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

OnGuard® 7.1 Release Notes

Contents

1. Introduction

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

The Release Notes, Limitations, Resolved Issues, Installation, and User documents are available in portable document format (PDF) on the OnGuard disc in the **..\Program Files\OnGuard\doc\en-US** folder. The documents can be searched using the Search All User Guides feature. For corrections and additions to the Release Notes document, 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.)

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

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

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

2. Upgrades

- **Upgrading to OnGuard 7.1 (OG-29586):** Direct upgrades of the OnGuard software are supported for all systems OnGuard 2008 Plus (6.1) and newer.

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

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

  1. Checks for existing configuration data that must be manually removed before the upgrade can continue. Installation cannot proceed if any of the following are detected:
     - **Hardware:** AAD Readers, AMD-12 Input Panels, Apollo Hardware, Asset Reader Interfaces, Cisco AIC Hardware, Digitize CAPSII Receivers, Fargo DTC550, HID Read/Writer Non-programmer Encoder, ID-Check Terminal Scanner, Identix Fingerscan V20 Readers, LNVS 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 browser-based applications:** Customers migrating from Bosch ReadykeyPRO to Lenel OnGuard who use browser-based applications on the LS Platform Server must clear cached information in their browser in order to see the correct branding.

3. Versioning Information

3.1. Current CASI Firmware

- CASI DirecDoor: v2.4.8
- CASI M5, M2000, M3000: v3.4.8

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

IMPORTANT!

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

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

- LNL-1100-U, LNL-1200-U, LNL-1300-U, LNL-1320-U: v10.16.01
- LNL-500, LNL-1000, LNL-2000 ISC: v3.121
- LNL-2210, LNL-2220, LNL-3300, LNL-3300-M5 ISC: v1.201
- 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: v1.52.13
- LNL-1300e: v1.5.12
- LNL-1320 Series 1: v1.13
- LNL-1320 Series 2: v1.57.5
- LNL-1320-2RP, LNL-1320-S2RP: v1.57.3
- LNL-1380-8RP: v1.57.5
- Bioscrypt with LNL-500B gateway firmware: v1.26
- RSI biometrics with LNL-500B gateway firmware: v1.25
- Recognition Source PIM-485-16-OT with wireless LNL-500W gateway firmware: v1.10

3.3. Current Security Series (NGP) Firmware

- NGP: v1.4.8 (applies to NGP-22xxx and NGP-33xxx panels)
- NGP-1300-U: v12.09.02
- NGP-1320-U: v12.09.02
- NGP-1100-U: v12.09.02
- NGP-1200-U: v12.09.02

3.4. Current ILS Firmware

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

3.5. Current Digital Video Software

- Lenel Digital Video Recorder (LDVR): Software Version 7.21 Hot Fix 2.0
- Lenel Network Video Recorder (Lenel NVR): Software Version 7.1.1027
- IntelligentVideo Server (IVS): Software Version 7.1.1027
- IntelligentVideo Application Server (IVAS): Software Version 7.1.1027
- Lenel Streaming Video Server (LSVS): Software Version 7.1.1027

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

3.6. Minimum System Hardware Requirements

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

3.7. Supported Operating Systems

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

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

3.7.1. Windows Server 2012

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

3.7.2. Windows Server 2012 R2

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

3.7.3. Windows 8/Windows 8.1 Update

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

3.7.4. Windows 7 Professional with Service Pack 1

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

3.8. Service Packs and Critical Patches

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

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

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

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

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

3.9. Security Utility

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

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

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

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

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

3.10. Supported Database Systems

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

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

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

- For 32-bit operating systems: Click Start, then navigate to Settings > Control Panel > Administrative Tools > Data Sources.
- For 64-bit systems: Navigate to **C:\windows\SysWOW64** and run the **odbcad32.exe** file.
- Microsoft SQL Server 2012 SP1 (32-bit and 64-bit) and Express
- Microsoft SQL Server 2012 Service Pack 2 (SP2)
- 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 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 (11.2.0.3 and 11.2.0.4)
- Oracle 11g R2 Server 64-bit (11.2.0.3 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 browser-based applications require 32-bit drivers to connect to an Oracle database.

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

3.12. Internet Information Services (IIS)

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

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

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

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

Application Development:

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

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

3.13. Virtual Platforms

- VMware ESX/ESXi Server 6.X for all OnGuard services and database server with software-based license only
- VMware Workstation 10.0 and 11.0
- Microsoft Hyper-V Server 2012

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

3.14. Supported Third-party Components

- Crystal Reports version 2011 (14.0).

> **Note:** OnGuard 7.1 ships with Crystal Reports 2011. Earlier OnGuard versions shipped with Crystal Reports 11.5. Reports created with Crystal Reports 11.5 will function normally with Crystal Reports 2011.

3.15. Antivirus Software Applications

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

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

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

3.16. Supported Web Browsers

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

* Supported OnGuard applications: License Administration

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

3.17. Supported Terminal Services

OnGuard 7.1 supports Terminal Services. This support is a licensed feature. Refer to the Lenel Web site to review the current testing status before configuring terminal services. The Third Party Applications Compatibility Chart can be accessed at: https://partner.lenel.com/downloads/onguard/compatibility-charts. (You will need your Lenel login to gain access to this site.)

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

Citrix XenApp is not supported for viewing video.

3.18. OPC Versions

- OPC Data Access 2.0
- OPC Alarms and Events 1.0

3.19. SNMP Versions

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

3.20. Supported High Availability Systems

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

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

- NEC ExpressCluster X R3 32-bit LAN 3.1 (tested 3.1.5.1 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

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

3.21. End of Life Products and Features

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

4. New Features and Updates

4.1. Alarm Monitoring

- **LNL-1300e IP Interface support:** In Alarm Monitoring, view LNL-1300e alarm status events, perform firmware downloads to LNL-1300e interface readers or alarm panels, LNL-1300e reader operations (including change reader mode, open door, and mask alarms) and alarm panel operations (including mask/unmask inputs, and activate/deactivate/pulse outputs).

  LNL-1300e reader and alarm panel inputs and outputs can be placed on maps and are viewable within Alarm Monitoring.

Note:	The LNL-1300e is currently not supported by Device Discovery or the Add Reader Wizard.

4.2. Access Control

- **LNL-1300e (IP Interface) integration:** The LNL-1300e behaves like a Single Door Controller with the second reader interface configured as a slave reader for the first reader interface. Together the paired readers function as one logical reader. Therefore, the REX, Strike, and Door Contact settings are only available for reader #1. In addition, reader **Output** type "OSDP Protocol" is available for LNL-1300e (IP interface) reader #1, only. The first reader must be configured as **Reader number** 0 and the second as **Reader number** 1.

  The LNL-1300e IP interface can be configured as a reader or an alarm panel. In both cases, **Port** was extended to include the network addressing mode options for LNL-1300e readers and alarm panels. In DHCP mode, **Mac Address** entry is available. In Static IP mode, **IP Address** entry is available. (LNL-1300e readers support connection type IPV4, only.)

  The LNL-1300e supports:

  - Elevator control (128 floors and floor tracking)
  - Local I/O, Global I/O. APB, Alarm Notification, Linkage, and badge formats and offsets functionality.

  Access panels that support the LNL-1300e include the LNL-3300/3300-M5/2220/2210. The maximum number of LNL-1300e readers supported:

  - 16 readers per LNL-2210
  - 32 readers per LNL-2220, LNL-3300, or LNL-3300-M5
- **Reader board and technology separation:** On the ***System Administration*** > ***Access Control*** > ***Readers and Doors*** > ***General*** form, reader technology (such as Wiegand / Prox) was separated from reader board **Type** to better define each reader and ease configuration with a shorter list of items in **Type** as more readers are supported. Reader **Type** is now only used to specify the type of reader board you are configuring. After selecting reader **Type**, choose the reader technology separately from the new reader **Output** drop-down. (See 4.6 NGP for NGP/CASI Reader Board and Technology Separation.)

  Reader number changes: Where reader #1 and #2 were previously specified as part of the reader **Type**, this is now configured separately in the **Reader number** field. Therefore, for reader types LNL-1320 (Dual Interface), Onboard Reader, 2RP Board, and S2RP Board, the first reader must be configured as **Reader number** 0 and the second reader as **Reader number** 1.

Reader technology names remained the same except for the following:

- Lenel & Lenel M Series panels: “All Other Readers” was changed to “Magnetic.”
- ILS panels: “Prox” was changed to “Wiegand / Prox.”

Note: Pre-existing reader configurations will be migrated automatically to the new **Type** and **Output** format as described in the following table.

Panel Type	Previous Reader Type	Current Reader Type	Outputs
LNL-	Single Interface (<*Reader Technology*>)	LNL-1300 (Single Interface)	Bioscrypt RS-485 F/2F Format Mag with Wiegand Output Magnetic OSDP Protocol Wiegand / Prox
	Dual Interface Rdr 1 or 2 (<*Reader Technology*>)	LNL-1320 (Dual Interface)	
	Onboard Reader 1 or 2 (<*Reader Technology*>)	Onboard Reader	
	n/a	LNL-1300e (IP Interface)	F/2F Format Mag with Wiegand Output Magnetic OSDP Protocol Wiegand / Prox
	RS-485 Command Keypad (<*Reader Technology*>)	RS-485 Command Keypad	LNL-1300T Mag with Wiegand Output Magnetic Wiegand / Prox
	Aperio Hub 1-1 (<*Reader Technology*>)	Aperio Hub 1 to 1	Wiegand / Prox
	Aperio Hub 1-8 (<*Reader Technology* >)	Aperio Hub 1 to 8	
	Schlage PIM-485 (<*Reader Technology* >)	Schlage PIM-485	Mag with Wiegand Output Wiegand / Prox
	Schlage Wired-485 (<*Reader Technology* >)	Schlage Wired-485	
	Schlage Wireless Access (<*Reader Technology* >)	LNL-500W (Wireless gateway)	
	HandKey w/ biometric gateway	LNL-500B (HandKey biometric gateway)	n/a
	Bioscrypt RS-485 w/ biometric gateway	LNL-500B (Bioscrypt biometric gateway)	
LNL- M-Series	2RP Board Rdr 1 or 2 (<*Reader Technology* >)	2RP Board	F/2F Format Mag with Wiegand Output Magnetic Supervised F/2F Board Edge Inputs Supervised F/2F Remote Inputs
	S2RP Board Rdr 1 or 2 (<*Reader Technology* >)	S2RP Board	

Panel Type	Previous Reader Type	Current Reader Type	Outputs
			Wiegand / Prox
	8RP Board Rdr 1-8 (<*Reader Technology* >)	8RP Board Rdr 1-8	F/2F Format Supervised F/2F Board Edge Inputs Supervised F/2F Remote Inputs
HID	Reader 1 (<*Reader Technology* >)	HID VertX Base Board	Magnetic Wiegand / Prox
ILS Integra	Stand-Alone Lock	Stand-Alone Lock	n/a
ILS Offline & ILS Wireless	ILS Lock (<*Reader Technology* >)	ILS Lock	iCLASS Magnetic MIFARE Wiegand / Prox
Other (OAAP)	Generic Reader	Generic Reader	n/a
Otis	DEC Reader	DEC Reader	n/a

- **Reader Configuration Wizard enhancements for new reader board types:** Based on the addition of the Lenel M-Series panels to OnGuard, and the updates to the reader configuration forms to separate reader **Type** into separate options for reader board **Type** and reader (communication) **Output**, the Reader Configuration Wizard in OnGuard was enhanced to accommodate these changes.

  Also the reader numbering process was adjusted to make it more appropriate to the devices now supported. Previously, you selected the board type and interface as one item. This meant that if you selected "Dual Interface Rdr 1" you could only add readers to that specific reader resulting in multiple Reader 1's being created but no Reader 2 entries. Using the updated process, select the reader board type indicating if it supports 1, 2, 8, or 16 Readers, along with the Starting Address and Reader Number. From this starting point, the new numbering is simply advanced through the available reader ports on each board until all readers are assigned.

Note:	These adjustments are supported by Lenel, Aperio and Schlage. At this time, these adjustments do not include support for NGP or NGP/OCF-based panel and reader architectures.

4.3. Open Access

- Open Access is a new alternative to DataConduIT. In OnGuard 7.1 both Open Access and DataConduIT are supported. In the future, Open Access will replace DataConduIT as the OnGuard API. Therefore, new integrations should use Open Access, if possible.
- The Open Access Tool is also installed with the Open Access service for troubleshooting purposes, and is a client to the Open Access service. Both the service and the tool are server-level applications that are installed on the Platform Server. The Open Access service is a server-level application, and the Open Access Tool is a client- or server-level application.
- Currently, Open Access does not provide event or credential change notifications. Also, Open Access does not accept automatic SSO authentication, but it does accept many other kinds of authentication, making it more flexible than DataConduIT.
- In OnGuard 7.1, port 8080 will be used by the Web Server (NGINX) for Open Access.

Note:	Although NetDVMS connections also use port 8080, NetDVMS connections cannot be hosted on same server as Open Access.

  Port 8032 will be used by the LS Open Access Web Proxy from all client applications.

Note:	Previously, the LS Site Publication Server used port 8032 but this server no longer requires the use of a port.

  In addition, port 5671 is used by the LS Message Broker service with SSL.

  Ports used in OnGuard for the Open Access Web Proxy, Web Server (NGINX) for Open Access, and Message Broker can be changed via the Security Utility. For more information, refer to the Security Utility release notes. (Click [More info] from the disclaimer when the Security Utility opens to view the release notes.)

4.4. NGP

- **New Local I/O enhancements for NGP intrusion**
    - **Longer area delay timeouts added:** Three new area exit delay timeout options were added for NGP intrusion hardware. On the ***System Administration*** > ***Areas*** > ***Intrusion Detection*** form, the **Exit delay** parameter has been extended to include 5, 10 and 15 minute options.

    Notes: In Alarm Monitoring, the area status "Armed Exiting" changes to "Armed" after the time Exit delay expires.
    The "Armed On" event is generated when the arming process begins.
    After the area is armed, there is no additional event from NGP but if you have a linked Local I/O function, it will report in the Alarm Monitor.

    - **New area exit function: Area Exit Time** has been added to the **Link Area** logical events for NGP intrusion hardware. Use the **Area Exit Time** logical event to control an output (such as a sounder) during the **Exit delay** time by linking the Local I/O to this event.
- **Reader board and technology separation:** On the ***System Administration*** > ***Access Control*** > ***Readers and Doors*** > ***General*** form, reader technology (such as Wiegand / Prox) was separated from reader board **Type** to better define each reader and ease configuration with a shorter list of items in **Type** as more readers are supported.

  Reader **Type** is now only used to specify the type of reader board you are configuring. After selecting reader **Type**, choose the reader technology separately from the new reader **Output** drop-down.

  Reader number changes: Where door #1 or #2 was previously specified as part of the reader **Type**, this is now configured separately in the **Reader number** field. Therefore, for reader type Onboard Door, the first door must be configured as **Reader number** 1 and the second door as **Reader number** 2.

  Reader technology names remained the same except for "Magstripe F/2F Format" which was changed to "F/2F Format" and "Magstripe Strobed" which was changed to "Strobed."

  Notes: Pre-existing NGP reader configurations will be migrated automatically to the new **Type** and **Output** format as described in the following table.

Panel Type	Previous Reader Type	Current Reader Type	Outputs
NGP	Onboard Door 1 or 2 (<*Reader Technology*>)	Onboard Door	Magnetic Wiegand / Prox
	Dual Interface Door 1 (<*Reader Technology*>)	Dual Interface Door 1	Magnetic OSDP Protocol Wiegand / Prox
	Dual Interface Door 2 (<*Reader Technology*>)	Dual Interface Door 2	
	Single Door Interface (<*Reader Technology*>)	Single Door Interface	
	LCD Keypad	LCD Keypad	n/a
NGP/CASI	Magstripe F/2F Format Magstripe Strobed Wiegand / Prox	OnBoard I/O	F/2F Format Strobed Wiegand / Prox
		2RP/S2RP Board	
		8RP Board	
	Notes: OnBoard I/O is available for the M2000 and DirecDoor. 2RP/S2RP Board or 8RP Board is available for the M5/M3000 depending on the slot assignment. In prior releases, the CASI reader types only included reader technologies.		

4.5. System Administration

- **Print Report Options:** In ***System Administration > Administration > Reports***, clicking [Print] and then selecting **Export directly to a file** allows you to now generate more than only a PDF file. You can now select:
    - Adobe Acrobat (PDF)
    - Crystal Reports (RPT)
    - HTML 4.0
    - Microsoft Excel 97-2000 (XLS)
    - Microsoft Word (DOC)
    - Rich Text Format (RTF)
    - Separated Values (CSV)
    - Text (TXT)

  PDF remains the default report file type. Existing scheduled report actions are not affected, and will still generate PDF files if **Export directly to a file** was chosen.

- **Logical Sources (formerly DataConduIT Sources):** Logical Sources allow system administrators to add, modify, and delete third-party logical sources, devices, and sub-devices. Changing "DataConduIT Sources" to "Logical Sources" supports the addition of the LS Open Access service to the OnGuard software. When upgrading to OnGuard 7.1, existing DataConduIT Sources, Devices, and Sub-Devices are renamed to Logical Sources, Devices, and Sub-Devices.

  In ***System Administration > Additional Hardware***, the **DataConduIT Sources** menu choice is renamed to **Logical Sources**. In addition:

  - The **DataConduIT Sources** tab is now **Logical Sources**,
  - The **DataConduIT Devices** tab is now **Logical Devices**, and
  - The **DataConduIT Sub-Devices** tab is now **Logical Sub-Devices**.

  Logical Sources, **Logical Devices**, and **Logical Sub-Devices** can be added, modified, and deleted through the Open Access API.

4.6. Enterprise

- **Performance When Replicating Incremental Credential Changes, Log Table Records, and Alarm Acknowledgments:** Replicator uses a new Message Bus architecture to transfer incremental credential data from one site to another. The Message Bus architecture provides data queuing, guaranteed delivery, and SSL, resulting in improved performance, reliability, and security when transferring incremental credential data, log table records, and alarm acknowledgments. Enterprise no longer uses an ODBC connection when transferring incremental credential data and log table records.
- **Alarm Acknowledgment Replication:** Alarm acknowledgments replicate starting with OnGuard 7.1. Alarm acknowledgments that already existed prior to the OnGuard 7.1 upgrade are ignored, and updates to those alarm acknowledgments are marked as “skipped” in Enterprise.
- **Archiving to database:** By default, OnGuard replicates all data that can be archived to the Master server. For this reason, you might wish to **Archive to database** on the Master server only.

4.7. Replication Administration

- **Configuring when Log Table replication occurs:** In Replication Administration, select a Regional Server Node or Mobile Station in the System Tree, and then click **Log Transactions** in the Available Views pane. The Log Transactions window opens.
    - In general, it is best to leave replication of log transactions set to **Always**. The LS Site Publication Server service replicates faster than in earlier versions of OnGuard, so do not change this setting from **Always** unless necessary.
    - The default **Starting at** configuration is 00:00:00, and the default **Ending at** configuration is 23:59:59. If you do not change these defaults, then the **Replication occurs** field on the Log Transactions form indicates **Always**, which means the log transactions can replicate at any time.
    - If you configure both the **Starting at** and **Ending at** times to 00:00:00, then the **Replication occurs** field on the Log Transactions Form indicates **Never**, which means the log transactions will never replicate.
    - Transactions that have not replicated yet will not replicate after selecting **Never**, and are deleted from the replication queue.
    - When changing from **Never** to **Always**, transactions from this point forward will replicate. Past transactions will not replicate.
    - It is recommended to leave at least 1 hour between the **Starting at** and **Ending at** times. Shorter time intervals might not give the LS Site Publication Server service adequate time to perform the replication.

4.8. Language Support

- **Language support available with OnGuard 7.1:** Language packs are included and automatically installed when OnGuard 7.1 is installed. Customers will not need to download or apply a language pack at all. All customers will need to configure their OnGuard systems to run with a language pack (for example, run the Database Translator utility). For more information, refer to the Language Pack Release Notes (DOC-1055-EN-US) and the Language Pack User Guide (DOC-930).

5. Known Issues

5.1. General

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

  To work around this issue:

  - Add the Admin user to the **ACS.INI** file security settings and allow full control, or
  - Run the application that you use to edit the **ACS.INI** file (i.e., Notepad) using the "Run As Administrator" option, or use the configuration editor.

- **SafeNet driver (OG-23789):** The SafeNet driver has been removed from the installation, but if needed it is available on the Supplemental Materials disc.

- **Mobile Monitoring support in OnGuard pending (OG-30103):** At this time, support in OnGuard for Mobile Monitoring is pending. Refer to the Applications Compatibility Chart at https://partner.lenel.com/downloads/onguard/compatibility-charts. (You will need your Lenel login to gain access to this site.)

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

- **Client Update:** When performing an upgrade, refer to the Upgrade Guide for information about Client Update. If upgrading from a release prior to OnGuard 2012 (6.5), when upgrading the client machines, the manual steps indicated in the Client Update section in the Upgrade Guide must be followed so that the automatic client update can be used in the future.

  The Client Update Server allows the OnGuard server workstation to automatically update client workstations. When a client workstation opens an application in OnGuard, the application detects that the software version does not match the database. The application then allows the user to either cancel the login or update the client software. This functionality only exists for applications that are part of the OnGuard installation suite. Two services enable this functionality, one installed on the server workstation (LS Client Update Server Service) and another installed on each client workstation (LS Client Update Service). These services are only used to update client workstations. Server workstations must still be updated manually.

- **Replicator Actions after upgrading to OnGuard 7.1:** When upgrading to OnGuard 7.1, all full download and incremental download actions are deleted from Scheduler. These Replicator actions cannot be recreated in OnGuard 7.1 because they are no longer necessary. For more information, refer to Run Replication as a Windows Service in the Replicator User Guide.

- **Replication and Open Access issues in cluster systems:** When installing or upgrading to OnGuard 7.1, certificates to be used for SSL with the Message Broker are deployed by default. As of 7.1, Message Broker is used with Enterprise and Open Access. Due to this, you may experience issues where replication fails or Open Access is not working in an NEC ExpressCluster X or MS Cluster environment. This issue will be addressed in a future releases.

To work around this issue, update the **MessageBroker.config** file for SSL.

Note:	If you plan to use your own self-signed certificates, this is not necessary.

1. At the command prompt, execute the following command:

   ```
   lnl_app_server_certificate_installer.exe -
   key=DRIVE:\\PATH\\TO\\nginxConfFile\\og_cert_key.pem -
   cert=DRIVE:\\PATH\\TO\\nginxConfFile\\og_cert.pem -store="LS
   Certificate Store" -cn=<virtual computer name>
   ```

Note:	The default file location of the .exe file is **C:\program files (x86)\OnGuard\LSP\Certificates** and the default location of the nginx.conf file is **C:\ProgramData\Lnl\nginx\conf**.

2. Navigate to and open the **MessageBroker.config** file that is located by default at **C:\ProgramData\Lnl**.
3. Edit the following line and uncomment the line by removing the "#" character from the beginning.

   ```
   ssl-cert-name=<virtual computer name>
   ```

4. Save the file, and then restart the services.

Note:	"Virtual cluster name" is another reference to "virtual computer name" in our documentation.

5.2. 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.

5.3. Installation

- **'Allow service to interact with desktop' option required when using Client Update to update OnGuard (OG-29277, OG-29291):** When using Client Update to update from OnGuard 2012 and service releases, or OnGuard 2013 and service releases, to OnGuard 7.1, the LS Client Update Service on ALL client machines must have the **Allow service to interact with desktop** option selected.

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

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

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

5.4. Lenel NVR

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

5.5. Visitor Management

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

6. Copyright and Trademark Notice