LenelS2
1212 Pittsford-Victor Road
Pittsford, New York 14534
Tel 866.788.5095  Fax 585.248.9185
www.LenelS2.com

# OnGuard 8.0 Release Notes

## Release Notes Introduction

This document provides an overview about this release and lists of 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 installation media in the **\*Program Files*\*OnGuard*\*doc*\*en-US*\** folder. Documents can be searched using the Search All User Guides feature. Any corrections and additions to the Release Notes document will be posted on the LenelS2 Web site: https://partner.lenel.com/downloads/onguard/user-guides as a Release Notes Addendum.

> ⓘ When accessing the Downloads section at https://partner.lenel.com, always select the version of OnGuard that is currently installed.
>
> Effective October 1, 2020, "UTC Fire & Security Americas Corporation, Inc." changes to "Carrier Fire & Security Americas Corporation".

## OnGuard Materials and Training

OnGuard installation packages and supplemental materials are available at https://partner.lenel.com/downloads/onguard/software. Log in to access and download the OnGuard software and create a master disc or USB drive for all of your client installations.

The LenelS2 Learning Center provides instructor-led CORE training for new students, and advanced courses for returning students. To maintain certifications or to learn about new product features, the LenelS2 Learning Center provides e-Learning. The training is available for Value Added Resellers (VARs), Certified OnGuard System Users, and OnGuard System User Administrators. For details and schedules, visit http://www.lenel.com/training.

## OnGuard Installation and Upgrades

Refer to this section, the OnGuard Installation Guide (Doc-110), and the OnGuard Upgrade Guide (DOC-120) for information about installing and upgrading OnGuard.

### TCP/IP Required for Installation

Installation of OnGuard 8.0 requires using the TCP/IP protocol, which is not always active by default. Prior to installation of OnGuard, installers should go into the SQL Server Configuration Manager for Network Configuration and enable the TCP/IP protocol.

### Additional Database Permission Required for OnGuard Installation and the 'Lenel' User

A new database permission is required for the 'Lenel' user. For more information, refer to "Create a Login" in the Microsoft SQL Server chapter in the Installation Guide or the Upgrade Guide.

# Client Update for OnGuard 7.5 and Later

When a user tries to run Client Update from a client running OnGuard 7.5 or OnGuard 7.5 Update 1, the client cannot connect to a server running OnGuard 8.0. The user is presented with a system error. This impacts the Client Update process, as the user cannot log in without the SA or SA delegate account password. OnGuard currently requires a user to log in before beginning the Client Update process.

There are two options for this limitation:

- Log into an OnGuard application as the SA or an SA delegate user and allow the software to begin the Client Update process.
- Run **Lnl.OG.AutoUpgrade.Client.exe** manually from the client machine, without logging into a thick client. **Lnl.OG.AutoUpgrade.Client.exe** is located in the OnGuard directory (***C:\Program Files (x86)\OnGuard*** by default).

This is not an issue on systems utilizing Windows single sign-on functionality for third-party authentication to log into OnGuard thick clients. It only affects users logging into internal OnGuard accounts (DE128413).

# Remove End of Life Products and Features

Refer to this section for products and features that have reached end-of-life status.

## End of Life Products Must Be Deleted Prior to Upgrade (OG-23947)

The Database Incompatibility Wizard runs during an upgrade and performs the following checks:

Check 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

ⓘ The LDVR and Loronix recorders have not been available for purchase for a long time. As part of a planned migration to another recorder/camera technology, an upgrade does not require these recorders to be deleted before performing an upgrade unlike other end-of-life-products. As a result, the OnGuard 8.0 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.

## Upgrading to OnGuard 8.0

Carefully review the following items to determine whether additional steps are needed before your upgrade. Users may wish to save components that are otherwise deleted or over-written before starting the upgrade.

### OnGuard Modules (CSS, WATCH, Policies)

When planning your OnGuard upgrade, make sure you have the latest supported versions of any OnGuard modules installed in your current OnGuard environment. Check the compatibility charts to confirm what module versions are necessary to support the upgraded version of OnGuard.

For OnGuard 8.0, changes to the configuration of our NGINX web server require that you upgrade versions of your installed OnGuard Modules. If incompatible versions of the modules are present, the system might experience issues with running the LS Web Services for the platform.

ⓘ **CAUTION:**

Using OnGuard with incompatible versions of the OnGuard modules might cause unexpected issues with your installation.

### DataExchange

Any existing custom reports and DataExchange scripts should be validated for upgrade.

### STENTOFON

If STENTOFON audio server is configured, users need to install the STENTOFON add-on after the OnGuard upgrade completes.

### MobileVerify

Starting with OnGuard 7.4, MobileVerify is no longer supported. If this feature was enabled, the MobileVerify controls must be manually removed from cardholders using OnGuard FormsDesigner.

## Upgrading to OnGuard Enterprise 8.0

It is critical that upgrading an enterprise system to OnGuard Enterprise 8.0 is performed in the proper sequence.  For more information, refer to “Proper Sequence for Upgrading an Enterprise System” in the OnGuard Upgrade Guide (DOC-120) .

# New Features and Updates

## Interface Terminology Updates

Beginning in the OnGuard system version 8.0, LenelS2 will begin to update terminology within the OnGuard platform applications. In particular, the use of 'Master/Slave' previously used to describe configuration of our reader hardware, and the use of 'Master' to describe the authoritative database within the platform’s enterprise management, are being replaced within the user interface for this release. A follow-on effort for similar updates to our documentation, literature, and language packs will continue through the 2021 release of the OnGuard platform.

As part of this effort, the following terminology changes will be made in the interface, so users will need to be aware of the updated terms and their mapping within both documentation and prior versions of the software:

- 'Master/Slave' with regard to reader configuration will now use the terms 'Primary/Secondary.'
- 'Master' with regard to describing the top-level OnGuard Enterprise application server will now use the term 'Global.'

While updates to OnGuard system-specific terminology are being made, these do not account for all uses of the term 'Master' within other industry domains at this time. In these cases, the terms will remain in use to avoid confusion. Areas that will not be updated include ‘Master Keys’ in the credential technology and encryption domains, and ‘Master Permissions’ in the intrusion domain, among others.

## Allegion Schlage Wireless RU/RM Support

OnGuard now supports Schlage's Von Duprin RU (Remote Undog) and RM (Remote Monitor) modules installed inside new or existing 98/99 and 33A/35A exit door push bars. These battery powered modules connect wirelessly to the Schlage ENGAGE Gateway allowing use of the RU/RM (Remote Undogging/Remote Monitoring) options in OnGuard. Undogging (securing) of the door is automated so that the push bar is active (latched). In an emergency, immediately lock/unlock (undog/dog) doors manually, or issue a central lockdown to all doors with RU/RM push bars. For instructions to configure this device in OnGuard, refer to “Schlage Reader and Lock Solutions” in the OEM Device Configuration Guide.

The RU/RM is supported on LNL-X-series controllers (LNL-X4420, LNL-X3300, LNL-X2220, and LNL-X2210) and can be mixed on the same ENGAGE Gateway with Schlage NDE/LE electronic locks. The RU/RM is configured in OnGuard similar to Schlage AD-400 and NDE/LE electronic locks.

Each RU or RM module defined in the system counts against the standard OnGuard Reader License.

- **RU/RM Reader Modes in System Administration**:
    - “Locked” puts the door in a secured (undogged) mode, where the push bar is latched.
    - (New) “Unlock Next Exit” secures the door until the next use when the push bar is pressed.
- **Setup Required to Have an RU/RM Report Door Use When in Locked State**:
    - In the System Administration > Reader and Doors folder for an RURM, select the Controls tab. Under REX, select the option "Report request to exit events".
    - This option is configured individually for each RU/RM you want to have report Door Usage.
- **New RU/RM Events**:
    - Reader Mode Unlock Next Exit: Generated when the reader mode changes to “Unlock Next Exit".
    - Latchbolt Active: Generated when a latchbolt active condition is detected for the RU/RM device.
    - Latchbolt Failed to Engage: Generated when a latchbolt blocked condition is detected for the RU/RM device.
    - Lock Device Failure (Failed to Unlock): Generated when the door fails to unlock due to a mechanical key being placed in an incorrect position.
    - Lock Device Failure (Slipped): Generated when the door fails to lock due to the hook becoming disengaged from the trigger, leaving the trigger in the "Unlocked" (dogged) mode.
    - Door Open by Key: The door was opened by use of a mechanical key.
    - Several existing events are used for the RU/RM such as "Reader Mode Locked", "Reader Mode Unlocked", "Reader Manipulation Tamper - Magnetic Manipulation", and "Request to Exit - Door Used".
- **RU/RM Reader Statuses in Alarm Monitoring**:
    - (New) Reader Status Unlock Next Exit
    - Reader Status Locked
    - Reader Status Unlocked
- **New Reader RU/RM Status Icons Added to Maps**:

| | |
|---|---|
| 🟥🔒 | Locked |
| 🟥➜ | Unlock Next Exit |

| | |
|---|---|
| 🔓 | Unlocked |

## Magic Monitor Support

OnGuard 7.5 and later support Magic Monitor integration.

- Magic Monitor integration with OnGuard requires an OnGuard subscription software license with the Magic Monitor feature enabled. When adding the OnGuard system to Magic Monitor, if the OnGuard system's connection status shows **Not licensed**, then the OnGuard subscription software license does not have the Magic Monitor feature enabled. Each Magic Monitor installation also requires a Magic Monitor "PLUS" license, provisioned through the Cumulus cloud portal.
- Specific video recorders and cameras (Lenel NVR, UltraView, and Milestone only) integrated with OnGuard are automatically imported into Magic Monitor as part of the OnGuard system, and do not require additional licensing in Magic Monitor. Milestone recorders that are not integrated with OnGuard must be configured locally in Magic Monitor, and require separate third-party camera licensing in Magic Monitor.
- In order to view or modify cardholder information in  Magic Monitor when used with OnGuard 7.5 or OnGuard 7.6, the customer must also have an OnGuard subscription software license that includes the "OnGuard Credentials client" license.
- When OnGuard 8.0 and later is installed, a card for the Magic Monitor thick client application is created in Lenel Console by default. This card is not functional unless Magic Monitor is installed on the client machine. If Magic Monitor will not be used, you can hide this card. For instructions on hiding a card, refer to the online help in Lenel Console.
- If the OnGuard server is not configured in Magic Monitor, launching Magic Monitor from Lenel Console will not allow Magic Monitor to log into OnGuard. Add the OnGuard system in Magic Monitor if necessary.
- If Lenel Console is connecting to an OnGuard system running on Machine A, and the OnGuard system configured in Magic Monitor is running on Machine B, Magic Monitor does not log into the OnGuard server automatically when launched from Lenel Console. Confirm that the OnGuard system configured in Magic Monitor matches the Lenel Console URL in your browser.
- While Magic Monitor's integration with OnGuard is supported for OnGuard 7.5 and later, complete cardholder management functionality with OnGuard 7.5 and OnGuard 7.6 requires that the OnGuard Credentials web application is version 2.2.9 or later.
- If you change your configured OnGuard system in Magic Monitor to a different OnGuard system, any widgets you created that were associated with the original OnGuard system might need to be reconfigured. Inconsistent behavior might occur until the widgets are reconfigured.
- If a Magic Monitor system is configured to connect to an OnGuard system, then Forensics functions are available for analyzing events and video from that OnGuard system.
- The user will not get video from an UltraView recorder in Magic Monitor if the UltraView RTP server has authentication enabled. The solution is to install the UltraView RTP server without authentication enabled.
- The OnGuard Maps widget type is only available for OnGuard 8.0 and later systems.
- Magic Monitor might prompt the user for Lenel NVR credentials (once per recorder) when Lenel NVR security is turned on and OnGuard 7.5 or OnGuard 7.6 versions are used.
- Milestone recorders connected through OnGuard are only supported with OnGuard 8.0 and later. Milestone recorders can be configured directly in Magic Monitor with any OnGuard version, but features such as event-camera links only work in OnGuard 8.0 and later.
- Cameras marked offline in OnGuard System Administration are still available in the Magic Monitor user interface when OnGuard 7.5 or OnGuard 7.6 are used.
- After adding a new cardholder in OnGuard 7.5 or OnGuard 7.6 using Magic Monitor, the list of cardholders and the OnGuard Credentials menu are shown in the Add Person pane.
- When cardholders are assigned additional segments in OnGuard, it is not possible to search for those cardholders in Magic Monitor by using the additional segment as a filter.
- The dark theme is not supported in the version of OnGuard Credentials that is officially compatible with OnGuard 7.5.
- The user is not shown a warning prompt if the Add Person page is closed with unsaved data.
- In addition to French, Magic Monitor is now also localized into Spanish.

## SA Delegate User Account

OnGuard now supports the option of creating an SA Delegate User Account. An SA Delegate User Account has all the permissions of the OnGuard System Account, but can be associated to a specific user(s) in support of better transaction auditing as well as allowing the default System Account (with a shared password) to be disabled for use. It is recommended that new and existing customers take advantage of this option to create specific SA Delegate Accounts (for their 'system level' users) and that these accounts be treated as privileged and in general separate from accounts used for day to day operations.  For more information, see the Users Folder in the System Administration User Guide.

## SQL Server 2019 Support

OnGuard 8.0 supports SQL Server 2019 (64-bit). Refer to the Compatibility Charts and open the **Database Compatibility Chart**.

## Transport Layer Security (TLS) Encryption and Certificates

TLS encryption between LNL-X Series access panels and the OnGuard server is enabled by default when adding new controllers. TLS encryption is unchanged for existing LNL-X Series access panels.

The default TLS certificate for LNL-X Series access panels (Mercury_CertRootCA4096.crt ) is installed on the OnGuard Communication Server during the OnGuard installation process.

## OnGuard Monitor 1.3 (with Maps)

With OnGuard Monitor 1.3, users now have the ability to view existing OnGuard maps in an integrated browser-based environment. Maps can be displayed in a separate browser window, as a new tab, or create a map widget to be displayed within your custom layouts.

This support also provides the following features/functions:

- View devices on one or more graphical maps within your browser.
- Allows for Pan/Zoom within the area of the maps.
- Launch maps from the device within the hardware tree or from an alarm.
- View status and control supported devices with your mouse, or use a touch interface.

## Wacom Intuos Pro Tablet Support

The Wacom Intuos Pro Small USB Signature Capture Kit (LenelS2 part number INTUOS-PRO-SMALL) is a graphics tablet with a compact footprint that you can use to capture and digitize signatures. Includes digitizer tablet, pen, and pen stand.

***Note:*** The Wacom part number for the newest signature capture kit is PTH-460. The previous kit’s part number is PTH-451. OnGuard supports both versions.

For information on how to use the Wacom Intuos Pro Small USB Signature Capture Kit with System Administration or ID CredentialCenter, refer to the OnGuard OEM Device Configuration Guide.

For hardware assembly and installation, refer to the Wacom product documentation.

## OnGuard Video Web Package

The OnGuard Video Web Package is installed in an OnGuard environment to support Milestone XProtect video in LenelS2 web-based applications such as OnGuard Surveillance and OnGuard Monitor. Additional future video recorders will be provided through the LenelS2 OAAP program, requiring an updated OnGuard Video Web Package.

The OnGuard Video Web Package is not required for Lenel NVR or UltraView recorders.

## OnGuard Reporting and Dashboards

OnGuard Reporting and Dashboards is a new reporting engine that enables browser-based report execution and scheduling on a variety of platforms, including desktop and mobile. An optional "OnGuard Advanced Reporting" license allows customization of reports and dashboards. OnGuard Reporting and Dashboards provides a new set of reports that complement and extend the reports already provided in OnGuard, and allows graphical dashboards to be embedded in Lenel Console.

### Report Types

The following types of reports are provided:

- **Page reports:** These reports provide pixel-perfect rendering and preview.
- **Dashboards:** Dashboards consist of metrics displayed in the form of charts, graphs, and tables, which can be embedded in Lenel Console, or run from the new browser-based OnGuard Reports client.

### OnGuard Reports Client

Browser-based report execution and scheduling is conducted via the new OnGuard Reports client. This client is included with OnGuard 8.0 and does not require any additional installation or licensing in order to run, schedule, or edit page or dashboard reports. Users can sort and filter reports before outputting. Advanced customization of reports requires "OnGuard Advanced Reporting", which is enabled by a separate license bit. The OnGuard Reports client respects OnGuard permissions and segmentation, and supports per-report permissions. Reports can be exported and scheduled in a variety of formats, including print, PDF, email, and csv.

## License Administration Change

- **"Activation ID" field change (DE132005):** In the License Administration application, the “Activation ID” field was renamed to “System ID” to avoid confusion.

# OnGuard Version Support

Refer to this section for OnGuard version support.

## Compatibility Charts

Compatibility charts list currently supported OnGuard versions and components and are available on the LenelS2 Web site: https://partner.lenel.com/downloads/onguard/8.0/compatibility-charts.

To access OnGuard Compatibility Charts:

1. Click the **Choose product or service** drop-down, select **OnGuard**.
2. Click the **Choose version** drop-down, select **OnGuard 8.0**.
3. Click the **Choose type of download**, select **Compatibility Charts**.

## HID pivCLASS SDK Update for FICAM

Refer to the Compatibility Charts and open the **Third Party Applications Compatibility Chart**.

## Firmware

Refer to this section for information on firmware version support.

### Current CASI Firmware and Drivers

Refer to the Compatibility Charts and open the **Access Control Hardware Compatibility Chart**.

### Current Access Series (LNL) Firmware and Special Application Versions

Refer to the Compatibility Charts and open the **Access Control Hardware Compatibility Chart**.

Reader to interface wiring installation instructions are provided with this release.  This includes the diagrams for Supervised F/2F support.

> ⓘ For LNL-3300-M5: v1.267, use AES encryption with controller firmware version 1.256 or higher, the OnGuard system must be updated to OnGuard 7.6 or later. Prior versions of the DLL file in OnGuard ISC AES encryption are not supported by firmware version 1.256 or higher.

**IMPORTANT!**

This 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.

### Current ACU Series and SH Series Firmware

Refer to the Compatibility Charts and open the **Access Control Hardware Compatibility Chart**. Locate **Migration (ACU)** in the **Hardware Series** column of the chart.

### Current SH Series Firmware

Refer to the Compatibility Charts and open the **Access Control Hardware Compatibility Chart**. Locate **Migration (SH)** in the **Hardware Series** column of the chart.

### Current Security Series (NGP) Firmware

Refer to the Compatibility Charts and open the **Access Control Hardware Compatibility Chart**.  Locate **Security** in the **Hardware Series** column of the chart.

### Current ILS Firmware

Refer to the Compatibility Charts and open **Badge Printers Compatibility Chart**.

## Current Digital Video Software

Refer to the Compatibility Charts and open the **Digital Video Products Compatibility Chart**. The Remote Monitor software version matches the OnGuard product version. Open any OnGuard application and select ***Help*** > ***About*** to view the OnGuard product version.

## Recommended Minimum System Hardware Requirements for OnGuard

These are general hardware requirements for OnGuard servers and client workstations.

**Notes:**

- Operating system requirements may be higher. Consult Microsoft documentation for operating system minimum/recommended hardware specifications. The same applies to the Database Management System if hosted on the OnGuard server.
- In some cases, third-party requirements may exceed the recommended minimum hardware requirements for OnGuard. Refer to the relevant third-party documentation prior to installing OnGuard.

### Access Control Server

- Operating System: Windows 64 bit (For a complete list of supported operating systems, refer to the Compatibility Charts and open the **Operating Systems Compatibility Chart**.)
- CPU: Intel Core i3 @ 2.5 GHz
- RAM: 16 GB
- Hard Drive: 10 GB available disk space (excluding the operating system). If hosting the database locally, take database growth into account when projecting future disk space.
- Monitor: 1920 x 1080
- Media: USB 2.0 or higher
- Network: 100/1000 Mbps Ethernet card

### Access Control Client Workstation

- Operating System: Windows 64 bit (For a complete list of supported operating systems, refer to the Compatibility Charts and open the **Operating Systems Compatibility Chart**.)
- CPU: Intel Core i3 @ 2.5 GHz
- RAM: 8 GB
- Hard Drive: 10 GB available disk space (excluding the operating system). If hosting the database locally, take database growth into account when projecting future disk space.
- Monitor: 1920 x 1080
- Media: USB 2.0 or higher
- Network: 100/1000 Mbps Ethernet card

### Video Server

**Note:** The video server may optionally include the access control server, but hosting the database locally is not recommended.

- Operating System: Windows 64 bit (For a complete list of supported operating systems, refer to the Compatibility Charts and open the **Operating Systems Compatibility Chart**.)
- CPU: Intel Core i5 @ 3.7 GHz
  - **Note:** The majority of AMD CPU's support all the same software that can run on Intel, so it is expected that OnGuard would run normally on them. However, this has not been tested on actual hardware.
- RAM: 16 GB
- Hard Drive: 2 TB available disk space (discounting the OS). Project necessary disk space depending on recorded video retention policy, number of cameras, resolution, etc.
- GPU (if playing video): Intel HD Graphics 530. (If hardware acceleration is required add a graphics card fitting the processing requirements).
- Monitor: 1920 x 1080
- USB 2.0 or higher
- Network: 1000 Mbps Ethernet card

## Supported Operating Systems

For a complete list of supported operating systems, refer to the Compatibility Charts and open the **Operating Systems Compatibility Chart**.

> ⓘ **Operating system requirements are enforced.** Installations and upgrades of OnGuard are blocked in the main installation and when upgrading using Client Update on some operating system versions. However, this is not possible for some operating systems. Ensure you are using a supported operating system and service pack. For details of each operating system, refer to the Compatibility Charts and open the **Operating Systems Compatibility Chart**.

## Microsoft Security Bulletin and Service Packs

Refer to the https://partner.lenel.com/advisories/onguard/8.0/microsoft-security-bulletins. The bulletins detail Microsoft specific conditions and critical updates. Read through the latest posted bulletin carefully.

## Security Utility

The OnGuard Security Utility automatically installs during OnGuard, Lenel NVR, IVS, IVAS, Remote Monitor, and Device Discovery Console installations. This utility ensures OnGuard software functions properly and automatically adjusts all settings that affect OnGuard software. In addition, it displays current system settings, and lists actions required for normal operation of Lenel software installed on the local computer. The Security Utility does not open database communication ports.

The Security Utility must 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 installations
- Windows security setting changes

## Supported Database Systems

Refer to the Compatibility Charts and open the **Databases Compatibility Chart**.

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 64-bit systems, navigate to **C:\windows\SysWOW64** and run the **odbcad32.exe** file.

ⓘ Beginning with Supplemental Materials media 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.

For best performance and support of Oracle 19c, OnGuard 8.0 requires **Oracle Provider for OLE DB**. Previously, OnGuard used **Microsoft ODBC Driver for Oracle** by default. Starting with OnGuard 8.0, the ACS.ini configuration file defaults OnGuard applications to use Oracle Provider for OLE DB by adding the parameter **UseOraOLEDBProvider=1** on new installations and upgrades. Oracle Provider for OLE DB is installed with the OnGuard software. No additional user action is required. To switch to using Microsoft ODBC Driver for Oracle, change the ACS.ini setting to **UseOraOLEDBProvider=0**. However, Microsoft ODBC Driver for Oracle is not recommended and causes instability in some OnGuard applications.

Browser-based applications require 32-bit drivers to connect to an Oracle database.

The supported version of the SQL Server Express installer is available on the Supplemental Materials media.

## Supported System Components

Refer to the Compatibility Charts.

- Acuant SDK:
  - Refer to the **Third Party Capture Devices Compatibility Chart** for currently supported version.
  - Acuant SDK 10.19.14.01 (800DX) is installed with OnGuard 8.0. As part of this installation, the ScanShell 800R, SnapShell, and SS800DX drivers are installed.
  - Due to a third-party compatibility issue, ScanShell 1000 drivers must be installed manually after the OnGuard installation by running the Acuant SDK Scanning Solutions setup file on the Supplemental Materials media in the ***Credential Center Device Drivers > Acuant (Card Scanning Solutions)*** directory.
  - If a previous version of the ScanShell 1000 drivers are already installed, see Knowledge Base article #3585 for additional information.
- MSXML 6 is required and automatically installed with the OnGuard software.
- Adobe Flash Player 9 or later is required for Visitor Management Host.

ⓘ Adobe Flash Player will not be supported in Microsoft Edge and Internet Explorer browsers on 12/31/2020. LenelS2 recommends customers use Cardholder Self Service to provide visitor management functionality for hosts. Contact your LenelS2 sales representative if you do not already have Cardholder Self Service.

- Microsoft .NET is required. The most currently supported Microsoft .NET version is installed automatically with OnGuard when using the setup.exe file. Refer to the **Third Party Applications Compatibility Chart**. To shorten the OnGuard installation time, install Microsoft .NET (available on the Supplemental Materials media) prior to installing the OnGuard software.

ⓘ In order for browser-based applications such as FrontDesk 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.

## Internet Information Services (IIS)

IIS 8.5 is included with Windows Server 2012 R2 and Windows 8.1 Update

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

A detailed listing of the minimum services required by OnGuard, regardless of whether using a SQL Server or Oracle database, is available in the OnGuard Installation Guide (DOC-110).

## Security

Refer to this section for security-related version support information.

### Windows Authentication

Windows authentication is required to support Single Sign-On for the OnGuard web applications.

### Application Development

- **.NET Extensibility and ASP .NET**: Required to deploy and run the OnGuard web applications and web services. Refer to the Third-party Application Compatibility Chart on Partner Center for the supported versions of .NET.
- **ISAPI Extensions and ISAPI Filters:** Required to deploy video streaming through IIS.

### Management Tools

- **IIS Management Console:** Required to manage the IIS web server.
- **IIS 6 Management Compatibility, IIS Management Scripts and Tools and Management Service:** Used during the OnGuard installation process and to manage IIS via scripting.

## Virtual Platforms

Refer to the Compatibility Charts and open the **Virtualization Products Compatibility Chart**.

ⓘ VMotion, High Availability and Fault Tolerance are supported, however Fault Tolerance is not recommended at this time based on 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).

## Supported Third-party Components

Refer to the Compatibility Charts and open the **Third Party Applications Compatibility Chart**.

Additional third-party versioning information is located in the **Third Party Capture Devices Compatibility Chart**, the **Third-Party Encoders Compatibility Chart** and the **Third-Party Hardware Compatibility Chart**.

ⓘ To use the CP1000 encoder for iCLASS encoding with OnGuard 7.6, the most recently supported version of the Azure ID Client application (Asure_ID_Setup_v7.x.x.xxx.exe) must be installed. Refer to the **Third Party Encoders Compatibility Chart**.

Newly supported Third-party printers are listed below. For a detailed list of supported badge printer, refer to the Compatibility Charts and open the **Badge Printers Compatibility Chart**.

### Zebra ZC100 and ZC350

This version supports the Zebra ZC100 and ZC350 badge card printers. The ZC100 is a single sided card printer used for printing cards and badges with encoded magstripe in Thick and Web client environments. The ZC100 has similar functionality as the discontinued ZXP1 printers.

The Zebra ZC350 single and dual sided printer magstripe encoder is supported for use in Thick and Web client environments.

### Fargo HDP5600 and HDP6600

This version supports the use of the Fargo HDP5600 and HDP6600 single and dual-sided printer with magnetic stripe encoder. iCLASS and DESFire encoding are also supported when the correct encoder is added and configured.

### HID CP1000D and iCLASS SE Programmer

Configuration instructions for these programmers and upgrade kits are now included with the documentation. Administrator keys and prerequisites have been added for this release. For more information, refer to “HID CP1000S and 5127 iCLASS Programmer” in the OEM Device Configuration Guide (DOC-603).

ⓘ You must use the firmware and Asure ID software version supplied on the Supplemental Materials media unless otherwise instructed by LenelS2 OnGuard Technical Support.

## Antivirus Software Applications

- **McAfee Virus Scan:** McAfee Virus Scan is not tested. Use at your own risk.
- **Symantec Endpoint Protection:** Symantec Endpoint Protection is used internally and can be recommended. Refer to the Compatibility Charts and open the **Third Party Applications Compatibility Chart**.

ⓘ **CAUTION**

The following **MUST BE EXCLUDED** from antivirus scanning:<br>
**All Digital Video system data drives**<br>
The **\LicenseServerConfig\Licenses folder** on the License, otherwise the antivirus may corrupt the license file.

## Supported Web Browsers

Internet Explorer is required for legacy browser-based applications, such as Area Access Manager (browser-based client) and VideoViewer (browser-based client), and the Integrated Configuration Tool (ICT), which is used by the DirecDoor, M2000, M3000, M5, and NGP controllers. Refer to the Compatibility Charts and open the **Third Party Applications Compatibility Chart**.

ⓘ To ensure that the 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.

## Supported Terminal Services

OnGuard supports Terminal Services. This support is a licensed feature. Refer to https://partner.lenel.com to review the current testing status before configuring terminal services. Citrix Virtual Apps are not supported for viewing video.

## OPC Versions

- OPC Data Access 2.0
- OPC Alarms and Events 1.0

## SNMP Versions

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

## Supported High Availability Systems

Refer to the Compatibility Charts and open the **Third Party Application Compatibility Chart**.

Instructions are provided for upgrading the OnGuard software only when the NEC ExpressCluster X version or Microsoft Cluster Services, 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.

## End of Life Products and Features

Refer to the Remove End of Life Products and Features section for the list of end of life products that need to be removed prior to upgrade.

# OnGuard Known Issues

Refer to this section for known issues with the current version of OnGuard.

## Access Control Known Issues

- **Videology cameras (DE39825)**: When using a Videology camera in OnGuard, the attached flash unit does not activate no matter how dark the lighting for attempted pictures. The flash function is only supported through a TWAIN interface, not from the WDM interface. Resolution: In System Administration Cardholders Capture, select "Digital Camera" as the **Camera Source** and "Videology USB Camera" as the **Twain Source**, then click [Get Photo].
- **Advisor Advanced - incorrect device ID reported for Open Door (DE127165)**: Using Alarm Monitoring to unlock a door connected to an Advisor Advanced panel can sometimes generate an incorrect Open Door alarm due to an Advisor Advanced Device Translator error. This is a known issue that will be addressed in a future release.
- **Extended Open time is not correctly processed for Assa Abloy Aperio locks (DE131191)**:
Extended Open time is not respected for Aperio locks. This issue will be addressed in a future release.

## DataCondulT Known Issues

- **DataCondulT option installs during a custom installation, but the service fails to start and generates a WMI error (DE132252):** To resolve this issue, select the **DataCondulT** and **OpenAccess** options when performing a custom installation.

## Digital Video Known Issues

- **Video window returns to default size when Instant Rewind goes to a time prior to the start time (DE128291)**: In Alarm Monitoring, video is launched with a specific start time. If after resizing the Video Player window Instant Rewind is used to view a time that precedes the start time, the Video Player window returns to the original size. This is a known issue that will be addressed in a future release.

- **The Sub-stream camera Port is not the same as the main-stream even though the "Add a live sub-stream" checkbox is checked when adding a main-stream with a non-default port (DE39307)**: If a camera is added and configured for a non-default port value (not 80), and the "Add a live sub-stream" box is checked, the sub stream channel will not automatically be configured to use the same non-default port. Configure the port manually.
- **Cameras show as offline in VideoViewer tree if the camera name is changed in OnGuard Administration (DE14255)**: Log out and then log in again to view the camera with the new name.
- **There is no warning message to indicate that a camera is offline when attempting updating storage statistics in System Administration (DE14082)**: Reconcile with the status in Alarm Monitoring before attempting to update statistics.
- **Searching for video in Alarm Monitoring causes an error for TruVision recorders that have an "at" (@) symbol in the password (DE16768)**: To use Video Search with TruVision, the recorder cannot be configured with a password containing non-alphanumeric characters.
- **Sub-stream is not online after checking “Add a live sub-stream” (DE15601):** After adding a camera and selecting the “Add a live sub-stream” option in System Administration, the sub-stream has a yellow X and video cannot be viewed for that sub-stream in Alarm Monitoring. Re-enter the password for the sub-stream in System Administration.
- **De-warped views of 360-degree quad cameras (DE15602):** Changing a camera model from 360-degree does not update the 360-degree specification. For example, changing M3027 to M3027 Quad results in a de-warped view of the 360-degree quad. Delete the 360-degree camera and add it again with the correct model.
- **De-warped views of 360-degree cameras (DE7368, DE7620)**: This feature is currently not supported in Area Access Manager, remote monitoring, Web VideoViewer, Web Access Area Manager, and video verification.
- **Event Locking (DE14333)**: Video event locking settings and controls are enabled but ignored for recorders that do not support the feature including TruVision and some OAAP recorders. This is a known issue that will be addressed in a future release.
- **TruVision Recorders (DE15603):** Motion Detection and Video Sensor configuration in System Administration do not work for TruVision recorder channels configured using ONVIF and RTSP protocols.
- **UltraView Recorders (S62809):** The user will not get video from an UltraView recorder in Magic Monitor if the UltraView RTP server has authentication enabled. The solution is to install the UltraView RTP server without authentication enabled.

## High Availability Systems

**Updates needed to the MS Clustering Guide (DE132249)**: A command outdated since OnGuard 7.5 needs to be changed in the documentation to be inclusive of all supported versions of OnGuard. In addition, a new section needs to be added to sync the RabbitMQ password on both sides of the cluster. (Also applies to the NEC ExpressCluster guides.)

### Manually Issue an SSL Certificate

To change <*virtual computer name*> to the **CNAME** of the cluster, perform the following steps:

1. On the active node, open a command (CMD) prompt with run as administrator and navigate to C:\program files(x86)\OnGuard\Certificates\.
2. In the command prompt, execute the following command:
   Change <*virtual computer name*>:
   **For OnGuard 7.5 or 7.6:**
   lnl_app_server_certificate_installer.exe -key=C:\ProgramData\Lnl\nginx\conf\ls_server_cert_key.pem -cert=C:\ProgramData\Lnl\nginx\conf\ls_server_cert.pem -cn=<*virtual computer name*>

   **For OnGuard 8.0 and later:**
   lnl_app_server_certificate_installer.exe -key=C:\ProgramData\Lnl\nginx\conf\ls_server_cert_key.pem -cert=C:\ProgramData\Lnl\nginx\conf\ls_server_cert.pem -keystore="C:\Program Files (x86)\OnGuard\LicenseServerConfig" -cn=<*virtual computer name*>

3. Failover and repeat steps 1-2 on the other node.

### Sync RabbitMQ Password in OnGuard 7.6 and Later

To sync the RabbitMQ password on both sides of the cluster, perform the following steps:

1. On the active node, run cmd.exe as Administrator.
2. Navigate to the RabbitMQ Server directory (default location: C:\Program Files\RabbitMQ Server\rabbitmq_server-3.7.17\sbin).

3. Run the following command:  
   rabbitmqctl change_password LenelRabbit <*new_password*>
4. In System Administration: From the Administration menu, select System Options.
    a. On the RabbitMQ tab, click [Modify].
    b. Enter the new password.
    c. Click [Test Connection] to confirm the new password works.
    d. Click [OK], and then close.
    e. Close System Administration.
5. Failover to other side. Repeat steps 1-3.
6. In System Administration: From the Administration menu, select System Options.
    a. On the RabbitMQ tab, click [Modify].
    b. Click [Test Connection] to confirm the new password works.
    c. Click [OK], and then close.
    d. Close System Administration.

## OnGuard Reporting and Dashboards Known Issues

- The initial release of OnGuard Reporting and Dashboards is available only in English.
- OnGuard Enterprise is not supported.
- Oracle databases are not supported.
- Archive databases are not supported.
- MS Cluster environments are not supported.

## System Administration Known Issues

- **Unable to edit badge type and issue code after printing the badge. (DE16069):** Once a badge has been printed, the badge type cannot be changed and a code can no longer be issued.
- **Hebrew: Instruction template with Native Characters are removed while displaying in OnGuard Monitor (DE16001)**: When displaying double-byte characters like Hebrew, the text is not always clearly legible.

# Copyright and Notices

Non-English versions of LenelS2 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 described in this document is furnished under a license agreement and may only be used in accordance with the terms of that agreement.

SAP® Crystal Reports® is the registered trademark of SAP SE or its affiliates in Germany and in several other countries.

Integral and FlashPoint are trademarks of Integral Technologies, Inc.

Portions of this product were created using LEADTOOLS ©1991-2011, LEAD Technologies, Inc. ALL RIGHTS RESERVED.

Active Directory, Microsoft, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NEC, ExpressCluster and ExpressCluster X are registered trademarks or trademarks of NEC Corporation in the United States and other countries.

Oracle is a registered trademark of Oracle International Corporation.

Amazon Web Services and the "Powered by AWS" logo are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

Other product names mentioned may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

**Product Disclaimers and Warnings**

THESE PRODUCTS ARE INTENDED FOR SALE TO, AND INSTALLATION BY, AN EXPERIENCED SECURITY PROFESSIONAL. LENELS2 CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL SECURITY RELATED PRODUCTS.

LENELS2 DOES NOT REPRESENT THAT SOFTWARE, HARDWARE OR RELATED SERVICES MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED. LENELS2 DOES NOT WARRANT THAT SOFTWARE, HARDWARE OR RELATED SERVICES WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY SOFTWARE, HARDWARE OR RELATED SERVICES AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED FROM EXTERNAL SOURCES. THE ABILITY OF SOFTWARE, HARDWARE AND RELATED SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH LENELS2 HAS NO CONTROL INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND RELATED OPERATING SYSTEM COMPATABILITY; OR PROPER INSTALLATION, CONFIGURATION AND MAINTENANCE OF AUTHORIZED HARDWARE AND OTHER SOFTWARE.

LENELS2 MAY MAKE CERTAIN BIOMETRIC CAPABILITIES (E.G., FINGERPRINT, VOICE PRINT, FACIAL RECOGNITION, ETC.), DATA RECORDING CAPABILITIES (E.G., VOICE RECORDING), AND/OR DATA/INFORMATION RECOGNITION AND TRANSLATION CAPABILITIES AVAILABLE IN PRODUCTS LENELS2 MANUFACTURES AND/OR RESELLS. LENELS2 DOES NOT CONTROL THE CONDITIONS AND METHODS OF USE OF PRODUCTS IT MANUFACTURES AND/OR RESELLS. THE END-USER AND/OR INSTALLER AND/OR RESELLER/DISTRIBUTOR ACT AS CONTROLLER OF THE DATA RESULTING FROM USE OF THESE PRODUCTS, INCLUDING ANY RESULTING PERSONALLY IDENTIFIABLE INFORMATION OR PRIVATE DATA, AND ARE SOLELY RESPONSIBLE TO ENSURE THAT ANY PARTICULAR INSTALLATION AND USE OF PRODUCTS COMPLY WITH ALL APPLICABLE PRIVACY AND OTHER LAWS, INCLUDING ANY REQUIREMENT TO OBTAIN CONSENT. THE CAPABILITY OR USE OF ANY PRODUCTS MANUFACTURED OR SOLD BY LENELS2 TO RECORD CONSENT SHALL NOT BE SUBSTITUTED FOR THE CONTROLLER'S OBLIGATION TO INDEPENDENTLY DETERMINE WHETHER CONSENT IS REQUIRED, NOR SHALL SUCH CAPABILITY OR USE SHIFT ANY OBLIGATION TO OBTAIN ANY REQUIRED CONSENT TO LENELS2.

For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/en/policy/product-warning or scan the following code: