Lenel Systems International, Inc.
1212 Pittsford-Victor Road
Pittsford, New York 14534
Tel 866.788.5095 Fax 585.248.9185
www.lenel.com

Release Notes for OnGuard® 7.0 and Service Pack Releases

Contents

1. Introduction

These Release Notes cover OnGuard 7.0 and any subsequent service pack releases.

For an overview of this document:

- Section 1 Introduction (this section) provides information on where to find installation instructions, OnGuard client purchases, OnGuard training, and the scope of this document.
- Section 2 OnGuard 7.0 SP1 Release Notes lists the versioning information, new features and updates, and known issues that apply to the OnGuard 7.0 SP1 release.
- Section 3 OnGuard 7.0 Release Notes lists the supported operating systems, upgrades, versioning information, new features and updates, and known issues that apply to the OnGuard 7.0 release.
- Section 4 Copyright and Trademark Notice provides copyright and trademark notices for Lenel and other third-party vendors.

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, refer to the Release Notes Addendum 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.)

OnGuard installation and supplemental DVDs 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 DVD for all of your client installations.

Lenel Global Education provides instructor-led, Web-based Global Distance Learning for more in depth knowledge on these new features in OnGuard 7.0. 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. OnGuard 7.0 SP1 Release Notes

2.1. Versioning Information

Note: This section lists the versioning information new to OnGuard 7.0 SP1. OnGuard 7.0 SP1 also supports versions for OnGuard 7.0 as listed in Section 3.3 Versioning Information on page 9.

2.1.1. Current CASI Firmware

- CASI DirecDoor: v2.4.6
- CASI M5, M2000, M3000: v3.4.6

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

- LNL-2210, LNL-2220, LNL-3300, LNL-3300-M5 ISC: v1.194
- LNL-1300 Series 2: v.1.52.13
- LNL-1320 Series 2: v.1.57.5
- LNL-1320-2RP, LNL-1320-S2RP: v1.57.3
- LNL-1380-8RP: v1.57.5

2.1.3. Current Digital Video Software

- Lenel Network Video Recorder (Lenel NVR): Software Version 7.1.731
- Intelligent Video Server (IVS): Software Version 7.1.731
- Intelligent Video Application Server (IVAS): Software Version 7.1.731
- Lenel Streaming Video Server (LSVS): Software Version 7.1.731

2.1.4. Current Security Series (NGP) Firmware

- NGP: v1.4.6 (applies to NGP-22xxx and NGP-33xxx panels)
- NGP-1300U: v12.08.02
- NGP-1320U: v12.08.02
- NGP-1100U: v12.08.02
- NGP-1200U: v12.08.02

2.1.5. Supported Operating Systems

OnGuard 7.0 SP1 has been approved with the listed operating systems and system service packs. **Operating system requirements are now enforced.** Installations attempted on other operating systems will not run.

2.1.5.1. Windows Server 2012 R2 SP1

- Windows Server 2012 R2 Service Pack 1 (SP1) 64-bit is approved for all OnGuard server and client operations.
- Windows Server 2012 R2 SP1 is approved for use as a Lenel NVR product host operating system.

2.1.6. 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.

- Microsoft SQL Server 2012 Service Pack 2 (SP2)
- Microsoft SQL Server 2008 R2 Service Pack 3 (SP3)

2.2. New Features and Updates

- **1000 access level support for CASI/OCF Panels (OG-30037):** OnGuard 7.0 SP1 supports 1000 access levels for CASI-OCF panels.
- **New security enhancements available for LNL-2210, LNL-2220, LNL-3300, and LNL-3300-M5 ISCs:** With firmware version 1.194, new security enhancements are available:
  - A deliberate action is now required to enable the default user account. Once the default user account is enabled, it is active for only a short period of time.
  - Login access is now disabled for one (1) minute after three (3) consecutive failed login attempts.
  - The session ID length has been increased to a 64-bit number and the generation is now using a FIPS approved Random Number Generator.

  For more information about the new security enhancements, refer to the Default Login Security Enhancements document (DOC-1087-EN-US).
- **Duress support on OCF Panels:** OnGuard SP1 supports duress on OCF panels.
- **In/out reader support for Lenel M-Series (MerCasi) 8RP:** OnGuard SP1 now supports using paired 8RP readers for single door ingress/egress operation.
- **Dual Interface Reader 2 option renamed:** On the Readers and Doors > General form, **Dual Interface Reader 2** was renamed to “Paired Reader”.
- **New language support:** Support for Arabic, Lithuanian, and Romanian is now available in OnGuard 7.0 SP1.

- **Bioscrypt (DESFire) Encoding supported:** Encode Bioscrypt fingerprints to DESFire EV1 smart cards that will be used with Bioscrypt 4G smart card readers and MorphoAccess SIGMA Series readers. Bioscrypt (DESFire) application encoding can be performed inline with badge printing using a DigiOn24 encoder integrated into the Zebra ZXP Series 7 or 8 printer. Standalone encoding of the Bioscrypt (DESFire) application can be done using the DigiOn24 encoder.
  - **New Bioscrypt (DESFire) smart card application:** The Bioscrypt (DESFire) application was added to the smart card applications allowing you to encode DESFire EV1 cards. The Bioscrypt (Sagem Morpho) Hardware Support (SWG-1402) license is required to use the Bioscrypt (DESFire) application.
  - **V-Smart card format applications renamed:** The V-Smart applications were renamed to Bioscrypt. The V-smart (MIFARE) application was renamed to "Bioscrypt (MIFARE)" and the V-Smart (iCLASS) application was renamed to "Bioscrypt (iCLASS)".
  - **Biometric reader support:** MorphoAccess SIGMA Series and Bioscrypt 4G V-Station and V-Flex readers are supported.
- **Import badge IDs based on DESFire and MIFARE card serial numbers:** Support has been added to Badge Types that allows you to import badge IDs using the Mapping Table based on DESFire or MIFARE card serial numbers. Specifically on the Badge ID Allocation > ID Import Source form, when you select MIFARE as the **Card Technology**, Mapping Table can now be configured as the **Data Source**. In addition, support for DESFire **Card Technology** was added with the option to configure Mapping Table as the **Data Source** as well.
- **EST3 OPC Server configuration file updated (OG-30083):** The **LNLEST3OPC.ini** file contains the following changes to its configuration parameters:
  - `[Server]: NumPanels=1`
  - `[CommSettings]: BaudRate1=9600; ComPort1=1`
  - `[PanelSettings]: FirmwareVersion1=1; Heartbeat1=30`
- **Middle Name field length:** When creating a cardholder in System Administration, the maximum length of the **Middle name** field is increased from 32 to 64 characters.
- **Language Support Available after Upgrading OnGuard 7.0:** Upgrading to OnGuard 7.0 SP1 automatically installs all released language packs. Existing customers of OnGuard 7.0 will not need to re-apply a language pack after installing the upgrade. New customers will not need to download or apply a language pack at all. All customers must have the appropriate license bit enabled for language support, and must configure their OnGuard systems to run with a language pack (for example, run the Database Translator utility). Web application support of translations is also available after upgrading to OnGuard 7.0 SP1. For more information, refer to the Language Pack Release Notes and Language Pack User Guide.

2.3. Known Issues

- **DataConduIT service stops when the MoveBadge method is executed after changing the default segment of an access panel to another custom segment (OG-29952):** This issue occurs when a time value is not specified with the MoveBadge method.

3. OnGuard 7.0 Release Notes

3.1. Supported Operating System Requirements Enforced

The installation or upgrade of OnGuard 7.0 will be blocked on any operating system version not specifically listed as supported in section 3.3.7, Supported Operating Systems.

To install OnGuard 7.0, upgrade to a supported operating system and service pack.

3.2. Upgrades

- **Upgrading to OnGuard 7.0 (OG-29586):** All current versions of OnGuard can be directly upgraded. For some older versions, an incremental upgrade must first be performed. For example, a system older than OnGuard 2008 (6.0) must first be upgraded to OnGuard 2008 Plus (6.1). OnGuard 2008 (6.0) and later can be directly upgraded.

  When upgrading Enterprise systems older than OnGuard 2008 (6.0), the system must be upgraded to OnGuard 2008 Plus (6.1) and a full download to each regional database must be performed prior to upgrading to the final version. For more information, refer to Knowledge Base Article 1345 (http://kb.lenel.com).

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

- **Upgrading from OnGuard versions earlier than OnGuard 2005 Second Edition (5.11.216) (OG-22273):** If upgrading a database from versions of OnGuard earlier than OnGuard 2005 Second Edition (5.11.216), the installation utility notifies you that it cannot perform the upgrade because the database is too old. To resolve this issue:

  1. Go to https://partner.lenel.com/downloads/onguard/software. (You will need your Lenel login to gain access to this site.)
  2. Scroll down to **Legacy Database Setup**.
  3. Click **5.11.216 Database Setup – Read Me** to read the Readme file.
  4. Click **5.11.216 Database Setup** to download the file.
  5. Unzip the 5.11.216 Database Setup file.
  6. Run the **StpDB.exe** file, and then run Database Setup again.

- **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 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
  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 Web Applications:** Customers migrating from Bosch ReadyKeyPRO to Lenel OnGuard who use web applications on the LS Platform Server must clear cached information in their browser in order to see the correct branding.

3.3. Versioning Information

3.3.1. Current CASI Firmware

- CASI DirecDoor: v2.4.2
- CASI M5, M2000, M3000: v3.4.2

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

Note: This note applies to the following boards: LNL-500, LNL-1000, LNL-2000, LNL-1100, LNL-1200, LNL-1300, 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: v1.192
- LNL-1100, LNL-1200 Series 1: v1.04
- LNL-1100, LNL-1200 Series 2, LNL-1100-20DI, LNL-1200-16DO, LNL-1200-DOR:v1.32
- 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: v1.52.12
- LNL-1320 Series 1: v1.13
- LNL-1320 Series 2: v1.57.1
- LNL-1320-2RP, LNL-1320-S2RP: v1.56.10
- LNL-1380-8RP: v1.56.7
- 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

3.3.3. Current Security Series (NGP) Firmware

- NGP: v1.4.2 (applies to NGP-22xxx and NGP-33xxx panels)
- NGP-1300U: v12.07.02
- NGP-1320U: v12.07.02
- NGP-1100U: v12.07.02
- NGP-1200U: v12.07.02

3.3.4. 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

3.3.5. Current Digital Video Software

- Lenel Digital Video Recorder (LDVR): Software Version 7.21 Hot Fix 2.0
- Lenel Network Video Recorder (Lenel NVR): Software Version 7.1.725
- Intelligent Video Server (IVS): Software Version 7.1.725
- Intelligent Video Application Server (IVAS): Software Version 7.1.725
- Lenel Streaming Video Server (LSVS): Software Version 7.1.725

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***.

3.3.6. Minimum System Hardware Requirements

- Pentium IV 1 GHz Processor
- 2 GB RAM
- DVD-ROM
- USB Port
- 1024x768 color display
- 6 GB of available space

3.3.7. Supported Operating Systems

OnGuard 7.0 has been approved with the listed operating systems and system service packs. **Operating system requirements are now enforced.** Installations attempted on other operating systems will not run.

3.3.7.1. Windows Server 2008 R2 with Service Pack 1

- Windows Server 2008 Standard and Enterprise R2 SP1 64-bit are approved for all OnGuard server and client operations.
- Windows Server 2008 Standard and Enterprise R2 SP1 are approved for use as a Lenel NVR product host operating system.
- Windows Server 2008 Standard and Enterprise R2 SP1 can be utilized as the separate OnGuard server with Lenel Digital Video products. ***Note:*** Windows Server 2008 is **not** approved for use as any Lenel Digital Video product host operating system when using OnGuard 2010 and prior.
- Windows Server 2008 Standard and Enterprise R2 SP1 will be called Windows Server 2008 R2, from this point forward, in the OnGuard 7.0 Release Notes.

3.3.7.2. Windows Server 2012

- Windows Server 2012 Standard 64-bit is approved for all OnGuard server and client operations.
- Windows Server 2012 Standard is approved for use as a Lenel NVR product host operating system.

3.3.7.3. Windows Server 2012 R2

- Windows Server 2012 R2 Standard 64-bit is approved for all OnGuard server and client operations.
- Windows Server 2012 R2 Standard is approved for use as a Lenel NVR product host operating system.

3.3.7.4. Windows 8/Windows 8.1

- Windows 8 and Windows 8.1 Enterprise and Professional 32-bit and 64-bit are approved for all OnGuard server and client operations.
- Windows Server 8 and Windows 8.1 Enterprise and Professional are approved for use as a Lenel NVR product host operating system.
- Windows 8 and Windows 8.1 are **not** recommended for use as the OnGuard Web Applications and Web Service server because of the limited number of client connections in these operating systems.

3.3.7.5. Windows 7 with Service Pack 1

- Windows 7 SP1 Enterprise, Professional, and Ultimate 32-bit and 64-bit are approved for all OnGuard server and client operations.
- Windows 7 SP1 Enterprise, Professional, and Ultimate are approved for use as a Lenel NVR product host operating system.
- Windows 7 is **not** recommended for use as the OnGuard Web Applications and Web Service server because of the limited number of client connections in this operating system.
- Windows 7 SP1 Enterprise, Professional, and Ultimate will be called Windows 7, from this point forward, in the OnGuard 7.0 Release Notes.

3.3.8. 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.)

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.

3.3.9. 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

3.3.10. 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.

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 2008 SP3, 32-bit and 64-bit
- Microsoft SQL Server 2008 R2 SP2, 32-bit and 64-bit
- Microsoft SQL Server 2012 SP1 (32-bit and 64-bit) and Express
- Microsoft SQL Server 2014 (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 2012 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 11g R1 Server 32-bit (11.1.0.6)
- Oracle 11g R1 Server 64-bit (11.1.0.7) with 32-bit Client installed if OnGuard is running on the same server as the database
- Oracle 11g R2 Server 32-bit (11.2.03 and 11.2.0.4)

- Oracle 11g R2 Server 64-bit (11.2.03 and 11.2.0.4) with 32-bit Client installed if OnGuard is running on the same server as the database
- 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 Web applications require 32-bit drivers to connect to an Oracle database.

3.3.11. Supported System Components

- ScanShell SDK version 10.03.19
- 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: If the Microsoft .NET 4.5 installation fails during the OnGuard installation on Windows Server 2008 R2, you must run the System Update Readiness Tool available from Microsoft: http://support.microsoft.com/kb/947821. To prevent this issue, verify that the Windows Update service is turned on.

Note: In order for web applications such as FrontDesk, Kiosk, or AdminAPP, to function, HTTP Activation must be enabled for the WCF Services on the server where web 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.

3.3.12. 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 and Windows Server 2008 R2
- IIS 8.0 is included with Windows Server 2012 and Windows 8/Windows 8.1
- IIS 8.5 is included with Windows Server 2012 R2

The following IIS requirements are the minimum 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

3.3.13. Virtual Platforms

- VMware ESX/ESXi Server 4.X and 5.X for all OnGuard services and database server with software-based license only
- VMware Workstation 9.0 and 10.0
- Microsoft Hyper-V 2008 R2 SP1 and 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).

3.3.14. Supported Third-party Components

- Crystal Reports version 2008 (12) and 2011 (14.0.x).

Note: OnGuard 7.0 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.

3.3.15. 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.
- **Trend Micro OfficeScan Corporate Edition version 8.0:** Trend Micro OfficeScan can be recommended, but is not tested and is installed at the user's risk.

3.3.16. Supported Web Browsers

- **Internet Explorer (required for web applications):**
  - Versions 9.0, 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 20.0 or later
- **Mozilla Firefox*:** Version 23.0 or later

* Supported OnGuard applications: License Administration

Note: To ensure that the Integrated Configuration Tool (ICT) works as expected, use Internet Explorer (IE) 9. If 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.

3.3.17. Supported Terminal Services

OnGuard 7.0 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.)

Citrix XenApp is not supported for viewing video.

3.3.18. OPC Versions

- OPC Data Access 2.0
- OPC Alarms and Events 1.0

3.3.19. SNMP Versions

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

3.3.20. 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.)

- NEC ExpressCluster X R3 32-bit LAN 3.1 (tested 3.1.5.1 and 3.1.0.1)
- NEC ExpressCluster X R3 32-bit WAN 3.1 (tested 3.1.5.1 and 3.1.0.1)
- NEC ExpressCluster X R3 64-bit LAN 3.1 (tested 3.1.5.1 and 3.1.0.1)
- NEC ExpressCluster X R3 64-bit WAN 3.1 (tested 3.1.5.1 and 3.1.0.1)

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-Based Failover Clustering
- Windows Server 2008 R2-Based Failover Clustering

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

As of Windows Server 2008, the MSCS (Microsoft Cluster Server) service was renamed to "Windows Server Failover Clustering”.

3.3.21. End of Life Products and Features

Refer to Section 3.2 Upgrades for the list of end of life products that need to be removed prior to upgrade.

3.4. New Features and Updates

3.4.1. General

- **Support for Notifier ID3000 in OnGuard 7.0:** OnGuard 7.0 supports the Notifier ID3000 Fire Panel. For more information, refer to DOC-1062-EN-US Notifier ID3000 Configuration in the Lenel Knowledge Base (http://kb.lenel.com).
- **IPv6 support for Access and Security Systems Panels:** OnGuard now supports IPv6 protocol for the following Access and Security Systems panels that currently use IPv4 protocol: NGP/CASI, LNL-3300, LNL-3300-M5, LNL-2220, and LNL-2210.
- **Fargo DTC4500:** OnGuard supports the Fargo DTC4500 ID Card Printer/Encoder. The DTC4500 replaces the DTC550.

  Note: Fargo DTC4500 encoders are not supported for encoding of any iCLASS applications from the OnGuard software.

- **New Configuration Editor:** The new Configuration Editor provides an improved user interface that makes it easy for the user to keep the database and License Server information in the **ACS.ini** file and **application.config** file synchronized.

  The new Configuration Editor can be launched manually, and is also a module in the Setup Assistant. If the Configuration Editor detects that the **ACS.ini** file and **application.config** file are not synchronized, it will flag the problem on its user interface and allow the user to select which configuration is correct.

  Note: The user must have write access to the registry, **ACS.ini** file, and the **application.config** file in order to save changes from the Configuration Editor.

- **Online Help Changes (OG70-DOC-00102):** Changes have been made to all of the online help files in OnGuard. Screenshots with pop-up user interface definitions have been removed, but all related content, including user interface definitions, is now available in a single topic when [F1] is pressed for the form that is currently open.
- **Warning message for NGP Central Station Setup Report (OG-24558):** A warning message now appears to prompt the user to re-create the NGP Central Station Setup report and provide an updated copy to the Central Station for the following cases:
  - Adding a new alarm panel
  - Deleting and alarm panel
  - Increasing the number of alarm inputs allocated to an alarm panel
  - Reducing the number of alarm inputs allocated to an alarm panel
  - Adding a door
  - Deleting a door

3.4.2. Alarm Monitoring

- **Alarm Options:** In ***Alarm Monitoring > Configure***, the Alarm Options feature allows OnGuard operators to set the maximum alarms range to a value between 1000 and 25000 (default value is 10000. If alarms are automatically cleared, half of the alarms are automatically deleted after the maximum alarms range is reached. Alarms with the lowest priority and oldest time are deleted first. If alarms are not automatically cleared, the operator receives a message after the maximum alarms range is reached.
- **Threshold exceeded alarm for event recording:** When a camera exceeds the pre-set limit for event recording, a new alarm, "Video Event Threshold Reached," is generated. The operator can right-click on this alarm to view the camera in question and select **Stop Event Recording** if necessary to conserve storage space.
- **Auto-iris/focus improvements:** Auto-iris and auto-focus can now be toggled on or off on the PTZ control in the Video Player.

3.4.3. Accessibility

- **Keyboard Hot Keys and Shortcuts (Section 508):** The OnGuard guides and help files now contain an appendix that lists all of the available hot key and keyboard shortcut key sequences available in each OnGuard application.

3.4.4. Access Control

- **Lenel M Series:** OnGuard 7.0 supports the new Lenel M Series, a user-configurable controller for use with the OnGuard access control and alarm management software platforms. For more detailed information, refer to the following articles in the Lenel Knowledge Base (http://kb.lenel.com):
  - DOC-1016-EN-US Intelligent System Controller LNL-3300-M5 Quick Reference
  - DOC-1017-EN-US Input Control Module LNL-1100-20DI Quick Reference
  - DOC-1018-EN-US Output Control Module LNL-1200-16DO Quick Reference
  - DOC-1019-EN-US Output Control Module LNL-1200-16DOR Quick Reference
  - DOC-1020-EN-US Dual Door Control Module LNL-1320-2RP Quick Reference
  - DOC-1021-EN-US Dual Door Control Module LNL-1320-S2RP Quick Reference
  - DOC-1022-EN-US Reader Interface Module LNL-1380-8RP Quick Reference
  - DOC-1027-EN-US RS-485 Interface Module LNL-8000-MCOM Quick Reference
  - DOC-1039-EN-US Intelligent System Controller LNL-3300-M5 Configuration
- **Bosch 9412GV4 and 7412GV4 to OnGuard (OG-26776):** The GV4 update for the D9412GV4 panels includes an increase to the number of areas (32) and panel users (999), while the support for both the D9412GV4 and the D7412GV4 includes additional changes necessary to account for the expanded functionality set offered by the GV4 protocol panels. GV4 firmware version 1.10 is supported. The control panel is not configured using OnGuard, but rather the Bosch software; therefore, it should be installed and configured according to the manufacturer documentation. For more detailed information, refer to the Lenel Knowledge Base (http://kb.lenel.com) article, Bosch GV4 Series Intrusion Control Panel Configuration, DOC-1102-EN-US or the Intrusion Detection Guide.
- **Bosch B Series Control Panels to OnGuard (OG-28967):** OnGuard 7.0 supports the Bosch B4512 and B5512 control panels with firmware version 2.1.4 or later.

- **Bosch D6600/D6600i Receiver/Gateway:** In OnGuard 7.0, Alarm Monitoring can now receive alarms from the Bosch D6600/D6600i Communications Receiver/Gateway.
- **ATS Control Panels:** ATS control panels are supported. These control panels can be used for integrated intrusion alarm and access control systems. For detailed information on supported models, refer to the Intrusion Detection User Guide.
- **Secure PIN entry is supported using OMNIKEY 3821 PIN Pad Reader:** Enter the PIN on the same PC/SC device that is used to read the card. This eliminates the need to send the PIN from the client workstation to the reader and improves security.
- **Mercury Access Timing Support (OG70-CR038):** Adding specific settings to the ACS.ini configuration file will now allow customers to control the following settings for the LNL "Access Series" Controllers. In each case, the described setting must be added to, or updated in, the [Service] section of the ACS.ini configuration file on the machine running that controller's Communication Server:
    - **EscortTimeout:** Time to wait after a card is presented that requires an escort. Each subsequent card presented restarts the timer until a card that is an escort is presented, or the timeout value is reached. Valid range is 1-60 seconds; default is 15 seconds (`EpEscortTimeout=15`).
    - **MultiCardTimeout:** Time to wait for subsequent cards to be presented when multi-cards are required. Valid range is 1-60 seconds, default is 15 seconds (`EpMultiCardTimeout=15`).
    - **AssetTimeout:** Time to wait after an asset is presented for a subsequent asset or authorized card to be presented. Valid range is 1-60 seconds; default is 10 seconds (`EpAssetTimeout=10`).
- **HID EDGE EVO Controllers:** HID EDGE EVO controllers are supported in EDGE framework. Configure the EH-400-K controller as "HID EdgePlus" and the EHR40 and EHRP40 controller/reader as panel type "HID EdgeReader."
- **Override Reader Mode Feature:** The new **Override Reader Mode** feature overrides the standard reader mode. While an Override Reader Mode is active, any changes to the standard reader mode are not applied to the reader. Commands that use the override expire after a configured amount of time or must be aborted before the standard reader mode will be restored. When the override is aborted or expires, the current state of the standard reader mode is restored.

  Available on LNL and Lenel M-series controllers and access panels.

  OnGuard commands that support the Override Reader Mode feature include All Reader Lock/Set Mode (Local I/O), Double Card Unlock/Toggle, Schlage Interior Pushbutton (IPB), and First Card Unlock.

- **All Reader Lock/Set Mode (Local I/O function):** Use the new **All Reader Lock/Set Mode** function to change the mode of all readers assigned to a controller to Locked for the configured amount of time when executed with TRUE. This function uses the Override Reader Mode feature which remains in effect for the configured amount of time unless the function is aborted. The override can be aborted by executing the function with a PULSE (which aborts the Override Reader Mode, returning all readers on the panel to their current standard mode prior to expiration) OR by a manual Reader Access Mode change made in Alarm Monitoring.

  Note: If the **All Reader Lock/Set Mode** function is used with authenticated readers, it will cause the readers to behave as if they are locked when the mode of the reader is changed to anything other than "Card only" or "Locked".

- **Double Card Unlock/Toggle:** Configuring the **Double card unlock/toggle** option enables the ability to toggle between a secured and unsecured mode when an authorized badge is presented twice, with the second time being within five seconds of the first.

- **OnGuard Supports Assa Abloy Aperio Locks:** The Aperio hub is connected to a controller (LNL-3300/LNL-2220/LNL-2210) which communicates with the Aperio wireless lock. The Aperio Hub 1-1 supports one wireless lock. The Aperio Hub 1-8 supports up to 8 wireless locks. (Reader Types include Aperio Hub 1-1 (Wiegand/Prox) or Aperio Hub 1-8 (Wiegand/Prox), depending on the hub you are using.

  The controller requires firmware version 1.188 or later to communicate with the hub and OnGuard 2013 SP1 or later.

- **First Card Unlock for Aperio:** An unsecured reader mode is supported by Aperio locks only when the special feature is enabled (**First Card Unlock** or Double Card Unlock/Toggle). For first card unlock, there must be a predetermined time and duration for this particular mode. During the configured time interval, the first card with a valid access grant causes the Aperio lock to enter into an unlocked state. The Aperio lock is then automatically relocked at the end of the configured time interval.

  Limitations:

  - Only the first time interval for a given timezone is used for controlling the relock time for the Aperio lock. Assigning additional timezones will not affect the relock time.
  - If this timezone is changed, the new time interval will not become effective until the next time the lock enters the unlocked state.
  - An Aperio lock may be removed from its unlocked state by changing the reader mode in Alarm Monitoring. Note that the relock will not occur immediately. It will occur at the next scheduled check in time (based on the status report interval that was configured) or when there is access activity at the lock.
  - If the Communication Server and/or panel communications go offline, then are brought back online, any updates made to the timezone/timezone reader mode will be in effect only after performing a download to the panel or reassigning the timezone reader mode to the Aperio lock.

  The Aperio scheduled relock will only work for the Start timezone assigned to the reader. If First Card Unlock is selected for the End timezone reader mode association, it will not unlock the reader immediately when an access grant occurs. In this case, the lock will unlock the next time the reader checks in with the hub.

- **OnGuard Supports New Configurations for Allegion (Schlage) AD-400/300 Locks:** OnGuard 2013 SP1 or later supports the following Schlage reader and lock solutions:
  - **Schlage PIM wired to LNL-3300:** You can connect up to 16 PIMs per downstream port with a maximum of 64 locks across the entire controller. Each PIM supports up to 16 AD-400 (PIM-485 based) wireless locks. For performance reasons, a maximum of 8 PIMs per downstream port is recommended.
  - **Schlage PIM wired to LNL-2210:** Connect one (1) PIM to the LNL-2210 with up to 16 AD-400 wireless locks attached. Install the PIM400-1501-LC and LNL-2210 as separate units or the PIM400-1501 a single unit (includes a built-in LNL-2210 in same enclosure).
  - **Schlage AD-300 wired to Lenel controller (LNL-3300/LNL-2210):** With this configuration, you can mix both AD-400 wireless locks and AD-300 hard-wired locks on the same downstream port. Up to eight (8) AD-300 locks are supported by the LNL-2210. Once you configure an AD-400 or AD-300 device on a given downstream port, other device types cannot be mixed on that port. You can only add more Schlage devices. For example, Lenel devices (such as the LNL-1320) and Schlage devices cannot share the same downstream port.

Note: When you configure a Schlage PIM that is connected to a Lenel controller port (LNL-3300/LNL-2210), the controller will communicate using the Schlage protocol on its communication port. This port will then only support Schlage devices and cannot be shared with standard Lenel downstream devices.
The LNL-2220 does not support the Schlage protocol as this controller only supports a single communication port which would sacrifice its capacity.

  - **Wiegand only support** is available with the Schlage PIM400-TD2 connection to the LNL-2220/LNL-1320/LNL-1300. Connects up to 2 locks (Door 1 & 2) to the access panel. (The Wiegand only integration provides basic lock support. It does not provide the advanced lock support of the previously describe OnGuard integration.)

Note: The new Schlage PIM devices do not require the use of an LNL-500W gateway device.

- **Remote Linking from Alarm Monitoring:** Allows you to initiate the link mode for a Schlage PIM-485 wireless lock from Alarm Monitoring.

- **Wake-Up on Radio (WoR):** Wake-up on Radio is automatically enabled when wiring a PIM to a Lenel controller. If you switch Wake Up on Radio OFF using the Handheld Device (HHD), this setting will be overridden to ON once the PIM begins communicating with the Lenel controller. When Wake-up on Radio is enabled, the lock will respond in less than 10 seconds to a command from the access control panel. When Wake-up on Radio is disabled, the lock will respond only during its heartbeat.

- **Mechanical Key Override Detection:** If the key is used to open the door from the outside, the “Door Open by Key” alarm is reported.

- **Deadbolt Detection:** If you have a Schlage lock with the deadbolt wired, it can perform the following functions:
  - When “throwing” the deadbolt, an “Internal Deadbolt” alarm will be generated.
  - When the deadbolt is removed, an “Internal Deadbolt Off” alarm will be reported.
  - When the deadbolt is “thrown” it changes the reader access mode to Locked. If you present a card to the reader, it will generate an “Access Denied: Reader Locked” alarm.
  - When you remove the deadbolt, the access mode that was in place prior to the deadbolt being thrown will be restored.
- **Low Battery Indicators:** When a low battery condition is detected for the PIM-485 based wireless lock, a “Low Battery” event is sent. The lock will still operate for several hundred operations, but the lock batteries should be replaced immediately to avoid failure. When a “Battery Failure” condition occurs, the lock will send the “Battery Critical” event. Almost immediately after that, OnGuard will receive a “Communication Lost” event and then the lock will assume the offline condition configured from the Handheld Device (HHD). OnGuard Offline Modes do not affect PIM-485 based wireless locks.
- **Multi-Dropped PIMs:** PIMs are configured with a unique RS-485 communication address within each downstream port. The “low door” and “high door” range for the PIM allocates the number of readers that will communicate with the PIM.
- **Interior Push Button Mode (IPB):** Pressing the Interior Push Button (IPB) on the inside housing of the lock may be used to communicate various IPB lock and unlock requests (Classroom, Privacy, Office, and Apartment). The manner in which the IPB communication is used by OnGuard is configured in System Administration. AD-400/300 IPB activity is reported to OnGuard when you press the interior push button.

  Lenel controllers override the following lock functions:

  - AD-400 (Schlage PIM-485) heartbeat
  - Relatch later (number of seconds, timer only, on door open or timer, on door close or timer)
  - Wake-up on Radio (WoR)

  Request-to-Enter and Serial Number Polling from the lock are not supported.

3.4.5. Archiving

- **Archive to database option:** The new **Archive to database** option allows the user to archive Events, Events Video Location, Alarm Acknowledgments, User Transactions, Visits Records, and specific event types to an Archival database rather than text files.

Notes: Once you enable database archiving, you cannot go back to text file archiving.

Once you choose a database name for the Archival database and enable database archiving, it is strongly recommended that you never change the Archival database name. Data migration will not be done from within the OnGuard software.

3.4.6. Card Formats

- **iCLASS Encoding changes to include Book 1 support (OG-26099):** Users can now define smart card formats to include iCLASS cards secured with HID or INSIDE keys to Book 1 of the smart cards. Specifically for the IrisAccess application, “Book 1 / 16kbits / 2 Application Areas” and “Book 1 / 16kbits / 16 Application Areas” options were added. For the Lenel iCLASS application, “16kbits / 2 Application Areas” and “16kbits / 16 Application Areas” options were added, which use the default HID keys.
- **Iris ID Encoding Enhancement:** Use the HID Programmer (Rev A and B) to encode the IrisAccess (iCLASS) application in either the GSC-IS or Lenel iris data format to iCLASS cards.

Note: iCAM encoders (iCAM4000/4000U/7000) do not support the Lenel iris data format.

3.4.7. Database

- **New OnGuard database password (OG-29645):** Due to new password restrictions made by Microsoft, the default OnGuard database password has changed from `MULTIMEDIA` to `Secur1ty#`. This change also affects the default SQL Express password established in the BAT install file, changing from `Expre$$` to `Secur1ty#`. This change applies to the actual OnGuard SQL Server Desktop Engine, SQL Server, or Oracle database.

Note: If using a default password, it is recommended that you change your password as soon as possible.

3.4.8. DataCondulT

- New method added to Lnl_IntrusionArea (OG-29003): A new method, `void Arm([in] sint32 armState);`has been added to **Lnl_IntrusionArea** with the following values:
  - 1 = PerimeterArm
  - 2 = EntirePartitionArm
  - 3 = MasterDelayArm
  - 4 = MasterInstantArm
  - 5 = PerimeterDelayArm
  - 6 = PerimeterInstantArm
  - 7 = PartialArm
  - 9 = AwayArm
  - 10 = AwayForcedArm
  - 11 = StayArm
  - 12 = StayForcedArm

  The following Lnl_IntrusionArea methods are still supported, but the corresponding new values above should be used instead:
  - MasterDelayArm: use Arm() method with value of 3
  - MasterInstantArm: use Arm() method with value of 4
  - PerimeterDelayArm: use Arm() method with value of 5
  - PerimeterInstantArm: use Arm() method with value of 6

3.4.9. Digital Video

- **Single License for Multi Profile Streams:** In OnGuard 7.0, a single camera, no matter how many video streams it uses, only utilizes a single license. In previous versions of OnGuard, if a single camera had multiple video streams by using multiple profiles or multiple lenses it utilized multiple OnGuard licenses.
- **Support for TruVision Recorders:** OnGuard 7.0 supports the following TruVision recorders: TVR 41, TVR 40, TVR 11C, TVR 11, TVN 50, TVN 20, TVN 21, TVR 42, TVR 11D, TVR 60, and TruVision Generic. For more information, refer to the Digital Video Products 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.)
- **Barco Video Wall Integration:** OnGuard integrates with Barco to support large-format video walls. This functionality enables users to display numerous high resolution, high frame rate video streams simultaneously using Barco software and hardware. For more information, refer to DOC-1086-EN-US Barco Video Wall Integration in the Lenel Knowledge Base (http://kb.lenel.com).

3.4.10. Enterprise

- **Enterprise improvements:** Enterprise has received many changes that improve performance, reliability, and security, including:
  - How User Defined Forms are distributed from the Master to the Regional servers
  - How credential data is replicated across the servers
  - A new Message Bus architecture that eliminates the need for credential scheduling

  As a result, Enterprise customers must review their existing actions, logging, and schedules. Furthermore, the new LS Site Publication Server service must be managed.

  Notes: Hardware transactions, Log tables, and Last Location information are still replicated using the Replicator application, service, and scheduler.

  For more information, refer to the *Overview* chapter in the *Enterprise Setup & Configuration User Guide*.

- Prior to OnGuard 7.0, replication of incremental credential data was handled by the Replicator service. In OnGuard 7.0, incremental credential data is replicated by the Site Publication Server service.

  The Site Publication Server service uses a new Message Bus architecture that provides data queuing, guaranteed delivery, and SSL, resulting in improved performance, reliability, and security when transferring incremental credential data.

  For more information, refer to *What's New in OnGuard Enterprise 7.x* in the *Enterprise Setup & Configuration User Guide*. Also review the scheduled actions for Replicator.

3.4.11. Identity Management

- **Removal of View/Edit Only version of ID CredentialCenter:** The View/Edit Only version of ID CredentialCenter Workstation is removed from OnGuard 7.0. The ID CredentialCenter (View-Only) Workstation is still a licensable option, providing view-only access to the Cardholders, Visits, and Assets folders.
- **Lenel Installer for CSSN SDK 10.03.19 Supports ScanShell and SnapShell in System Administration and Visitor Management Front Desk**

  The SDK is backwards compatible for CSS-1000/1000-A/1000-B.

  - **System Administration:** Supports the new SnapShell R2 and Passport camera scanners and the ScanShell 800R/1000B scanners, allowing you to import information from a driver's license, barcode, business card, or passport.

    The SDK driver is automatically installed during the installation of OnGuard.
  - **Visitor Management Front Desk (IDVM):** Supports the ScanShell 800R/1000B allowing you to import information from a driver's license, barcode, business card, or passport. Before connecting the scanners, run the CSSN SDK provided on the Supplemental Material disc.

  For more information, refer to the *OEM Device Configuration Guide* and the *Visitor Management Front Desk User Guide*.
- **NIST SP 800-116 Support:**
  - **Integration with HID's pivCLASS government solution:** This integration enables you to establish NIST SP 800-116 compliance and access the Federal Bridge to validate FIPS 201 credentials during credential registration, on a recurring basis, and at the door.
  - Lenel and NGP panels support authorization based on the extended government identifiers, full FASC-N (200-bit) and full GUID (128-bit).
  - Multiple FIPS 201-based card types are supported including PIV, TWIC, CAC (v1, v2, Transitional, and Endpoint), and PIV-I/CIV (PIV-C).
- **Existing support for PIV/TWIC Import Source Continues as FIPS 201-Based Credential:** Importing the contents of PIV and TWIC applets from their FIPS 201 credentials continues to be supported. However, the PIV Card and TWIC Card import sources are now combined into the new import source "FIPS 201 Based-Credential" based on the OnGuard license settings.
- **Extended ID Field/Page Permission Added:** A field permission have been added for the new Cardholders Badge Extended ID UDF field. This field is intended to store the full FASC-N or GUID information imported from PIV-based cards.
- **Badges with Invalid Extended ID Events Reported:** Badges with invalid extended IDs will be reported via the Main Alarm Monitor window. If the extended ID UDF has been configured in the system, the Extended ID column will display the extended ID of the invalid badge.

- **Configure Maximum Extended ID Length for Downloading to Panel:** On the *System Options* > *Hardware Settings* form, configure the **Maximum extended id length** in order to download credential identifier to the panel. When segmentation is enabled, these options are available in the Segments folder on the Hardware Settings sub-tab of the Segments form.

  OnGuard supports using a 16-byte, 128-bit GUID or 25-byte, 200-bit FASC-N as the extended ID to validate PIV-based cards. In addition, identifiers are supported that are longer than the badge ID (64 bits long).

  The extended ID will be downloaded to the panel for new and modified badges if the value in this field is greater than zero.

  Note: Setting the **Maximum credential identifier length** requires that you use the system UDF, Extended ID, map it to the full GUID or full FASC-N, and configure the Wiegand card format with the extended ID.

- **New Cardholders Authorized Credential Form:** The Authorized Credential form has been added to the Cardholders allowing you to search and display data imported from PIV-based cards.

  This form is only available if the user has permission to view badges and any of the following conditions also apply:

  – A caching status proxy is enabled.
  – Certificate validation is enabled.
  – The FIPS 201 SDK license configured on the local workstation.

  In the System Administration and ID CredentialCenter applications, the Authorized Credential form is used to search for non-enrolled badges based on the Credential type and enrollment status of the badge. The **Credential type** is imported during the “FIPS 201-Based credential” import. However, if required, you can configure **Credential type** manually by selecting it from the available options: CAC, CAC EP, PIV, PIV-I/CIV, and TWIC.

- **Configure pivCLASS, PAM-Connected Readers as Authenticated Readers:** Select the new **Authenticated reader** check box to indicate a reader that is capable of authenticating FIPS 201-based credentials. Available on the Readers and Doors General form for readers assigned to Lenel access panels that support this feature. Available on the Readers and Doors In Reader/Out Readers forms for readers assigned to NGP access panels that support this feature.

  The **Authenticated reader** option is associated with the **Online (Reader Modes)** or **During schedule** reader modes which are populated with reader authentication modes. (The **Schedule** and **Outside schedule** reader modes do not support NGP authenticated readers.)

  Reader authentication modes dictate the mechanism used by an authenticated reader to validate FIPS 201-based cards. The reader authentication modes are downloaded via the *FIPS 201 Credentials folder* > *Authentication Modes* form. Readers with timezone-reader mode assignments cannot be configured as authenticated readers. Timezone/reader modes do not support authenticated readers.

  Note: The local I/O function **Reader Unlock/Set Mode** does not support authenticated readers.

- **Extended ID Added to Wiegand Card Configuration:** Configuring the extended ID in the Wiegand card format allows the panel to authenticate based on the extended ID.

  New fields added to the Wiegand card format for this purpose include:

  - Configure the **Starting Bit** (for Extended ID) by choosing a starting value from 0 to 255.

    Note: Card number and Extended ID cannot be specified at the same time. Extended ID is a unique field that supports credential identifier values longer than the badge ID (64 bits). Typically, when Extended ID is configured, it will be the only field defined for the card; card number, facility code, ADA, activate date, deactivate date, and authorization will not be configured. Fields which are not used are indicated by a starting bit set to "0" and number of bits set to "0."
  - Configure the **Number of Bits** (for Extended ID) by choosing a value from 0 to 256 bits.
- **Fingerprint Options Moved:**
  - Import fingerprints from card into database moved from Cardholder Options to FIPS 201 Credentials > General import settings.
  - Verify fingerprints on import moved from General Cardholder Options to the FIPS 201 Credentials > Credential Validation fingerprint verification settings and was renamed Fingerprint verification method.

  For more information, refer to the *ID CredentialCenter User Guide*.

3.4.12. Installation

- **Remote installation of OnGuard enhanced with Manual Unattended Client Deployment (OG-24632, OG-26679):** With this release, remote installation of OnGuard has been enhanced with the Manual Unattended Client Deployment. This deployment method makes use of a compressed OnGuard client installation package for custom unattended deployment initiatives. Specific user-defined parameters are passed to a special package provided within the source media. The Administrative Installation Mode (`setup /a`) has been removed. For more information, refer to the Advanced Installation Topics Guide.
- **New installation procedure Microsoft SQL Server 2012 (OG-27128):** The OnGuard Installation Guide contains a new installation procedure for installing OnGuard 7.0 with Microsoft SQL Sever 2012. SQL Server 2012 installs differently than SQL Server 2008.
- **SQL Server Express (OG-27736, OG-28202):** With earlier versions of OnGuard, SQL Server Express could be installed automatically. Users wanting SQL Server Express must install it manually from the Supplemental Materials disc before installing OnGuard. For more information, refer to the Installation Guide or Upgrade Guide.

  Note: SQL Server Express should be installed before installing the security management system software.
- **Idle Time-out for the OnGuard application pool in IIS has been disabled (OG-28823):** On an initial installation or upgrade of the OnGuard software, the Idle Time-out for the application pool that is configured for the OnGuard web applications has been set to zero (0). Prior to this change, authentication tokens used by wAAM clients (and cached by the web service) expired after 20 minutes of web service inactivity.

3.4.13. Licensing

- **Single License for Multi Profile Streams (OG-26934):** Currently, if a single camera has multiple video streams by using multiple profiles or multiple lenses, the camera utilizes multiple licenses of the OnGuard software. In OnGuard 7.0, a single camera only utilizes a single license no matter how many video streams it uses.

3.4.14. NGP

- **NGP Global I/O enhancements:** The following enhancements to NGP Global I/O are available in OnGuard 7.0:
    - Area state support
    - Arming state events and local areas now available in the configuration of the global I/O input event
- **Elevator control enhancements:** OnGuard-controlled elevators support is now available on NGP controllers:
    - **Supported hardware (Security Series):**
        - **Elevator Reader:** Single Door NGP-1300-U controllers only
        - **Elevator Inputs:** NGP-1100-U and NGP-1100 legacy modules
        - **Floor Tracking:** NGP-1200-U and NGP-1208 legacy modules
    - **Supported hardware (NGP-CASI):**
        - **Elevator Reader:** 2RP, 2SRP, 8RP reader interface modules
        - **Elevator Inputs:** 20DI modules
        - **Floor Tracking:** 16DO modules
    - Provides the same level of support as implemented with the Lenel Access Series platform (128 floors, Day Mode, Elevator Control Level)
    - Controller configuration extensions (configures the NGP Security Series/NGP-CASI controller to support elevator control)
    - Reader configuration extensions:
        - Enable elevator support
        - Change the behavior of the reader module to support elevator control and elevator hardware
        - Optional track floors (requires configuration of the required number of outputs to equal the number of elevator inputs)
        - I/O assignments in full banks of 16 floors
- **NGP Alarm Latching:** When an NGP user logs onto the NGP LCD keypad, the keypad provides information about alarms that occurred in the armed area prior to the user logging on. The alarm is maintained in Alarm Monitoring until it is acknowledged locally from the appropriate keypad.
- **User-definable area IDs:** The reporting area number sent to the central station can now be configured in OnGuard:
    - Range is 0 – 999; 0 is undefined
    - To ensure correct reporting to the central station, do not use duplicated reporting area numbers for the same account number
- **Central station proxy configuration:** The proxy address and port number, user name, and password for the central station can now be configured in OnGuard.

- **Improved Integration Configuration Tool (ICT):** The following enhancements have been made to the NGP ICT:
  - New design based on CASI ICT
  - Power tab configuration simplified to only the required settings
  - Flash download of firmware replaces FirmwareDownloadOnlyMode as the method for forcing a new firmware download
  - Remote logging and diagnostics capabilities
- **OnGuard provides status updates on NGP firmware downloads in Alarm Monitoring:** OnGuard now provides status updates (success or failure reports) in Alarm Monitoring for NGP firmware downloads.
- **Improved central timing subsystem:** The central timing subsystem in NGP has been updated to respond within 100 mS of timed activities.
- **Updates made to Power and Battery page in NGP ICT:** The Power and Battery page now only shows fields that are supported by NGP.
- **Universal I/O counting:** NGP can now count inputs/outputs in quantities less than four (4) based on what is available on the board or as configured in OnGuard.

3.4.15. Supplemental Materials Disc

- **SQL Server Management Tools no longer included on Supplemental Materials Disc (OG-28988):** 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 2012 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.

3.4.16. System Administration

- **Hypertext links in alarm instructions:** In ***System Administration > Monitoring > Alarms > Text***, OnGuard operators can enter a hypertext link, by typing or pasting, into the Text Form as part of the alarm response message.
- **Close Unattended Player After Timeout:** In ***System Administration > Video > Digital Video > Alarm-Video Configuration***, a new alarm configuration option, **Close Unattended Player After Timeout**, is available. This option specifies how long (in seconds) a video window that was launched in response to an event remains open before it automatically closes.
- **GOV Length support for MPEG4 and H.264 cameras:** In ***System Administration > Video > Digital Video > Camera***, time lapse settings now offer compatible values calculated based on the chosen GOV length for the selected camera.
- **Configure video retention times on a per-camera basis:** In ***System Administration > Video > Digital Video > Video Recorder***, a new feature, **Automatically delete video older than**, is available on the **Capacity** tab. OnGuard operators can limit the number of days that video is stored for the selected camera. Locked and unlocked video older than the specified number of days (that has not been archived) is automatically deleted.
- **Home PTZ Preset:** In ***System Administration > Video > Digital Video > Camera***, a new feature, **Home PTZ Preset**, is available on the **PTZ** tab. OnGuard operators can assign a previously created PTZ preset to be the home or default position for the selected camera.

3.5. Known Issues

3.5.1. 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, Windows 8, Windows 8.1, Windows Server 2008 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.

- **Temporary Files Remain After Installation Has Completed (OG-14475):** Some components needed by OnGuard might leave temporary files on the system root drive after the installation. More information can be found here: http://support.microsoft.com/kb/950683.

- **FormsDesigner Field Style Border and Inside Edge not Functioning Properly (OG-15759):** In order to support recently introduced changes to the user interface, the ability to turn off a sunken edge border for a control in FormsDesigner has been disabled.

- **OnGuard Installation no longer distributes the Sentinel Driver (OG-23538):** The OnGuard installation no longer distributes the Sentinel driver (for USB dongles) during the installation of the License Server feature on a server installation. Refer to the Supplemental Materials disc for the driver, if needed.

- **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.)

- **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 need to 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 7.0:** When upgrading to OnGuard 7.0, all full download and incremental download actions are deleted from Scheduler. These Replicator actions cannot be recreated in OnGuard 7.0 because they are no longer necessary. For more information, refer to *Run Replication as a Windows Service* in the *Replicator User Guide*.

3.5.2. Access Control

- **Integrated Intrusion LCD Display of Event History Adds Spurious Event for Alarms with Door Set for Entry Delay (OG-15920):** When utilizing the new Intrusion Mask Groups, an alarm caused by a Door Status event set for "Trigger" point mode will result in an extra event being displayed in the LCD keypad event history. The extra event will be labeled "256 TYPE ERROR" and have the same time as the door event, and can be ignored. This issue will be addressed in a future firmware version.
- **OSDP Reader Might Have Incorrect LED Display (OG-17529):** If power is lost to an Open Supervised Device Protocol (OSDP) reader, but power to the Lenel reader interface is maintained, the LED display pattern might be incorrect until an access activity takes place.
- **Strike Field States Cutoff on Close (OG-18019):** For HID Edge devices, the **Strike** field states Cutoff on close. The actual reader strike output will cutoff on open in all cases.
- **Area Access Manager (Browser-based Client) Reports Not Supported with Windows Authentication on Windows Server 2008 R2 (OG-18066):** Reports will not run properly from Area Access Manager (Browser-based Client) with Windows Authentication on Windows Server 2008 R2. For these operating systems, only SQL authentication is supported with browser-based reports.
- **Area Access Manager (Browser-based Client) Returns a Server Error for a Cardholder if a Field is Added to the Cardholder Form (OG-19281) (OG-20123):** Area Access Manager (Browser-based Client) will return the following server error for a cardholder if a field is added to the Cardholder form:

  ```
  “A server error has occurred. Please see your system administrator.”
  ```

  When a form is updated, IIS must be restarted along with the LS Application Server. If you receive this error, restart IIS and the LS Application Server.
- **Deleting Badges from Onity Integra Locks (OG-23265):** When badges are deleted from ILS Integra locks, at least one (1) badge must always remain on the lock. Attempting to delete all badges from a lock will not succeed, and the lock will retain the same access privileges it had before the attempt was made. If you want to prohibit all access to a lock, use some other mechanism, such as blocking or changing schedules.
- Guardall Px device translator filters out the Set/Unset alarms from being reported to OnGuard (OG-25249).

3.5.3. Alarm Monitoring

- **Alarm Monitoring stops responding when camera resolution is changed during live video (OG-29531):** If the resolution for a camera is changed after the Video Monitoring window is opened, Alarm Monitoring stops responding. To change the resolution, close the Video Monitoring window, change the camera resolution in System Administration, and then reopen the Video Monitoring window in Alarm Monitoring.

3.5.4. Digital Video

- **Joystick Control Difficult Due to Delays in Video (OG-15077):** PTZ might appear slow due to buffering that is included to allow better image quality. For customers that require better PTZ performance, a workaround exists that includes setting audio to off. The workaround is to update the registry [HKEY_CURRENT_USER\Software\Lenel\Lnr]"LiveVideoBuffer" -> DWORD. This value, when set to 0, will speed up the live viewing for both MJPEG and MPEG4 cameras but introduces audio issues.

  Note: Modifying the registry could cause irreversible damage to your Windows operating system. Back up the registry before making any changes. Follow the instructions located at: http://support.microsoft.com/kb/322756.

- **PAL Cameras might not have Frame Rates Color-coded to Indicate Supported Frame Rates (OG-15468):** Regions using PAL and incorporating the following list of cameras might not have the frame rate displayed in green/red to indicate supported frame rates:
  - Axis MPEG4 (only): 213 PTZ
  - Axis MJPEG (only): 240Q
  - Axis MJPEG and MPEG4: 214 PTZ, 215 PTZ, 241Q, 241QA, 241S, 241SA, 243Q , 243SA, 247S
  - Axis 231D MJPEG and MPEG4 (Both PAL and NTSC)
  - Axis 232D MJPEG and MPEG4 (Both PAL and NTSC)
  - Axis 233D MJPEG and MPEG4 (Both PAL and NTSC)
  - Axis Q7401 MJPEG and H264 (PAL)
  - Axis Q7406 MJPEG and H264 (PAL)
  - Bosch All Cameras (Both PAL and NTSC)
  - HikVision All Cameras (Both PAL and NTSC)
  - Lenel: All cameras
  - Panasonic MJPEG (only): WV-NW474
  - Panasonic WV-NF284 MPEG4
  - Panasonic WV-NF302 MPEG4
  - Panasonic WV-NP244 MPEG4
  - Panasonic WV-NP304 MPEG4
  - Panasonic WV-NS954 MPEG4
  - Panasonic WV-NW484S MPEG4
  - Panasonic WV-NS964 MPEG4
  - Sony MJPEG (only): RZ-30, CS3
  - Sony MJPEG and MPEG4: DF-40, DF-70, P5, RZ-25, Z20
  - Sony MJPEG, MPEG4, H264: CS50, DF-50, DF-80, RX-550, RZ-50
  - All Sony SNC-xxxxP PAL Cameras

- **Double Video on Alarm with LDVR (OG-15506):** For customers using LDVR (non-hybrid systems only), the `PauseOnDoubleVideoOnAlarm` setting in the **ACS.INI** file must be set to 0 on all client computers. Channel pre-roll values must be set to 15 seconds or more. This is required in order to avoid black screen issues and video not available error messages when recorded video is played back as part of the double video on alarm feature. The amount of pre-roll required depends on the video resolution and bitrate that is used. The larger the size and frequency of the frames, the smaller pre-roll time can be configured.
- **Double Video with Time-lapse Limitation (OG-15507):** When using the Double Video on Alarm feature, the time lapse setting must have the same value as the AlarmDurationMax value, otherwise there might be black video.
- **Streaming Video Server Not Supported with H.264 Video Source (OG-16019):** The H.264 camera codec is not supported with the BARCO/Streaming Video Server integration.
- **IntelligentVideo Events Allow Region of Interest that Extends Past the Image Boundaries (OG-16056):** The user interface allows a region of interest to be configured that extends outside of the image area with the Object Crosses a Region and People Counting events. This configuration is not supported and might cause the event to not function properly.
- **Frame Rates Higher than 50 FPS Might Not be Accurate (OG-16061):** Setting the frame rate to above 50 FPS on cameras that support high frame rates might result in a slightly different FPS value. For example, if the frame rate is set to 50 FPS, you might experience a frame rate of 52 FPS.
- **Lenel NVR Motion Detection Not Supported with IQinVision Cameras (OG-16501):** IQinVision cameras should not be configured with Lenel NVR motion detection. This configuration is not supported and might cause the system to become unresponsive. To work around this issue, utilize the camera motion detection functionality and configure the camera to send motion alarms to the OnGuard system.
- **Audio Limitations:**
  - Live video from the AXIS 210A MPEG4 with audio enabled appears to be in time-lapse mode (OG-16665)
  - There is a two second or greater delay in recording audio in MPEG4 (OG-16666)
  - Cannot export video from MPEG4 cameras with audio to ASF format (OG-16919)
- **Panasonic Camera Model Numbers in the Device Discovery Console (OG-17442):** Some Panasonic cameras are displayed by their series number rather than their model number in the Device Discovery Console. These cameras will not display their camera model numbers, but instead they display the series of the camera. For example, the Panasonic NS954 is part of the WV-NS950 series and would be displayed as a Panasonic NS950. For a list of Panasonic camera display names, refer to the Device Discovery Console User Guide.
- **Error When Switching to Live Video after Viewing Recorded from Archive Server (OG-17598):** When video is opened using the **Launch recorded video from** > **Archive Server** right-click menu item in Alarm Monitoring, the communication path becomes locked to the Archive Server and the player cannot be switched to live video. If you want to view live video, close the Video Player and launch live video.

- **Axis Cameras with H.264 Compression Do Not Support Square Pixel Compensation (OG-17659):** Square pixel compensation is not supported by Axis cameras with H.264 compression. When using square pixel compensation, the camera still transmits, for example, 352x240 if the camera is set to 320x240. The resolution is corrected in the viewer, thus providing no visual, storage, or bandwidth benefits.
- **Windows Server 2008 R2: Enabling Video Export (OG-17701):** To allow Windows Server 2008 R2 to export video, complete the following steps:
  1. Right-click My Computer and select **Manage**.
  2. Click on **Features** in the navigation tree.
  3. Click the **Add Features** link.
  4. Select the **Desktop Experience** check box and click [Install].

  Note: This installation requires a reboot. After Desktop Experience has been installed, export to ASF will work successfully.
- **False Motion Detection Alarms from Lenel ICT230 Located in a Dark Room (OG-17771):** There is a known issue with the Lenel ICT230 cameras (firmware version 3.0) generating false motion detection alarms when they are located in a dark room.
- **Gaps in Recorded Video when Saving Embedded Event Configuration to Camera (OG-17880):** Saving embedded analytics configuration changes to an LCi-100-dx camera might result in several seconds of unrecorded video for the channel. In rare instances this might result briefly in a Communication Lost alarm for the camera channel.
- **PTZ Tour Server Does Not Run on Channel in Failover (OG-17970):** The PTZ Tour Server does not work when a channel is in failover mode. The PTZ Tour Server can be configured while in failover mode, but will not run until the primary video recorder has been restored.
- **Video Artifacts with RTP over UDP with Some Bitrate/Resolution Combinations (OG-18053):** When using cameras with RTP over UDP, artifacts might occur in the final image. This is due to the fact that UDP is a transmission without acknowledgement protocol and could have loss of packets during transmission in busy networks. This becomes more obvious when the video is bigger (for example, in the case of transmission of larger bitrates and resolutions). RTP over TCP/IP or RTP over RTSP over HTTP might be a better option with cameras that support them because they are more reliable and do not present this issue.
- **Lenel NVR Issues with Axis Video Servers with No Feeds Connected (OG-19329):** Axis analog video servers configured on a Lenel NVR that do not have any video signals plugged into them might cause the Lenel NVR to leak memory and eventually stop responding. This issue can be avoided either by not adding the unconnected channels to OnGuard or by marking them logically offline.
- **Remote Monitor and Alarm Monitoring Might Become De-synchronized (OG-19830):** Remote Monitor and Alarm Monitoring might become de-synchronized after Alarm Monitoring is restarted. For example, Video Quality Enhancement (VQE) settings made for the Remote Monitor channel are no longer selected in the user interface after restarting Alarm Monitoring.

- **Import XML does not allow modification of inputs on Sony V704 (OG-20542):** When exporting XML from a Lenel NVR with the Sony V704 camera (all four inputs) and then importing into another Lenel NVR, the user cannot change the input number for the V704 camera. The workaround is to manually modify the channels to have the correct input number.
- **Cannot import HIK analog channels from an XML to an Lenel NVR (OG-20543):** Exporting XML from a Lenel NVR, which already has HikVision analog channels, and then importing the file into another Lenel NVR, selecting an analog channel, and clicking the add button, produces an error stating that the channel is missing or has an invalid IP address. The workaround is to type 127.0.0.1 and then click Add. The tool will then allow the channel to be added.
- **Remote Monitor Client and Server do not support Unicode (OG-20866):** The Remote Monitor Client and Server do not support Unicode. This might cause a username or password in a non-ASCII character set to not work in some cases.
- **Status bar does not show “Offline” if a camera is marked offline (OG-21062):** When a camera is manually marked offline, Alarm Monitoring and Video Viewer will not display a red footer with a “Communication Lost” message at the bottom of the video cell for the offline camera when the video stream is interrupted.
- **When live video buffering is enabled, “Communication Lost” message does not appear in the live video window (OG-21072):** When buffered video is enabled ("bufreader0=1" in **ACS.INI** file), Alarm Monitoring and Video Viewer will not display a red footer with a "Communication Lost" message at the bottom of a video cell when the video stream is interrupted.
- **Changing resolution of a camera while video search window is open causes LpsSearchSvc.exe to close unexpectedly on client (OG-21079):** The LpsSearchSvc Windows service might close unexpectedly if the camera resolution is changed while a camera is opened in the Video Search dialog (for configuring IntelligentVideo or Lenel NVR-based video analytics).
- **Selecting “Update Capabilities” on an SP408 hybrid channel produces a “Class not registered” error (OG-21204):** Configuring a Lenel NVR with SP408 hybrid channels, and then adding one of the channels, selecting the hybrid channel, and clicking [Update Capabilities], produces an error message of “...Class not registered.” If the user clicks [OK], it correctly says “No” in the Embedded column.
- **Performance Counters for Lenel NVR not showing up on 64-bit Lenel NVRs (OG-21565):** When running the Lenel NVR on 64-bit systems, perfmon needs to be running in simulation mode. The user must open an Explorer window and open the folder "C:\Windows\SysWOW64" and then run perfmon from that location, or run "mmc.exe /32 perfmon.msc".
- **“End Video Tour” not disabled after selecting “Remove Video” for single camera, anonymous tour (OG-22258):** This occurs after opening Video Monitoring (Live Video) in Alarm Monitoring, starting an existing Video Tour, and selecting a camera in an existing Camera Device Group. The tour does not display after selecting Video Tour, and when right-clicking on Video Tour, the End Video Tour menu option is still enabled. When selecting Remove Video after right-clicking on Camera Video, the tour does not redisplay.

- **Darkness in Alarm Monitoring When Using Arecont Vision AV5110 Camera (OG-22486):** When using the Arecont Vision AV5110 camera, Alarm Monitoring shows darkness if [Modify/OK] is clicked. During any modification or even no modification, the low light condition of the camera is set to "Balanced" which causes the sensor to reset the light conditions and cause the darkness. This is expected camera behavior.
- **Future versions of the Streaming Video Server will not support LDVR video (OG-22595):** With the release of Lenel NVR 7.0, the streaming server is now an embedded part of the LNV Suite. Those using LDVR must use the streaming server that was released and approved for their LDVR version.
- **SkyPoint: NetEVS delays (OG-22626):** The first connection to NetEVS will take up to 20 to 40 seconds. Streaming video, viewing recorded video, and getting a recipient list will result in this delay the first time one of these functions is performed. The next time any of these functions is performed, the response time should improve. If none of these functions are performed for 15 minutes, the delay will be observed again the next time one of the functions is performed. The same initial delay will also be observed for these functions when using a NetDVMS that is configured with an Auxiliary Server (SkyPoint Base). These delays will not be observed when using a NetDVMS that is not configured with an Auxiliary Server.
- **Performance Monitor in Lenel NVR Shows the Incorrect Live Frame Rate for IQinVision H.264 Cameras (OG-22699):** Using Performance Monitor in Lenel NVR to view live frame rate for the IQinVision cameras will show a frame rate that is more than the configured frame rate.
- **goVision video recorder cannot be discovered in Device Discovery Console (OG-22956):** goVision does not show up in the scanned list. WinPcap (from the Supplemental Materials disc) must be installed to correct this issue.
- **Remote Monitor does not handle an IP change when using a hostname (OG-22986):** In order to resolve this, the Communication Server must be restarted.
- **NAS Compatibility (OG-23272):** Network Attached Storage (NAS) devices are supported by Lenel NVR. Not all devices work the same. As with any storage device responsible for recording continuous streams of data, the continuous uninterrupted read/write rates for the unit must be in line with the expected incoming/outgoing data streams.
- **Buffering Streaming Video is Disabled by Default (OG-23275):** The Buffering Streaming Video feature is now disabled by default and will also be disabled after an upgrade. For more information about buffering, refer to the Video Monitoring chapter of the Digital Video Software User Guide.
- **Buffering Streaming Video with Audio Causes Lag in Timestamp (OG-23276):** When the Buffering Streaming Video feature is activated and the video stream contains audio, the timestamp that is presented by default lags by a few seconds and the lag increases gradually. This has no effect with the video presented which is in the current live time. A workaround is to click the arrow to get to the latest minute of the buffering.
- **Auxiliary Tab is missing for RC-C Recorder (NetDVMS) from Video Recorder Tab of System Administration (OG-23607):** This tab was intentionally removed. The user no longer needs to explicitly associate an auxiliary server with a video recorder in order to exercise the "Send Video To..." functionality for SkyPoint integration. This is now handled automatically.

- **VideoViewer (Browser-based Client) Cab file gets 'DVRCapsLib.dll' errors when installing (OG-23693):** Clients installing the Lenel Video Player browser loaded .cab installation from VideoViewer (Browser-based Client) must first have Microsoft .NET 4.5 Framework installed or they will receive errors during installation. This is not during the OnGuard installation but the Lenel Video Player that installs through the browser on a "thin" (no OnGuard installed) client accessing video in the VideoViewer (Browser-based Client).
- **PTZ Zoom with mouse wheel is non-responsive and/or slow (OG-23694):** When using PTZ mode in Alarm Monitoring with an Axis P5532-E PTZ camera, use the buttons on the toolbar to zoom rather than the mouse wheel. When attempting to zoom using the mouse wheel, the system might be unresponsive or zoom very little.
- **Live Video Being Viewed During a VMotion Event of an Lenel NVR Might Not Come Back (OG-23740):** During a VMotion event, at near completion, the majority of the channels might go to the "Video signal lost" state in Alarm Monitoring on every client. The channels might return to the full live frame rate on most clients, but on some they might never come back and stay in the Video Signal Lost state. Reloading the channels might work in some cases but it might still not solve the issue.
- **Unable to receive Communication Lost event from RC-E Recorder (OG-24126):** RC-E recorders will always appear to be online. If a RC-E recorder goes offline, there is no indication that the devices from which the RC-E is recording are no longer recording/available. This is a recorder limitation.
- **Communication Server needs to be restarted in order to import updated presets for the RC-E cameras (OG-24163):** Once the Communication Server restarts and performs Import Cameras from the recorder under the Digital Video module of System Administration, the updated preset information is available in Alarm Monitoring.
- **Connecting to VideoViewer (Browser-based Client) with Internet Explorer 64-bit on a computer with OnGuard does not work properly (OG-24258):** It is recommended to use the 32-bit version of Internet Explorer when using VideoViewer (Browser-based Client). If the 64-bit version is used, the system might download the CAB file every time the application is started. The user will see an 'x' where the video template should be. There is no way to get video to stream into the 64-bit application.
- **Schedule PTZ preset failed for the presets created in Alarm Monitoring (OG-24355):** The Schedule PTZ Action failed message is displayed.
- **NetDVMS: Restoring the network connection does not give "Video Source Signal Lost" alarm (OG-24376):** When using a NetDVMS or RC-C recorder with an Axis Encoder, there is a scenario in which camera status will not be reported properly in Alarm Monitoring. If the video cable that connects an analog camera to the Axis Encoder is disconnected while the Axis Encoder is offline or powered down, the camera will appear to be online in Alarm Monitoring when the Axis Encoder is brought back online or powered up. This is a recorder limitation.
- **Certain cameras do not have color-coded frame rates (OG-24432):** All AreCont Vision cameras do not have color-coded frame rates. The cameras added for OnGuard 2012 (6.5) do not have color-coded frame rates.
- **Unable to play recorded video from RC-E Cameras continuously for more than one hour (OG-24439):** Recorded video from RC-E cameras will not continuously play for more than one hour. It stops after playing for an hour. This is a limitation on the recorder and will be addressed in future releases.

- **Receiving incorrect "Responding" event from RC-C two minutes after Axis Encoder is disconnected (OG-24479):** When using a NetDVMS or RC-C recorder with an Axis Encoder, if the Axis Encoder is disconnected, Alarm Monitoring will correctly indicate the lost connections to the corresponding cameras. Approximately two minutes later, Alarm Monitoring will briefly (and incorrectly) identify those cameras as having been reconnected. Within a few seconds, the correct (disconnected) status will once again be reflected. This is a recorder limitation.
- **WinPCap installation changes (OG-24585):** In previous versions, WinPCap was installed along with the Device Discovery Console and Service. The system no longer installs WinPCap. The system administrator must install WinPCap. WinPCap is available on the Supplemental Materials disc.
- **Prism Migration Tool: Camera outputs are not migrated (OG-26793):** The Prism Migration Tool does not migrate camera outputs.
- **Video from third party recorder does not display in Alarm Monitoring (OG-27089):** Video from a third party recorder may not display in Alarm Monitoring even though the video displays in System Administration and Video Viewer.
- **Upgrading from SkyPoint 2.0 to SkyPoint 3.5 recommended before upgrading OnGuard:** To ensure proper operation of SkyPoint, Lenel recommends upgrading from SkyPoint 2.0 to SkyPoint 3.5 before upgrading OnGuard.

  In order to use SkyPoint 2.0, a manual update to the Communication Server application configuration file (Lnlcomsrvr.exe.config) is required.

  On each Communication Server:

  1. Stop the “LS Communication Server” service.
  2. In the OnGuard installation directory, navigate to the **Lnlcomsrvr.exe.config** file.
  3. Open the **Lnlcomsrvr.exe.config** file in a text editor.
  4. Change the default “3.5” to “2.0” as shown below:
     ```
     <?xml version="1.0" encoding="utf-8" ?>
     <configuration>
         <appSettings>
             <add key="SkyPointBaseVersion" value="2.0"/>
         </appSettings>
     </configuration>
     ```
  5. Save the **Lnlcomsrvr.exe.config** file.
  6. Restart the “LS Communication Server” service.

3.5.5. Enterprise

- **Global I/O Restrictions (OG-13969):** Global I/O linkages will not work between two Enterprise regions. Global I/O configurations must use the same Linkage Server.
- **IntelligentVideo Applications Not Available on Enterprise Master when Configured on a Child Region (OG-15971):** There is a known issue with the replication of IntelligentVideo Applications to the Master Server. IntelligentVideo Applications can be configured and monitored on a per Region basis.
- **IntelligentVideo Applications Not Supported with IntelligentVideo Application Server Located on a Different Region (OG-15972):** In Enterprise systems, IntelligentVideo Applications should not be configured for IntelligentVideo Application Servers that are located on other Regional Servers. This is not a supported configuration, and the IntelligentVideo Application will not function properly.
- **Referential Integrity Error when Saving Camera Layouts (OG-15973):** If a camera layout is saved with cameras added from another Regional Server via the Camera Lookup feature, a Referential Integrity error might occur. To save a layout that generates the error, remove the cameras located on other Regional Servers from the layout prior to saving.
- **Pre-existing User-specific Layouts Not Replicated to Enterprise Master (OG-16029):** Pre-existing user-specific video layouts are not replicated up to the Master Server when user replication is enabled. This only affects pre-existing layouts. New layouts will be properly replicated. To work around this limitation, open each existing layout and save it again with the same name.
- **Global Output Devices, Paging Devices, Workstations Specified at Master are Overwritten with Region Child Workstation after Upgrade (OG-19091):** When upgrading from a version prior to OnGuard 2008 (6.0.148), Global Output Devices, Paging Devices, and Workstations specified at the Master are overwritten with the Region Workstation after the upgrade. This does not occur when upgrading from OnGuard 2008 or later.
- **Full Download to Region Results in Unexpected Log Size and Application Error (OG-21309):** A full download to a Region could result in a log larger than expected and an application error.

3.5.6. Identity Management

- **Fargo DTC4500 Encoders (OG-15570):** Fargo DTC4500 encoders are not supported for encoding of any iCLASS applications from the OnGuard software.
- **Magicard Tango2e Must Use Driver V1.41 (OG-20299):** Magicard Tango2e driver V1.42 has a known issue with the installation of magapi.dll. Driver V1.41 is available on the Supplemental Materials disc and should be used instead.
- **Magnetic Encoding Does Not Work with Firmware V2.00 for Zebra printers (OG-23809):** Magnetic encoding will not work with firmware V2.00 for Zebra performance class card printers. Earlier versions of the firmware (up to V1.17.88 confirmed) should encode correctly.

3.5.7. 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 7.0, 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).

3.5.8. Intrusion Detection

- **NGP Panels will only support a Holiday Duration of 365 Days (OG-20814):** When setting the duration of a Holiday that will be configured in a system with NGP Controllers, do not exceed a value of 365 days. The Holiday interface will allow a value up to 366 (for support of LNL Controllers) but that value will not be compatible with an NGP Controller.
- **Unmask Door Held Open events time works differently in NGP panels compared to Mercury panels (OG-23259):** When a Mask Held Open event occurs at a reader in an NGP system, the alarm is sent after 60 seconds instead of immediately.
- **Only one event, instead of two, is generated in Alarm Monitoring when the same timezone is configured for masking Door Forced Open (DFO) and Door Held Open (DHO) alarms (OG-23263):** Only one event, instead of two, is generated in Alarm Monitoring when the same timezone is configured for masking Door Forced Open (DFO) and Door Held Open (DHO) alarms for a reader connected to a NGP Access Panel. This occurs when a door is open during the timezone, but is not closed after the end of the timezone.

3.5.9. Replicator

- **Vinca key registry setting required for Microsoft Cluster or NEC ExpressCluster 64-bit configurations (OG-30110):** In order to run the LS Client Update Server and the LS Site Publication Server service on a 64-bit operating system, add the Vinca key registry setting to the `Wow6432Node` inside the `SOFTWARE` key rather than at the `SOFTWARE` key level. This can be done by adding `Wow6432Node\ after SOFTWARE\` in each line of the registry file provided on the Supplemental Materials disc, or by manually moving the key in the registry.

3.5.10. System Administration

- **NGP label 'Check for battery' on the Power tab is misleading in how it affects the panel (OG-23942):** The 'Check for Battery' checkbox on the Power sub-tab of the NGP form in the Access Panels folder has been renamed 'Enable Battery'. This setting is enabled by default. If this setting is deselected, the NGP panel will be unable to use battery backup.

3.5.11. TruVision

- The system default time zone "Always" and "Never" are not displayed when adding a TruVision output (OG-28265).
- “A Failure establishing a connection with the search service” error message is displayed when performing a video search in Alarm Monitoring if there is no recorded video (OG-28485).
- “The file is not a valid video file” message appears when a TruVision video file is opened in Alarm Monitoring. TruVision recorders export video in a proprietary H.264 format. To view this video, use the TruVision player that is automatically installed when OnGuard is installed. This player must be manually launched. (OG-28488)
- OnGuard does not support the V-stream feature (OG-28490).
- System Administration does not send the bit rate from OnGuard into the TruVision TVR 60. The bit rate setting can be changed in the recorder’s configuration webpage or in the TruNAV software. Changes made outside of OnGuard are not reflected in the System Administration user interface. This issue does not apply to other DVRs or NVRs. (OG-29782)
- Camera names must be unique. If the camera name matches another camera in the database, you will not be able to import cameras until you specify a different name.
- Configuring alarm inputs and alarm outputs in System Administration causes the number of inputs and outputs to display as 16.
- Do not change the camera type for TruVision recorders on the System Administration Cameras form. If the camera type is changed in System Administration, then the incorrect configuration values are presented to the user (for example, the Resolution selections), and the selected values will be incorrectly applied to the recorder for that particular channel. To recover the camera type, set it back to the original camera type, or re-import the channel configuration from the recorder.
- Once the configuration for TruVision series NVRs and hybrid recorders is imported into System Administration, OnGuard cannot track configuration changes made to the TruVision recorder from the recorder web page. To synchronize OnGuard, use System Administration to re-import the camera configuration from the recorder.
- If the TruVision Add-On does not return the proper Frame Rate, Bitrate, and Resolution values for TruVision NVRs and hybrid recorders, the values of the analog channels on the DVR are automatically used in the OnGuard software.
- An IP camera connected to a TruVision recorder can support a set of frame rates and resolutions. For a given frame rate, only a few resolutions are supported. The frame rate and resolution combinations can be seen on the TruVision recorder, but not in the OnGuard software. With the current design of camera capabilities, it is not possible to display the combinations in OnGuard. Instead, all the possible frame rates and resolution sets are listed. The user should only configure valid combinations.

- OnGuard Open Video-Recorder API does not support sub stream and main stream differentiation. goVision 2 recorders always display the sub stream in live mode and main stream for recorded video. Whereas, TruVision only displays the main stream for both live and recorded video. This leads to following limitations:
  - OnGuard System Administration does not allow configuring sub stream.
  - Live fps settings in **System Administration > Camera Tab-> Normal Mode** sub-tab can be ignored, as this frame rate is for sub stream.
- TruVision channels cannot be added or deleted from the OnGuard System Administration application. Channels can only be imported.
- The Alarm Panels form in System Administration shows the number of alarm inputs and outputs as 16 even though these numbers are different in the actual recorder.
- The TruVision recorders do not support the following features in OnGuard 7.0:
  - VideoViewer (Browser-based client)
  - Remote Monitor
  - IntelligentVideo Solutions
- The PTZ icon is enabled automatically in matrix view even if the camera connected to the TruVision or goVision 2 recorder does not support PTZ. This is a third-party limitation, as there is no way for the recorder to identify if the connected cameras support PTZ. (OG-29012)
- When playing recorded video from a TVR 41 recorder, the audio does not synchronize with the video. This is a third-party limitation. (OG-28814).

3.5.12. Visitor Management

- **Supported Date Format (DE385):** “Short date, no time” (seen in FormsDesigner) is the only date format supported for date fields in Visitor Management Host.
- **Error Messages that Result From Not Having JavaScript Are Not Localized (DE395):** Visitor Management requires that JavaScript be enabled in the browser. When it is not enabled, the error message “This application requires JavaScript. Contact your administrator,” is not localized.
- **The Service Trace Viewer Tool is Needed to View the Visitor Management Tracing File (DE1472):** Windows Communication Foundation Service Trace Viewer Tool (SvcTraceViewer.exe) should be used to view the Visitor Management tracing file (Idvm.svcLog) on the server. This can be obtained from Microsoft’s Web site as part of the Windows SDK.
- **Access Control Badges Retain Previous Access Levels When Reassigned (OG-15158):** When an access control badge is assigned to a visitor being signed in, it retains the access levels currently configured for the badge. Signing in/out a previous visitor with the badge does not change the access levels.
- **Kiosk Virtual Keyboard is not localized for KOR, JPN, CHS, or CHT (OG-22235):** The Kiosk’s virtual keyboard is not localized for KOR, JPN, CHS, or CHT.

- **Front Desk Application: CSSN SnapShell: Need to run "Lenel Installer for CSSN SDK" on Supplemental Materials disc (OG-23349) (OG-24017):** In order to use the CSSN SnapShell device for scanning business cards in the Visitor Management Front Desk application, the "Lenel Installer for CSSN SDK" on the Supplemental Materials disc must be run. This should be run before connecting the SnapShell scanner for the first time and will install the necessary driver and SDK. It will also update the SnapShell SDK for existing installations.
- **Cannot log into Front Desk Application when the server operating system is Windows Server 2008 R2 (OG-25909):** The following error message appears when trying to log into the Front Desk Application when the server operating system is Windows Server 2008 R2:

  ```
  "The HTTP request is unauthorized with client authentication scheme
  'Negotiate'. The authentication header received from the server was
  'Negotiate,NTLM'."
  ```

4. Copyright and Trademark Notice