UTC Fire & Security Americas Corporation, Inc.
1212 Pittsford-Victor Road
Pittsford, New York 14534
Tel 866.788.5095 Fax 585.248.9185
www.lenel.com

OnGuard® 7.2 Release Notes

Contents

1. Introduction

This document provides an overview about the release and a list of the new features and known issues. For a list of resolved issues, refer to the Resolved Issues document. For a list of limitations, refer to the Limitations document.

The Release Notes, Limitations, Resolved Issues, Installation, and User documents are available in portable document format (PDF) on the OnGuard disc in the **..\Program Files\OnGuard\doc\en-US** folder. The documents can be searched using the Search All User Guides feature. For corrections and additions to the Release Notes document, a Release Notes Addendum will be posted on the Lenel Web site: https://partner.lenel.com/downloads/onguard/user-guides. (You will need your Lenel login to gain access to this site.)

Note:	When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

OnGuard installation packages and supplemental materials are now available for download directly from the Lenel Web site: https://partner.lenel.com/downloads/onguard/software. (You will need your Lenel login to gain access to this site.) Download the OnGuard software and create a master disc for all of your client installations.

Lenel Global Education provides instructor-led, Web-based Global Distance Learning for more in depth knowledge on new features. The training is available for Value Added Resellers (VARs), Certified OnGuard System Users, and OnGuard System User Administrators. Visit the Lenel Web site for more details and schedules: http://www.lenel.com/training.

2. Upgrades

- **Upgrading to OnGuard 7.2 (OG-29586):** Direct upgrades of the OnGuard software are supported for all systems OnGuard 7.0 and newer.

  Note: Carefully review the following items to determine whether additional steps are needed for your particular upgrade.

- **End of Life Products Must Be Deleted Prior to Upgrade (OG-23947):** The Database Incompatibility Wizard will run during an upgrade and perform the following checks:

  1. Checks for existing configuration data that must be manually removed before the upgrade can continue. Installation cannot proceed if any of the following are detected:

     - **Hardware:** AAD Readers, AMD-12 Input Panels, Apollo Hardware, Asset Reader Interfaces, Cisco AIC Hardware, Digitize CAPSII Receivers, Fargo DTC550, HID Read/Writer Non-programmer Encoder, ID-Check Terminal Scanner, Identix Fingerscan V20 Readers, LNVS (Lenel Network Video Suite) Hardware
     - **Smart Card Formats:** Cartographer Smart Card Format, CombiSmart Smart Card Format, GSC (DESFire) Smart Card Format, GuardDog Smart Card Format, IE Smart Touch Smart Card Format, Offline Guest Smart Card Format, TI Access Control Smart Card Format, UltraScan Smart Card Format, Windows Certificate Smart Card Format

     Note: For some time, the LDVR and Loronix recorders have not been available for purchase as a product. As part of a planned migration to another recorder/camera technology, the upgrade will not require that these recorders and cameras be deleted. This is normally the case with other end-of-life-product configured in OnGuard. As a result, the OnGuard 7.2 upgrade will mark all camera channels permanently offline. The video configuration for these camera channels will be visible in System Administration, but video for these channels cannot be viewed anywhere, including the camera tab in System Administration. Only the configuration information about the channels can be viewed. They can be deleted, but cannot be modified. This will allow viewing of existing camera device links and related configurations, allowing for an easier configuration of a new recorder technology. The recorders and cameras must eventually be deleted.

  2. Warns that any existing custom reports and DataExchange scripts might not work after upgrade (if they exist). User is prompted as to whether or not they would like to continue installing the OnGuard software.
  3. Warns the user about the existence of the following biometric data that is automatically removed by Database Setup. User is prompted as to whether or not they would like to continue installing the OnGuard software.

     - Identix Fingerprint Templates
     - Ultrascan Fingerprint Templates
     - Biocentric Fingerprint Templates

4. Warns the user, if STENTOFON audio server is configured, that they will need to install the STENTOFON add-on after upgrading the OnGuard software. This prompt does not allow the user to stop the upgrade. It is simply an informative message.

- **Bosch ReadykeyPRO migrations and browser-based applications:** Customers migrating from Bosch ReadykeyPRO to Lenel OnGuard who use browser-based applications on the Application Server must clear cached information in their browser in order to see the correct branding.
- **Visitor Management Kiosk:** The Kiosk is no longer supported. For visitor self sign-in, refer to the new Visitor Self Service product in Section 4 New Features and Updates.

3. Versioning Information

3.1. Current CASI Firmware

- CASI DirecDoor: OCF v2.4.10
- CASI M5, M2000, M3000: OCF v3.4.10

3.2. Current Access Series (LNL) Firmware and Special Application Versions

IMPORTANT!

This note applies to the LNL-500, LNL-1000, LNL-2000, LNL-1100, LNL-1200, LNL-1300, LNL-1300e, and LNL-1320.

Before downloading the firmware in this release to downstream Lenel access control boards, ensure that DIP switch or jumper 8 is in the OFF position. Failure to take this step will result in an inability to communicate to these boards until the switch or jumper position is corrected, and might therefore affect normal operation of your system. By default, boards are shipped with DIP switch or jumper 8 in the OFF position.

- LNL-1100-U, LNL-1200-U, LNL-1300-U, LNL-1320-U: v10.16.01
- LNL-500, LNL-1000, LNL-2000 ISC: v3.121
- LNL-2210, LNL-2220, LNL-3300, LNL-3300-M5 ISC: v1.207
- LNL-4420 ISC: v1.209
- LNL-1100, LNL-1200 Series 1: v1.04
- LNL-1100, LNL-1200 Series 2: v1.32.1
- LNL-1100-20DI, LNL-1200-16DO, LNL-1200-DOR: v1.32.2
- LNL-CK:
    - Rev A: v1.30
    - Rev B: v1.50
    - Rev C: v1.63/v1.50
- LNL-1300 Series 1: v1.11
- LNL-1300 Series 2: v1.52.13
- LNL-1300e: v1.05.13
- LNL-1320 Series 1: v1.13
- LNL-1320 Series 2: v1.57.5
- LNL-1320-2RP, LNL-1320-S2RP: v1.57.3
- LNL-1340-M2K: v1.57.1
- LNL-1380-8RP: v1.57.5
- Bioscrypt with LNL-500B gateway firmware: v1.26
- RSI biometrics with LNL-500B gateway firmware: v1.25
- Recognition Source PIM-485-16-OT with wireless LNL-500W gateway firmware: v1.10

3.3. Current Security Series (NGP) Firmware

- NGP: v1.4.10 (applies to NGP-22xxx and NGP-33xxx panels)
- NGP-1300-U: v12.09.02
- NGP-1320-U: v12.09.02
- NGP-1100-U: v12.09.02
- NGP-1200-U: v12.09.02

3.4. Current ILS Firmware

- Control Module (ACU): 3.0.0.25
- Prox Reader: 3.0.0.1
- iCLASS Reader: 3.0.0.2
- MIFARE® Reader: 3.0.0.14
- WLM NA (North America): 0.9.21358
- WLM EU (Europe): 0.9.21366
- PDA Application (serial): 2.0.4.6
- PDA Application (USB): 3.0.1.3
- WWM NA (North America): 0.9.21358
- WWM EU (Europe): 0.9.21366
- WMC Ethernet Firmware: 2.0.238510
- WMC Wi-Fi Firmware: 2.0.238510

3.5. Current Digital Video Software

- Lenel Network Video Recorder (Lenel NVR): Software Version 7.2.134
- IntelligentVideo Server (IVS): Software Version 7.2.134
- IntelligentVideo Application Server (IVAS): Software Version 7.2.134
- Lenel Streaming Video Server (LSVS): Software Version 7.2.134

> **Note:** The Remote Monitor software version matches the OnGuard product version. To check the OnGuard product version, open any OnGuard application and select ***Help > About***.

3.6. Minimum System Hardware Requirements

- Pentium IV Dual Core Processor, 3.4 GHz clock speed
- 2 GB RAM
- DVD-ROM
- USB Port
- 1024x768 color display
- 6 GB of available space

3.7. Supported Operating Systems

Note:	**Operating system requirements are now enforced.** The installation or upgrade of OnGuard will be blocked on any operating system version not specifically listed as supported in this section. To install OnGuard, upgrade to a supported operating system and service pack.

The following products have been approved with the listed operating systems and system service packs.

3.7.1. Windows 10 Professional

Windows 10 Professional and Enterprise 64-bit editions are approved of OnGuard client operations ONLY. Do not use Windows 10 for OnGuard server installations.

Issues found with OnGuard 7.2 and Windows 10 will be considered for correction in future versions of OnGuard.

Edge Browser is not supported for any OnGuard web applications with this release of OnGuard. Internet Explorer 11 should be used instead in the Windows 10 environment to support OnGuard web applications.

3.7.2. Windows Server 2012

Windows Server 2012 Standard and Enterprise 64-bit editions are approved for all OnGuard server and client operations.

3.7.3. Windows Server 2012 R2

Windows Server 2012 R2 Standard and Enterprise 64-bit editions are approved for all OnGuard server and client operations.

3.7.4. Windows 8/Windows 8.1 Update

- Windows 8 and Windows 8.1 Update 32-bit and 64-bit editions are approved for all OnGuard server and client operations.
- Windows 8 and Windows 8.1 Update 32-bit and 64-bit editions are **not** recommended for use as the Web Service server because of the limited number of client connections in these operating systems.

3.7.5. Windows 7 Professional with Service Pack 1

- Windows 7 SP1 Professional 32-bit and 64-bit editions are approved for all OnGuard server and client operations.
- Windows 7 SP1 Professional 32-bit and 64-bit editions are **not** recommended for use as the Web Service server because of the limited number of client connections in these operating systems.

3.8. Service Packs and Critical Patches

Visit the Lenel Web site for a complete and up-to-date list of approved Microsoft Service Packs (Compatibility Charts section) and Critical Patches (MS Patches section): https://partner.lenel.com/downloads/onguard/compatibility-charts. (You will need your Lenel login to gain access to this site.)

> **Note:** When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

The Security Bulletin and Service Pack Certification Policy, located at https://partner.lenel.com/guide/security-bulletin-and-service-pack-certification-policy, details the specific conditions and frequency of certification for Microsoft Windows Critical Updates. (You will need your Lenel login to gain access to this site.)

Read through this information carefully since it addresses **both operating systems and databases**.

For all instances, Lenel **strongly recommends** enabling the uninstall option when installing the service pack. There have been rare instances where communications and database activity have been affected by the installation of a service pack. When these situations have occurred, uninstalling the service pack resolved the issues. Lenel also **strongly recommends** backing up your database before performing any service pack installation.

3.9. Security Utility

Windows Firewall is supported by use of the Security Utility; other third-party firewalls are not supported.

The Security Utility allows OnGuard users to take advantage of the capabilities of Windows. The utility must be run to ensure that the OnGuard software will continue to function properly. The utility automatically adjusts all settings that affect the OnGuard software. It also displays the current system settings, as well as a list of actions required for normal operation of Lenel software installed on the local computer.

> **Note:** The Security Utility does not open database communication ports.

The Security Utility runs automatically during OnGuard, Lenel NVR, IVS, IVAS, Remote Monitor, and Device Discovery Console installations. It must be run manually after LDVR installations. It must also be run manually as a maintenance procedure after making any of the following changes:

- Lenel NVR security setting changes
- IntelligentVideo Server security setting changes
- Windows updates
- Windows service pack changes
- Windows security setting changes

3.10. Supported Database Systems

For an up-to-date list of tested database systems, refer to the compatibility charts on the Lenel Web site: https://partner.lenel.com/downloads/onguard/compatibility-charts.

> **Note:** When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

When creating or modifying an ODBC connection on a 64-bit operating system, the location where the ODBC Data Sources are configured is different than on 32-bit operating systems:

- For 32-bit operating systems: Click Start, then navigate to Settings > Control Panel > Administrative Tools > Data Sources.
- For 64-bit systems: Navigate to **C:\windows\SysWOW64** and run the **odbcad32.exe** file.
- Microsoft SQL Server 2012 SP2 (64-bit) and Express
- Microsoft SQL Server 2014 R1 (32-bit and 64-bit) and Express
- Microsoft SQL Server 2014 R1 SP1 (32-bit and 64-bit) and Express

> **Note:** Beginning with Supplemental Materials disc revision 16, the SQL Server Management Tools are no longer included. SQL Server Management Tools for Microsoft SQL Server Express are included with Microsoft SQL Server Management Studio Express, and are available at www.microsoft.com. If using a full version of SQL Server, SQL Server Management Studio is included in the full version.

- Oracle 12c R1 Server 64-bit (12.1.0.1) with 32-bit Client installed if OnGuard is running on the same server as the database.

> **Note:** The browser-based applications require 32-bit drivers to connect to an Oracle database.

3.11. Supported System Components

- Acuant SDK version 10.07.16.01
- MDAC (required)
- MSXML 6 (**required**) - MSXML 6 is installed automatically with the OnGuard software.
- Adobe Flash Player 9 or later (**required** for Visitor Management Host)
- Microsoft Silverlight 3.0 or later (**required** for Visitor Administration)
- Microsoft .NET 4.5 (**required**) - Microsoft .NET 4.5 is installed automatically with OnGuard when installing using the **setup.exe** file. To shorten the OnGuard installation time, install Microsoft .NET 4.5 (available on the Supplemental Materials disc) prior to installing the OnGuard software.

Note:	In order for browser-based applications such as FrontDesk, Kiosk, or AdminAPP, to function, HTTP Activation must be enabled for the WCF Services on the server where browser-based applications are deployed. The process for enabling HTTP Activation depends on which operating system you are running. For more details, refer to http://msdn.microsoft.com/enus/library/hh167503%28v=nav.70%29.aspx.

3.12. Internet Information Services (IIS)

Note:	When installing IIS features, you might need to specify an alternate source path to the \Sources\SxS\ directory on the installation media.

- IIS 7.5 is included with Windows 7
- IIS 8.0 is included with Windows Server 2012 and Windows 8
- IIS 8.5 is included with Windows Server 2012 R2 and Windows 8.1 Update

The following IIS requirements are the minimum role services required by OnGuard, regardless of whether using a SQL Server or Oracle database:

- **Common HTTP Features:**
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Redirection
  - Static Content
- **Health and Diagnostics:**
  - HTTP Logging
- **Performance:**
  - Static Content Compression
- **Security:**
  - Request Filtering
  - Windows Authentication

Application Development:

- .NET Extensibility 3.5
- .NET Extensibility 4.5
- ASP .NET 3.5
- ASP .NET 4.5
- ISAPI Extensions
- ISAPI Filters

- **Management Tools:**
  - IIS Management Console
  - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 WMI Compatibility
  - IIS Management Scripts and Tools
  - Management Service

3.13. Virtual Platforms

- VMware ESX/ESXi Server versions 5.5 and 6.0 for all OnGuard services and database server with software-based license only
- VMware Workstation 10.0 and 11.1
- Microsoft Hyper-V Server 2012

Notes:	VMotion, High Availability and Fault Tolerance are supported, however Fault Tolerance is not recommended at this time based upon the mandatory single core limit for current VMware versions. Virtual platforms are not supported with video viewing clients. The software-based license is limited to only VMware ESX/ESXi Server and also to a standard hosted system (non-VMware).

3.14. Supported Third-party Components

- Crystal Reports version 2011 (14.0).

Note:	OnGuard 7.2 ships with Crystal Reports 2011. Earlier OnGuard versions shipped with Crystal Reports 11.5. Reports created with Crystal Reports 11.5 will function normally with Crystal Reports 2011.

3.15. Antivirus Software Applications

Notes: Digital Video systems **must exclude all data drives** from the antivirus scanning operations.

The \LicenseServerConfig\Licenses folder on the License server should also be excluded, since it will sometimes corrupt the license file.

- **McAfee Virus Scan:** McAfee Virus Scan can be recommended, but is not tested and is installed at the user's risk.
- **Symantec Endpoint Protection version 12.1.x:** Symantec Endpoint Protection is used internally and can be recommended.

3.16. Supported Web Browsers

- **Internet Explorer (required for browser-based applications):**
  - Versions 10.0 or 11.0
  - 32-bit version of Internet Explorer when using VideoViewer (Browser-based Client)
- **Apple Safari*:**
  - **Windows:** v5.1.7 or later
  - **Mac:** v8.x or later
- **Google Chrome*:** Version 40.0 or later
- **Mozilla Firefox*:** Version 37.0.1 or later

* Supported OnGuard applications: License Administration

Note: To ensure that the Integrated Configuration Tool (ICT) works as expected and you are using Internet Explorer 10 or later, use the Compatibility View to run in IE 9 mode. Running the ICT on later versions of Internet Explorer without using Compatibility View may cause the ICT to stop responding. The ICT can also be run on the latest versions of Google Chrome and Mozilla Firefox. The following systems use the ICT: DirecDoor, M2000, M3000, M5, and NGP.

3.17. Supported Terminal Services

OnGuard 7.2 supports Terminal Services. This support is a licensed feature. Refer to the Lenel Web site to review the current testing status before configuring terminal services. The Third Party Applications Compatibility Chart can be accessed at: https://partner.lenel.com/downloads/onguard/compatibility-charts. (You will need your Lenel login to gain access to this site.)

Note: When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

Citrix XenApp is not supported for viewing video.

3.18. OPC Versions

- OPC Data Access 2.0
- OPC Alarms and Events 1.0

3.19. SNMP Versions

- SNMPv1 Trap Messages are supported.
- SNMPv2 and SNMPv3 Trap messages are not supported.

3.20. Supported High Availability Systems

For more information, refer to the Third Party Applications Compatibility Chart on the Lenel Web site at: https://partner.lenel.com/downloads/onguard/compatibility-charts. (You will need your Lenel login to gain access to this site.)

> **Note:** When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.

- NEC ExpressCluster X R3 32-bit LAN 3.1 (tested 3.3.0.1)
- NEC ExpressCluster X R3 32-bit WAN 3.1 (tested 3.3.0.1)
- NEC ExpressCluster X R3 64-bit LAN 3.1 (tested 3.3.0.1)
- NEC ExpressCluster X R3 64-bit WAN 3.1 (tested 3.3.0.1)

> **Notes:** Lenel provides instructions for upgrading the OnGuard software only when the NEC ExpressCluster X version, operating system, and database version remain constant. For any other upgrade scenario, we recommend a database backup, the cleansing of both servers in the cluster, clean installs, database restoration, and then database setup. There might be operating system and database system upgrade scenarios where very knowledgeable administrators could avoid erasing the entire configuration, but we cannot guarantee their support.
>
> If your NEC ExpressCluster X configuration is for UL 1981, refer to the section "Recommended NEC ExpressCluster Configuration for UL 1981" in the *UL 1981 Compliance Option Setup and User Guide*.

- Windows Server 2012 R2 Failover Cluster
- Windows Server 2008 R2 Failover Cluster

> **Notes:** For more information, refer to "Clustering and High-Availability" at http://blogs.msdn.com/b/clustering/.

3.21. End of Life Products and Features

Refer to Section 2 Upgrades for the list of end of life products that need to be removed prior to upgrade.

4. New Features and Updates

4.1. Enterprise

- **Last Location replication:** Starting with OnGuard 7.2, Last Location information is replicated using the LS Site Publication Server service. Hardware transactions are still replicated using the Replicator application, service, and scheduler.

  By default, Last Location transactions replicate through the system. However, you can configure a scheduled window for when replication occurs. On upgrade, if no action or schedule was configured for Last Location replication, then the default will be that the replication is disabled.

4.2. OpenAccess

- **Event subscriptions:** OpenAccess allows authenticated users to subscribe to hardware and alarm acknowledgment activity events.
- **Lnl_PersonSecondarySegments:** The Lnl_PersonSecondarySegments data class provides authenticated users View, Add, and Delete access to determine the additional segments assigned to a person. This data class is only available if cardholder or visitor segmentation is enabled.
- **logged_in_user:** The logged_in_user method returns name and ID information about the authenticated user.
- **managed_access_levels:** The managed_access_levels method allows authenticated users to query the access levels they can manage.

4.3. Visitor Management

- **Front Desk:** The Front Desk application has been enhanced for:
  - Signing in/out multiple visitors simultaneously
  - Toggling between event details and visitor profiles tabs
  - Advanced searching
  - Adding multiple hosts for a visit
  - E-mailing and importing templates to register multiple visitors in the system
  - Adding a visit event to an Outlook calendar through e-mailed notifications
  - Updated icons
  - Viewing documents signed by the visitor
- **Visitor Self Service:** Visitor Self Service is an iPad app that allows visitors to sign themselves in or out for visit events. Each iPad must have the proper license to run the application.

4.4. Access Control

- **LNL-4420 Integration:** OnGuard now supports the LNL-4420, an on-board Dual Reader Interface that provides control for up to two single reader doors. Port 1 and Port 2 are available for configuring LNL-4420 readers and alarm panels. The LNL-4420 supports up to 32 downstream devices (reader modules or alarm panels) on each port, with 64 total downstream devices (including 1 onboard reader module).

  Existing LNL-500/1000/2000/2210/2200 controllers can be promoted to an LNL-4420.

- **LNL-1340-M2K Integration:** OnGuard now supports the LNL-1340-M2K, a Four Reader Interface board that accepts data from readers with F/2F and supervised F/2F signaling and door hardware.

  The LNL-1340-M2K supports a flexible door contact, REX, or strike device configuration. The readers can have either standard Reader Edge terminations or custom Board Edge terminations for Door Contact/REX/Strike inputs or outputs from the available 10 alarm inputs and 8 relay outputs of the local LNL-1340-M2K board.

  When the first LNL-1340-M2K reader (number 0) is configured, an associated alarm panel is added automatically. If the LNL-1340-M2K board is physically attached to an LNL-3300-M5, the alarm panel will be on Port 2. If the LNL-1340-M2K is downstream of the LNL-3300-M5, the alarm panel will be on Port 3.

  Elevator and floor tracking support: When the first LNL-1340-M2K elevator reader (number 0) is configured, an associated alarm panel is added automatically but not if the elevator reader has floor tracking. For elevator readers *without* floor tracking, the linked alarm panel allows you to define up to 10 inputs.

  Readers on the same LNL-1340-M2K board can be combined in paired master-slave sets.

- **OSDP Biometrics Updates and ANSI 378 Fingerprint Reader Support:**
  - **Access Panels:** A new **OSDP biometrics** setting was added to the Options form that allows you to specify the type of OSDP biometrics supported by the controller (LNL-4420/3300/2220/2210). Large (640 byte) and Small (320 byte) INCITS 378 fingerprint options are available for better management of template size/access panel memory.
  - **System / Segment Options:** New settings were added to the Biometrics form for configuring the maximum number of templates allowed to be stored in the controller, the minimum score required to pass biometric verification, and whether or not to store the minimum score value per template.
  - **Readers and Doors:** A new "OSDP Biometric" option was added to the reader **Output** setting on the General form. This configuration is supported by both LNL-2220/4420 on-board readers and the LNL-1300e/2210 on-board reader #1.

    Alternate biometric reader support: Biometric readers including the Bioscrypt RS-485 reader, LNL-500B (HandKey biometric gateway), and LNL-500B (Bioscrypt biometric gateway) are now automatically configured as **Alternate Readers**. However, OSDP biometric alternate readers are user-defined to specify 2 different configurations:
    - For OSDP biometric readers used as standard alternate readers, select **Alternate Reader**.

- For OSDP biometric readers that perform both card reading and biometric verification, **Alternate Reader** is *not* selected. Such readers are treated as a single reader.

- **Alarm Monitoring:** If the number of OSDP biometric templates is specified in the System / Segment Options, the hardware tree will display the maximum and current number of OSDP Bio Templates stored on the controller. (Display Controller Capacity must be selected for this to display.) Alternatively, right-click on the controller, and then select ***Properties*** to view this information.

  Biometric Verify Mode > **Enable** / **Disable** menu options are available for primary readers associated with an OSDP biometric alternate readers. This allows you enable or disable biometric verification on demand. (Alternatively, schedule when the biometric verify mode will be enabled or disabled via the Timezone/Reader Modes in the Holidays/Timezones folder.)

- **OSDP Secure Channel Support:** On the Readers and Doors > General form, enable **Secure channel** for the reader to communicate using secure channel communications over OSDP. Supported for LNL-2220 onboard readers # 1 and # 2, LNL-2210 onboard reader # 1, and LNL-1300e reader # 1 with **Output** types "OSDP Protocol" or "OSDP Biometric". Enables the reader to be placed into **Remote Link Mode** in Alarm Monitoring. When the reader is in link mode, the controller and the reader can negotiate secure channel communications.

  Note: Readers configured for secure channel, that are assigned to controllers that support downstream encryption, can also be configured with one of the downstream encryption communications settings.

  Inverted Strike Relay (Failsafe) Configuration: A new setting on the Readers and Doors > General form allows you to specify an Inverted Strike Relay configuration for supported readers:

  - LNL-1300/1300e/1320 readers
  - LNL-2210 on-board reader #1
  - Both LNL-2220/4420 on-board readers
  - 2RP and S2RP readers (Configure inverted strike on the Controls form.)

  Inverted Strike Relay changes the typical behavior of door strike relays. Use this option when the strike and panel use separate power sources and the desired behavior, if the panel loses power, is to automatically release the door strike (activate failsafe). For typical (default) strike wiring, **Inverted Strike Relay** is not enabled.

  Behavior when the strike relay is wired and configured for inverted strike:

  - During Normal conditions (NC or NO), the output relay is activated.
  - When the reader interface module loses power, the relay is deactivated and the door strike is released.

  Note: This option is not available if the reader communication is supervised F/2F or if using a flexible door contact, REX, or strike device configuration.

- **Communication Server Event Reliability:** Events that occur during critical conditions are now preserved from the event queue. (Critical conditions: The database is slow or down for an extended period of time where events are not recorded in a timely fashion and the event queue becomes too large.) Further enhancements include:
    - Improper previous shutdowns are detected and logged upon startup
    - Threshold queue size for a duration: Messages are logged to the database (and LenelError log) when the recording of event transactions to the database exceeds a pre-defined queue size and time threshold.

4.5. Identity Management

- **Encode the Open Encoding Standard (DESFire) Application to the DESFire EV1 Credential:** In order to encode the Open Encoding Standard (DESFire) application to the DESFire EV1 credential, OnGuard supplies the ANSI INCITS 378 fingerprint templates and Badge ID to be encoded into the credential. Prior to encoding, the cardholder fingerprints or biometric PIN is captured using a supported OpenCapture device. The Mapping Table feature is used to import the Badge ID.

  Supported encoder: The HID CP1000 iCLASS SE Encoder Sam SIO firmware version 1.117. The minimum Main Firmware Version is 01000021. Use the encoder as either a desktop encoder or integrated into a Fargo DTC4500e card printer for badge printing. Asure ID Card Personalization Software version 7.5. Asure ID is required to change the encoder's default Administrative Keys and upload credential credits for card transactions.

  Supported reader: Use the MorphoAccess SIGMA Series Terminal firmware release 1.3.9 to read the Open Encoding Standard (DESFire) smart card and authenticate the cardholder fingerprints. This is an Ethernet-connected device. Installation of MorphoBioToolbox software release 2.1.2 is required for configuration of this reader and the key settings.
- **Encode the Custom Data Object (DESFire) Application to the DESFire EV1 Credential:** Configure Custom Data Object (DESFire) card formats using a DESFire card template XML file. Use the template to specify keys, key settings, and file access rights. The contents of the files to be encoded consist of access control data (Wiegand, badge ID, issue code, facility code), UDFs (User Defined Fields) as well as biometric and binary data, and static text that can be customized based on how your data is structured. For information on creating an XML template, refer to the DESFire Card Template XML Specifications guide.
- **Expanded Corporate 1000 Support:** New Wiegand card format **Special** option added for automatically setting all parameters for HID Edge and Edge EVO readers. Support now includes the new "HID Corporate 1000 - 48" option and the update from the previous "HID Corporate 1000" option to "HID Corporate 1000 - 35 ".
- **Multimedia OpenCapture Enhancements:** Two new features were added to the OpenCapture form. In addition, the OpenCapture form was redesigned to make it more intuitive.

  New Save Defaults button was added to customize the OpenCapture default settings after choosing your preferred selections for Store Images, Device, Primary template, and Secondary template.

  Capture and Encode a Biometric PIN: When the cardholder fingerprints cannot be captured, select **Templates not required**, and then enter a **Biometric PIN** to authenticate the cardholder.

4.6. Digital Video

- **De-warped Views of 360-degree Cameras:** Double-click to center and drag the image in Live and recorded video. One license required to stream video. The user interface is the same regardless of camera brand and model.
  - **Modes supported:** Ceiling, Desk
  - **Cameras supported:** Axis (M3007, M3027), Interlogix (TVF-3101, TVF-3102, TVF-3103, TVF-3104), and Panasonic (WV-SF438, WV-SFV480, WV-SFV481)
- **Support for ONIVF Profile S:** ONVIF Profile S is now supported for the Lenel NVR. Refer to the Lenel NVR Release Notes for camera limitations.
- **End-of-Life for LDVR and Loronix Recorders:** For some time, the LDVR and Loronix recorders have not been available for purchase as a product. As part of a planned migration to another recorder/camera technology, the upgrade will not require that these recorders and cameras be deleted. This is normally the case with other end-of-life-product configured in OnGuard. As a result, the OnGuard 7.2 upgrade will mark all camera channels permanently offline. The video configuration for these camera channels will be visible in System Administration, but video for these channels cannot be viewed anywhere, including the camera tab in System Administration. Only the configuration information about the channels can be viewed. They can be deleted, but cannot be modified. This will allow viewing of existing camera device links and related configurations, allowing for an easier configuration of a new recorder technology. The recorders and cameras must eventually be deleted.

4.7. Visitor Self Service (VSS)

- **Visitor Self Service:** Visitor Self Service allows visitors to sign in or out themselves without the assistance of a front desk attendant. After visitors are scheduled, they will receive a confirmation e-mail containing a visit key, which is a barcode or number allowing them to sign in. By using Visitor Self Service to sign in, visitors may update or add contact information, capture their own photograph, and print a temporary badge. That same temporary badge can be designed to have a barcode for signing out visitors. Visitor Self Service is supported on the iPad Air or later, with iOS9. Install Visitor Self Service from the App Store.

5. Known Issues

5.1. General

- **ACS.INI File Cannot be Edited by Administrator Group Member (OG-14034) (OG-19970):** By default, the Admin account does not have permission to save the **ACS.INI** file in Windows 7 Professional, Windows 8, Windows 8.1 Update, Windows Server 2012 R2, or Windows Server 2012.

  To work around this issue:

  - Add the Admin user to the **ACS.INI** file security settings and allow full control, or
  - Run the application that you use to edit the **ACS.INI** file (i.e., Notepad) using the "Run As Administrator" option, or use the configuration editor.
- **SafeNet driver (OG-23789):** The SafeNet driver has been removed from the installation, but if needed it is available on the Supplemental Materials disc.
- **Mobile Monitoring support in OnGuard pending (OG-30103):** At this time, support in OnGuard for Mobile Monitoring is pending. Refer to the Applications Compatibility Chart at https://partner.lenel.com/downloads/onguard/compatibility-charts. (You will need your Lenel login to gain access to this site.)

  Note: When accessing the **Downloads** section at https://partner.lenel.com, make sure to select the version of OnGuard that is currently installed.
- **Client Update:** When performing an upgrade, refer to the Upgrade Guide for information about Client Update. If upgrading from a release prior to OnGuard 2012 (6.5), when upgrading the client machines, the manual steps indicated in the Client Update section in the Upgrade Guide must be followed so that the automatic client update can be used in the future.

  The Client Update Server allows the OnGuard server workstation to automatically update client workstations. When a client workstation opens an application in OnGuard, the application detects that the software version does not match the database. The application then allows the user to either cancel the login or update the client software. This functionality only exists for applications that are part of the OnGuard installation suite. Two services enable this functionality, one installed on the server workstation (LS Client Update Server Service) and another installed on each client workstation (LS Client Update Service). These services are only used to update client workstations. Server workstations must still be updated manually.
- **Replicator Actions after upgrading to OnGuard 7.2:** When upgrading to OnGuard 7.2, all full download and incremental download actions are deleted from Scheduler. These Replicator actions cannot be recreated in OnGuard 7.2 because they are no longer necessary. For more information, refer to Run Replication as a Windows Service in the Replicator User Guide.

5.2. Digital Video

- **De-warped views of 360-degree cameras:** This feature is currently not supported in Area Access Manager, remote monitoring, Web VideoViewer, and video verification.
- **TruVision Recorders:** Motion Detection and Video Sensor configuration in System Administration do not work for TruVision recorder channels configured using ONVIF and RTSP protocols. This is TruVision SDK limitation.

5.3. Installation

- **"Allow service to interact with desktop" option required when using Client Update to update OnGuard (OG-29277, OG-29291):** When using Client Update to update from OnGuard 2012 and service releases, or OnGuard 2013 and service releases, to OnGuard 7.2, the LS Client Update Service on ALL client machines must have the **Allow service to interact with desktop** option selected.

  If using a Windows 8 system, an additional registry change is needed. Set **NoInteractiveServices** to **0** in the registry:
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows`

  Restart the service on each client machine where this change was made.

Note:	For larger numbers of clients, Group Policy can be used to apply this change to the proper organizational units (OU).

5.4. Lenel NVR

- **Digital Video Hardware Guide (DOC-811) discontinued (HPQC# 7598):** The Digital Video Hardware Guide has been discontinued. For Lenel NVR hardware-related information, refer to the Lenel NVR User Guide (DOC-909).

5.5. Visitor Management

- **Front Desk Application: Acuant SnapShell®/Acuant ScanShell®: Must follow "Lenel Installer for Acuant SDK" on Supplemental Materials disc (OG-23349):** In order to use the Acuant SnapShell or Acuant ScanShell devices for scanning business cards in the Visitor Management Front Desk application, run the Acuant SDK installer located on the Supplemental Materials disc. This should be run before connecting the scanner for the first time and will install the necessary driver and SDK. It will also update the Acuant SDK for existing installations.

6. Copyright and Trademark Notice