)<br>Timed Unlock (TruPortal — Cut Off on<br>Duration (OnGuard) |

## DirecDoor Readers and Doors (Continued)

| OnGuard parameter   | TruPortal parameter           | Notes   |
|---|-------------------------------|---|
| <b>Settings tab</b>   |                               |   |
| Enable request to exit  | Request To Exit Enabled       |   |
| Request to exit circuit   | Request To Exit               | Resolved OnGuard supervision. Limitations apply. See <a href="#">Supervision Types on page 21</a> . |
| Do not activate strike on request to exit   | Do Not Activate Strike On RTE |   |
| Door tab - same as NGP. See <a href="#">Door tab on page 17</a> .                           |                               |   |
| In Reader tab - same as NGP. See <a href="#">In Reader tab on page 17</a> .                 |                               |   |
| Out Reader tab - same as NGP. See <a href="#">Out Reader tab on page 18</a> .               |                               |   |
| Timing and Alarms tab - same as NGP. See <a href="#">Timing and Alarms tab on page 18</a> . |                               |   |
| Auxiliary Inputs tab - same as NGP. See <a href="#">Auxiliary Inputs tab on page 19</a> .   |                               |   |
| Auxiliary Outputs tab - same as NGP. See <a href="#">Auxiliary Outputs tab on page 19</a> . |                               |   |

## Access Levels

Access levels are automatically created. The mapping of access levels from TruPortal to OnGuard can be defined in the migration wizard. Access levels may be either:

- Created in OnGuard with the same name as in TruPortal
- Replaced (mapped into) any of existing OnGuard access levels
- Not mapped at all

For every access level in OnGuard, the report shows the list of readers to be linked with a particular single schedule, and the name of single schedule itself. This is repeated for each schedule used per TruPortal access level.

Additionally, for every OnGuard access level, there is an additional parameter, Name on LCD, which is defined as follows: “ACC x” where x is an auto-incremented, consecutive value. This parameter is important if LCD keypads are to be used on migrated systems.

## Anti-passback Functionality and Area Mapping

Anti-passback (APB) settings and areas require some manual configuration.

APB configuration in TruPortal may be converted to OnGuard only if TruPortal does not have IPSCD devices configured. In this case, all TruPortal areas are converted or mapped to OnGuard areas.

However, if IPSCDU devices are configured in TruPortal, areas defined in OnGuard must be assigned to NGP or DirecDoor panels. The Migration tool tries to resolve area assignments so that at least one side of the door is an area belonging to the panel which controls that door.

The following scenarios may occur:

- Area resolution is possible. Every TruPortal area maps to a single OnGuard area which is assigned either to NGP or DirecDoor panel. If this is the case, the configuration report suggests switching to Global APB mode in the OnGuard system. APB can be used on all readers.
- Area resolution is not possible. Some TruPortal areas may be multiplied (the same physical area is represented by multiple logical areas in OnGuard, assigned to various panels). If this is the case, APB cannot be used on the readers adjacent to these areas. All other readers can still work in standard local APB mode (controlled by particular panels).

## Supervision Types

OnGuard does not support end-of-line resistor configurations with one resistor only.

- **4k7, Single Parallel** or **1k, Single Series** TruPortal modes may be replaced with non-supervised configuration in the OnGuard system. Non-supervised configuration would report “active” and “non-active” input states properly, but “tamper” states would no longer be reported.
- **4k7, Single Series** or **1k, Single Parallel** modes cannot be replaced with any other OnGuard modes. Change of physical input wiring is required in these cases.

Both instances will be reflected in the configuration report.

## Parameter Mapping for Supervision Types

This section depends on the Input EOL configuration in TruPortal (found under System Settings > Security > Input EOL configuration).

- If the parameter is **1k, Dual**, the section does not exist, as supervision types for inputs are automatically and quietly mapped to the OnGuard standard supervision types (non-supervised NO/NC and standard supervision NO/NC).
- If the parameter is **4k7, Dual**, the section shows the hard-coded values to be entered in OnGuard, as follows:

| OnGuard parameter | Value  | Notes                           |
|-------------------|--|---------------------------------|
| Table name        | Dual 4k7, Normally Open<br>Dual 4k7, Normally Closed | Two separate EOL configurations |
| Table type        | Basic Custom   |                                 |
| Normal low range  | 4175 4975  |                                 |
| Normal high range | 4975 9700  |                                 |
| Normally open     | Selected<br>Deselected                               | Two separate EOL configurations |
| Table name        | Dual 4k7, Normally Open                              |                                 |

- If the parameter is **4k7, Single Parallel** or **1k, Single Series**, these modes are not supported by OnGuard but can be replaced with non-supervised modes. A warning is displayed along with the information of original ranges (0...4175...4975 or 725...1275...infinity).

All further references to supervised modes in inputs are converted to non-supervised modes and highlighted in red.

- If the parameter is **4k7, Single Series** or **1k, Single Parallel**, these modes are not supported by OnGuard and cannot be replaced with any OnGuard modes. An error is displayed along with the information of original ranges (4175...4975...infinity or 0...725...1275).

All further references to supervised modes in inputs are marked as “change of wiring required” and highlighted in red.

---

## Unlock All Doors

The **Unlock all doors** setting for inputs must be replaced with Global I/O linkage in the OnGuard system. The functionality is slightly different, but it allows for unlocking all the doors on input activation (the doors will not be reinstated on restoration of the triggering inputs).

---

## PINs Longer than Four Digits

In OnGuard 7.0, the PIN code length for DirecDoor controllers is four digits. The use of six or nine digit PINs is not possible on DirecDoor controllers.

---

## Card Formats

TruPortal allows for full configuration of parity checking (bit range to be checked and resulting location value, for both even and odd checks), while OnGuard supports even or odd field length configuration only. If the card format defined in TruPortal is not compliant with OnGuard, card parity checking will be dropped, but the card format will still work.

The maximum card number field length in TruPortal is 128 bits. OnGuard supports card field lengths up to 64 bits, and real card numbers up to 18 decimal digits. Any card formats with card number fields larger than 64 bits will be converted to exactly 64 bits. This would result in proper operation for the cards of the original format, but with real card numbers fitting into 18 decimal digits. The cards with longer numbers will not work properly.

### Parameter Mapping for Card Formats

| OnGuard parameter            | TruPortal parameter        | Notes                 |
|------------------------------|----------------------------|-----------------------|
| Name                         | Format Name                |                       |
| –                            | Format Type                | Ignored               |
| Card Format Type             | –                          | Hard-coded to Wiegand |
| Facility Code                | Facility Code              |                       |
| Total Number of Bits On Card | Total Bit Length           |                       |
| Card Number - Starting Bit   | Card Number - Starting Bit |                       |

**Parameter Mapping for Card Formats (Continued)**

| OnGuard parameter              | TruPortal parameter          | Notes  |
|--------------------------------|------------------------------|--|
| Card Number - Number of Bits   | Card Number - Bit Length     | If the TruPortal card number length is greater than 64, the OnGuard card number length is limited to 64. A relevant warning is displayed in this case.   |
| Facility Code - Starting Bit   | Facility Code - Starting Bit |  |
| Facility Code - Number of Bits | Facility Code - Bit Length   |  |
| Issue Code - Starting Bit      | Issue Code - Starting Bit    |  |
| Issue Code - Number of Bits    | Issue Code - Bit Length      |  |
| Number of Even Parity Bits     | Even Length + 1              |  |
| Number of Odd Parity Bits      | Odd Length + 1               | <p>OnGuard supports only the following setup of parity fields/ranges:</p> <ul style="list-style-type: none"> <li>• even parity bit at 0</li> <li>• even parity check range, starting at 1</li> <li>• odd parity check range (may overlap with previous field but must end right before the last bit in card)</li> <li>• odd parity bit at the last bit in the card</li> </ul> <p>If the parity check specification does not meet OG standard, the relevant message is displayed, and parity checking is dropped (both OG parameters: 0).</p> |

**Module Tamper Alarms**

Tamper alarm reporting for modules (door controllers, IO expanders, main panel) is available for the main NGP panel only — no relevant configuration parameters in OnGuard.

**Note:** Door and input tampers are not affected by this limitation.

**Fallback Modes for IPSDC**

The DirecDoor device does not support cache-based fallback mode. **Valid card format** is used instead.

## Holiday “Custom” Mode

Holiday definitions that are based on their occurrence in the calendar year (for example, “second Wednesday of January”) are not supported in OnGuard. This type of holiday definition will be represented in the report as multiple holidays, defined for exact dates in five consecutive occurrences (years) with the range of recurrence starting at the date when the report was generated.

## Parameter Mapping for Holidays

| OnGuard parameter | TruPortal parameter        | Notes  |
|-------------------|----------------------------|--|
| Name              | Holiday Group Name<br>[+i] | One holiday in TruPortal may consist of many particular holiday definitions. Each definition needs to be converted to separate OnGuard holidays, so the names for these holidays are derived from TruPortal name as follows: <ul style="list-style-type: none"> <li>• If there is only one definition, the name is just copied to OnGuard.</li> <li>• If there are many definitions, OnGuard names for them are the TruPortal name with a consecutive numbers appended.</li> </ul> |
| Type [1] - [8]    | –                          | One of the types will be marked. This corresponds to a separate TruPortal holiday. The order is not specified, but the types are taken starting at 1.  |
| Start date        | Date                       | This is the same date in TruPortal for “single” and “repeat yearly” holiday types. For custom holiday types, this is the date computed for one particular year (not present in TruPortal).   |
| Duration (days)   | Duration                   |  |
| Repeat yearly     | –                          | Configured if “repeat yearly” is selected in TruPortal.  |

**Note:** The custom holiday type is not supported in OnGuard, so it is specified as exact dates for five consecutive years, starting “today.” A warning message is displayed for each case.

### Parameter Mapping for Schedules

| OnGuard parameter | TruPortal parameter | Notes   |
|-------------------|---------------------|---|
| Name              | Schedule Name       |   |
| Start             |                     | The start and end time for a particular time range in this schedule. These parameters are not named in TruPortal.   |
| End               |                     |   |
| Sun...Sat         | Sun...Sat           | Days marked for a particular time range.  |
| H1...H8           |                     | Holidays marked for this schedule. These would be the same for all ranges in this schedule. For a linkage between particular Hx check boxes and TruPortal holiday names, see <a href="#">Parameter Mapping for Holidays</a> on page 24. |

---

### World Time Zone Setting

There is no one-to-one mapping between TruPortal and OnGuard settings. You must select the most appropriate time zone available in the OnGuard system.

---

### Name Lengths

Some object names (panels, areas) may get truncated on migration, as relevant OnGuard name fields are shorter.

---

### Reader Groups in Access Levels

This TruPortal feature will be simulated by per-reader assignments, with the same functionality.



---

# *Index*

---

|                                     |           |
|-------------------------------------|-----------|
| <b>A</b>                            |           |
| Access level mapping .....          | 3         |
| Access levels .....                 | 8, 20     |
| Access panels .....                 | 11        |
| Action triggers .....               | 9         |
| Alarm panels .....                  | 14        |
| APB .....                           | 20        |
| APB settings .....                  | 9         |
| Area mapping .....                  | 20        |
| Areas .....                         | 9, 15     |
| <b>C</b>                            |           |
| Card formats .....                  | 10, 22    |
| Certificate .....                   | 10        |
| Custom field mapping .....          | 3         |
| <b>D</b>                            |           |
| DB and event backup schedules ..... | 10        |
| DirecDoor readers and doors .....   | 19        |
| Door controller .....               | 7         |
| Door fallback mode .....            | 9         |
| Doors .....                         | 7, 16, 19 |
| <b>E</b>                            |           |
| Email .....                         | 10        |
| Event history .....                 | 7         |
| <b>F</b>                            |           |
| Fallback modes for IPSDC .....      | 23        |
| <b>H</b>                            |           |
| Holidays .....                      | 9, 24     |
| <b>I</b>                            |           |
| Input eol termination .....         | 10        |
| Inputs .....                        | 8         |
| IO expander .....                   | 7         |
| IPSDC .....                         | 23        |
| IPSDC devices .....                 | 12        |
| IPSDC encryption .....              | 10        |
| IPSDC fallback mode .....           | 10        |
| <b>L</b>                            |           |
| Labels .....                        | 5         |
| Limitations .....                   | 7         |
| <b>M</b>                            |           |
| Main truportal panel .....          | 11        |
| Mapping                             |           |
| access levels .....                 | 3         |
| custom fields .....                 | 3         |
| Max pin attempts .....              | 9         |
| Max pin length .....                | 9         |
| Migration .....                     | 3         |
| Module tamper alarms .....          | 23        |
| <b>N</b>                            |           |
| Name lengths .....                  | 25        |
| Network configuration .....         | 10        |
| Network shares .....                | 10        |
| NGP readers and doors .....         | 16        |
| <b>O</b>                            |           |
| OnGuard settings .....              | 4         |
| Operator roles .....                | 10        |
| Outputs .....                       | 8         |

**P**

Person ..... 8  
PIN lockout time ..... 9  
PINs ..... 22  
Prerequisites ..... 2

**R**

Reader groups ..... 9  
Reader groups in access levels ..... 25  
Readers ..... 7, 16, 19  
Restrictions ..... 7

**S**

Schedules ..... 8, 25  
Stickers ..... 5  
Supervision types ..... 21  
System controller ..... 7

**T**

Tamper ..... 23  
Terminology ..... 1  
TruPortal panel ..... 11

**U**

Unlock all doors ..... 22

**V**

Video devices ..... 7

**W**

Wiring diagram ..... 5  
World time zone setting ..... 25