OnGuard 2010 6.4 Technology Update 1.1 Limitations

Last Modified on 12/10/2021 1:37 pm EST

This document contains a list of OnGuard and third-party known limitations for OnGuard 2010 Technology Update 1.1, and is intended as a supplement to the OnGuard 2010 Technology Update 1.1 Release Notes.

After the Preparing to Install window closes, there may be a pause before the installation appears to continue on slower systems. During this time the mouse pointer may not indicate an hourglass and it may appear that the installation has stopped. The installation will continue after a few moments.

A rapid double-click on a graphic within the online help produces an error. This is a known limitation within HTML help.

System settings changes, such as font sizes, theme colors, and new printers are not reflected in running OnGuard applications until they are restarted.

After linking a cardholder to a directory, the values in the Name and User Name columns may be displayed as a long string of numbers. The SID is displayed when the system cannot establish the name of the user based on the SID. This issue is related to the trust between users, domains, computers, sub-networks.

2. Next Generation Panels (and downstream devices)

2.1. Global Anti-Passback (and Mustering) NOT supported on the NGP Panels

Global Anti-Passback will have no effect on Readers or Areas controlled by the NGP Controllers. The feature can still be enabled at the system level to support LNL Controllers within the environment.

2.2. Host Controller Encryption is only supported with Automatic Key Management

Systems containing NGP Controllers will support 128-bit AES encryption between the host and controller, but should only be configured for ‘Automatic Key Management’.

2.3. NGP Card Format Support

Card Formats on the NGP Controller cannot be specified at the reader level. Card Formats are selected and prioritized at the panel level. All card formats selected for the panel are evaluated at all the readers connected to the panel. Only the first two card formats assigned to the panel can be used on NGP LCD Keypads with attached readers. This is outlined in the NGP Hardware Installation Guide in section 8.1.3 "Keypad Wiring".

2.4. STU (Subscriber Terminal Unit) Connections not supported

The STU connections available on the NGP World Wide Modem, and the STU configurations on the panel from System Administration are not supported with Release 1 of NGP. Please leave them set to the defaults.

2.5. NGP Reader Types MUST match per Door

Each NGP Door Controller supports both IN (Entry) and OUT (Egress) readers. The reader technology, Wiegand or magnetic, MUST be the same for both readers.

2.6. NGP Controllers DO NOT support the use of Masking Groups (Alarm or Intrusion)

As the NGP Controllers are capable of supporting native Intrusion, there is no need for the use of Masking groups.

2.7. NGP Inputs cannot be masked based on a timezone

There is a possibility for this to cause confusion with arming schedules and the numerous point types, so it was not included.

2.8. NGP Readers DO NOT support the use of ‘Facility (Site) Code’

This reader mode is not available for access unless the readers are in an offline or ‘fall-back’ situation. The fall-back setting is located on the NGP Panel Options Tab.

2.9. NGP Panels will support only 4 types of EOL for the panel

This includes the default supervision settings that are built into OnGuard. A value for line supervision is only loaded to the panel when it is specifically used for a NGP circuit.

2.10. NGP Panels DO NOT support selective cardholder download

With NGP’s higher level of cardholder support (500K) this was not enabled as a feature at this time.

3. Intrusion Detection

3.1. A PX/QX/RX panel cannot be marked as offline

A PX/QX/RX panel cannot be marked as offline.

3.2. If using the Guardall PX Config tab in System Administration, then the Communication Server must be running.

- If using the Guardall PX Config tab in System Administration, then the Communication Server must be running.
- Guardall Intrusion Panel - "Unable to communicate" pop-up appears twice for every panel. (OG-21165): If the Communication Server for the panel cannot be accessed, you may get error messages indicating that it can't communicate. The issue is due to the previously mentioned limitation and not having the Communication Server running or not reachable.

The HID Edge software provided to Lenel by HID for device communications is not compatible with 64-bit operating systems (Windows 7 64-bit, Windows Server 2008 R2 64-bit) and Windows Vista. Communication Servers expected to communicate to Edge devices cannot use these operating systems.

HID Edge devices are supported with Windows XP SP3, Windows Server 2003 R2 SP2 Standard Edition, Windows Server 2008 SP2 Standard Edition 32-bit, and Windows 7 Enterprise 32-bit.

4.2. Door Strike Time (OG-19333)

For LNL access panels, the Door Strike time is about ½ second shorter than what you configure it for.

4.3. Inaccurate Search Results Count in Browser-based Area Access Manager (6x-9279)

On a system with cardholder and/or badge type segmentation enabled, the results count for searches displayed in the browser-based Area Access Manager can be incorrect. The workaround is to use the desktop client Area Access Manager.

A “Load report failed from C:\WINDOWS\Temp” error may occur when running reports from the Area Access Manager Browser-based Client. To successfully run reports, the IIS_WPG (in Windows Server 2003) or IIS_IUSRS (in Windows Server 2008) account must have read/write access to the **C:\WINDOWS\Temp** folder.

During a biometric verification, additional keys pressed at an associated keypad will be ignored and will not start a new access attempt.

Port 6 on the LNL-2000 should not be treated as the primary port when using dual path communications. If it is, status may not be properly reflected regarding the active port in Alarm Monitoring.

Galaxy Ethernet module is not supported for Dimension panels.

The Magicard Prima 3 printer should use driver version 5.7, not version 5.7 issue 1. If driver version 5.7 issue 1 is used, the printer will not pick up the card from the hopper; it will just time out and not print at all.

5.2. Change in 10 Print Slap Record Format (OG-13658)

The 10 Print Slap capture and license have been renamed OpenCapture. Sagem-Morpho templates are now captured for use with Lenel bioCLASS readers. 10 Print Slap records are now stored in an optimized format in the database. The record only allocates the amount of space necessary for the fingerprint; the record is optimized so that it does not save space for all fingerprints if only one is captured. Any existing 10 Print Slap records must be deleted and re-captured following the upgrade to OnGuard 2010 in order to maintain use of this feature. If existing 10 Print Slap records are not re-captured, Database Setup may fail, and a database error will be received when viewing a cardholder record that has not been updated.

5.3. IE SmartTOUCH Sector Allocation Limitation

The IE SmartTOUCH only works with first 1K (Sector 0 to 15) of a 4K MIFARE card. Any data encoded in sector 17 or above will not be read by the reader.

Fargo DTC550 HID read/writer non-programmer encoders are not supported for encoding of any iCLASS applications from OnGuard.

The Magicard Prima M, print driver 3.0.7.0, F/W C02/29/57 printer does not include parity in its bit count for track 1, and its default setting is 7-bit sign. On most other printer drivers, 7-bit as a default would be correct. However, to encode standard magnetic track data (IATA) to track 1 on the Prima M, the print driver must be set to 6-bit sign.

User-defined phone number fields must have a field type of text, not numeric. To restrict use to numbers, use a “9” Template when defining the field in FormsDesigner. Phone numbers entered as numeric fields may have their values truncated.

HID VertX/Edge firmware has an 8-digit PIN limitation. OnGuard allows a PIN of up to 9 digits. When used with Edge readers, the last digit of any 9-digit PIN will be ignored, and the first 8 digits will be matched.

The workaround for this issue is to configure the system to truncate the PIN to 8 digits. This configuration will grant or deny access based on the validation of the first 8 digits entered by the user.

OnGuard clients intending to display video from SkyPoint systems must meet the minimum specifications for SkyPoint clients.

6.2. Spservn.exe Service Stops or Closes Unexpectedly When More Than 20 TB of Storage is in Use (OG-19312)

A maximum storage capacity of 20 TB is recommended for LDVR. Larger storage sizes may cause the spservn.exe service to use a high amount of memory, causing it to eventually stop or close unexpectedly.

6.3. Recorded Video Cannot be Exported from a Failover Video Recorder (OG-15744)

Video that is recorded to a failover video recorder cannot be exported.

- Camera time-stamps are not available with Axis MPEG4 cameras.
- Due to the way the Axis cameras communicate, the Inputs and Outputs are not as reliable in MPEG4 as they are with MJPEG.
- Lenel does not recommend Capture Video only on Event with MPEG4, as it takes several seconds to connect to the camera and begin recording.
- When using MPEG4 and moving in and out of Time-Lapse recording, there is a one-frame loss. Therefore, Pre-roll should be set at least one second greater than you need. The higher the frame rate, the less noticeable this one-frame loss is. Lenel also recommends using a high frame rate with MPEG4 and Time-Lapse Recording.
- When using an Axis Video Server (241Q, 241S, 241QA, 241SA) you will occasionally experience a problem where the video will stop recording when you change the frame resolution. This can be fixed by opening a live video stream and letting it run for several seconds, or restarting the LNVR services.
- Video Acceleration in the Video Player MUST be set to None in order to insure a clear video picture.
- Axis cameras may experience a ghosting effect at higher Group of Video Object Planes (GOV) lengths. This issue is resolved with Axis firmware version 4.40, which is available for download on the Axis Web site. If the firmware cannot be upgraded, the GOV length should be set to 30 or less frames.

- The Inputs on the Lumenera camera cannot be configured or monitored through OnGuard. This applies to both Lumenera and the Lenel Smart Camera.
- Starting video search may cause the computer's CPU to enter a constant loop due to the high resolution of the video. Megapixel video searches that are lengthy may cause the system to stop responding and require a reboot. Results will vary by computer. Short searches are recommended to avoid this issue.
- Setting a camera to 1024 x 768 and a compression of 10 or less may result in 0 frames being streamed.
- Lumenera 375 camera image may change from normal to dark if a large dark object blocks or is placed in close proximity to the lens and covers more than 60% of the field of view for more than 2 seconds.

Lumenera Technical Support can be reached at +1 613-736-4077 (press 2 from the auto-attendant) between the hours of 9:00 a.m. to 5:30 p.m. EST or via e-mail at support@lumenera.com.

The White Balance for Panasonic cameras cannot be updated from the OnGuard user interface and must be adjusted manually from the camera Web page.

Note: For more information about Panasonic i-Pro Network Cameras with MPEG4, refer to the Lenel Knowledge Base. When multiple connections are made to Panasonic i-Pro network cameras, some of the connections may fail. This may occur during specific conditions when LNVR services, or network connectivity, are lost and then restarted, and/or when Lenel LNVR clients simultaneously attempt/make direct connections to individual cameras. This is fundamentally a camera limitation caused by a limit to the number of concurrent sessions supported by the cameras. The problem is experienced only in very specific circumstances. Once a camera is disconnected, the session/UID may not be properly terminated, and is not automatically released until a timeout has been reached. The default time out for unresponsive sessions/UIDs with i-Pro network cameras is two (2) minutes. To resolve this issue, close all connections to the camera and wait two (2) minutes before reconnecting.

Panasonic WV-NP1000/1004 cameras have settings that cannot be applied by OnGuard. These settings can be applied to achieve either the best quality or the best frames per second performance. The following settings modify either of these: "Scan mode" and "Maximum resolution" (depending on the Scan mode either 1280x960 or 960x720.) When the scan mode is set to Partial Scanning the user can get higher frame rates but lower quality. At Full Scanning the user gets better quality but lower frames per second. The maximum resolution needs to be turned off when the user is trying to access lower resolutions from the LNVR.

The Lumenera LI045C camera has a limitation which only allows a resolution of 720x480 for NTSC and 720x576 for PAL.

Mobotix cameras will not work properly with Direct Connect at default timeout. The default 5 second timeout will not work since the camera may take longer to start. Set the Direct connect to something longer, such as 10 seconds.

The frame rate drops when viewing video from an AXIS 241Q through OnGuard when the camera Web page is opened. This is a known third-party limitation with the video server. Camera Web pages should be closed when viewing video through OnGuard.

The AXIS 240x video servers do not support the detection of the video channel interface. These models will not support the Video Signal Offline feature found in the latest LNVR servers.

Inputs are not supported with HIKVision cameras in this release.

Non-numeric passwords are not supported for HIKVision cameras. It is possible to successfully change the password for the camera using the Security tab in System Administration to a non-numeric password. If this occurs, the user will be locked out of the camera Web page.

Adjusting the resolution in the HIKVision DS-2CD852F camera causes the video to appear washed-out. To return the video image to normal after changing the resolution, open the Camera > Video Sensor sub-tab, click [Reset to Defaults], then click [Apply].

If HIKVision/Lenel PCI boards are added to an existing LNVR, the drivers for the boards may need to be installed manually.

Toshiba cameras do not support the ability to obtain the maximum frame rate with the maximum resolution. This is a third-party camera limitation of Toshiba cameras. The OnGuard system will attempt to obtain the maximum frames out of the camera but some configurations might not achieve the desired frame rate because the camera may provide less.

Bosch cameras are not supported with IntelligentVideo events.

The Web page for Bosch cameras offers a Performance Option to limit the frame rate. This option does not affect the frame rate in OnGuard.

A shadow effect on the Bosch Dinion Camera can be removed by enabling the Dynamic Noise Reduction setting on the **Camera Settings** > **Camera Profile** > Enhance section of the camera Web page.

There is a three (3) second delay before video is displayed from a Bosch 8008 camera. This delay is seen when launching video from the Bosch 8008 and when switching from one 8008 channel to another.

Changes to Sony firmware affect the H.264 protocol. The LNVR supports both methods, but when upgrading cameras to the newest firmware you may need to perform a full download for the LNVR to communicate properly with the camera.

When using a Device Camera link, there may be a small lag time of 1 to 2 seconds before the event actually triggers the event on the camera. This delay should be taken into account when setting pre-roll on a camera.

When an LNVR is offline, there may be a delay before alarms are received by the Communication Server.

The Go To Preset action cannot be executed when there is a direct connection to the camera. The LNVR must be online for this action to be successful.

If a video cell appears black in Remote Monitor, press stop and then play. If this does not resolve the issue, right-click the Remote Monitor and select Download Database.

When a user selects a cell in browser-based VideoViewer, PTZ control is assumed and PTZ is locked for other users. To release control of the PTZ, select the lock/unlock button or wait for the timeout.

- Users should refrain from viewing video during times that the LNVR is downloading video from the camera. The In-Camera Storage timezone should not be set to Always.
- Cameras configured with In-Camera Storage appear offline in Alarm Monitoring. Communication Loss/Restored alarms are generated each time video is launched for the camera. As a workaround, users can configure Camera I/O or Camera Motion Detection.
- Users should not use the filename prefix option on the camera Web page. This setting will “hide” the files from the LNVR download service. The filename prefix should be left blank.
- If the LNVR is downloading from the camera users may experience delays in stopping LNVR services.
- Extra memory in the camera can cause it to stop responding. If this occurs, the drive may need to be formatted.

Advanced Systems Format (ASF) files are not compatible with Alarm Monitoring. If an ASF file is loaded, the date will appear incorrect. ASF files should be opened with Windows Media Player.

VideoViewer must be opened once before exported LDVR files can be opened with a mouse double-click.

When exporting video in Windows Vista, the Windows user must have write access to the location that the video is saved. The default save location is the Desktop.

Users may request recorded video from the LNVR with the VideoViewer (Browser-based Client) that the video recorder does not have. The video recorder will provide whatever video it can so if the user requests 12:10:00 and the LNVR has video after 12:15:00, the video will play from that available time and onward. The time in the cell will be different from the time in the requested Begin Time window. When the user selects a different cell and then re-selects the original cell with the time mismatch, the video will play from the beginning of the available video.

The Grayness slider for the color mask in the Object Detection engine is not guaranteed to smoothly change the color mask. Configure color mask as much as possible using the color palette tool and the Hue slider.

The Intel Decoder is required for playback using the stand-alone video player for the Panasonic 474. Install the Intel IPP by running **Setup.exe** from the OnGuard Installation disc in the **\Temp\INTEL** folder. Copy the **LnrIntIDmo.dll** file from the OnGuard disc in the **\Common\Lenel** folder to **C:\Program Files\Common Files\Lenel** and register the file.

6.35. Remote Monitor 6.4.500 Hot Fix 1.0 is required with OnGuard 6.4.500 Technology Update 1.1.

6.36. Customers using the SkyPoint video system with integration of OnSSI recorders into OnGuard must use SkyPoint SP4 with OnGuard 6.4.500 Technology Update 1.1.