OnGuard 2010 6.4 Technology Update 1.1 Resolved Issues

Last Modified on 10/06/2022 4:20 am EDT

This document contains a list of issues that have been resolved in OnGuard 2010 Technology Update 1.1, and is intended as a supplement to the OnGuard 2010 Technology Update 1.1 Release Notes.

1. General

This release contains a resolution for this issue. The issue caused several files (DLLs and EXEs) not to be signed.

1.2. Database installation utility has an error reading from the registry on SQL Express 64-bit install (OG-20592)

This release contains a resolution for this issue. The error no longer occurs while using the database installation utility with SQL Express, 64-bit install.

1.3. DataConduIT: Lnl_IncomingEvent.SendIncomingEvent method should not require time parameter (OG-20804)

This release contains a resolution for this issue. The method does not require a time parameter. The only parameter that is now required is the source. Time will be filled in with current UTC time if left blank. Description is also not required.

1.4. Potential lockup in DataExchange Service (OG-21225)

This release contains a resolution for this issue. The resolution prevents potential lockups in the DataExchange service.

1.5. Message boxes presented to the user when an exception occurs, causing a service to stop responding (OG-21226)

This release contains a resolution for this issue. The issue only occurs if running as a service, and could cause a service to stop responding. The resolution prevents a message box from being displayed to the user when an exception occurs when running as a service.

1.6. Add ‘pause’ or threshold functionality to DataExchange when interfacing with the Communication Server RPC thread (OG-18996)

This release contains a resolution for this issue. DataExchange now waits until the threshold is reached before it moves to the next record.

1.7. DataConduIT service leaks memory when using the Execute() method on any DataConduIT object (OG-20621)

This release contains a resolution for this issue. This fixes a leak when using the Execute() method on any DataConduIT object.

1.8. Special characters in the OnGuard user’s password will prevent the user from logging into Web applications (OG-20816)

This release contains a resolution for this issue.

1.9. Performance issues with use of the Segmentation Utility (OG-20919)

This release contains a resolution for this issue. There were performance issues with the Segmentation Utility on systems with 1000 or more segments. The issue was the filling of the Segment List control that appears when adding a Segmented Cardholder. Before this change and with 15 milliseconds latency the control fill took 3.3 minutes to fill with 2000+ segments. After the fix the control is filled in 205 milliseconds. Along with this change any other use of the Segmentation Utility will be much faster after this change since it is just accessing in memory data.

1.10. Events may fail to be restored due to improper processing of some values in the SERIALNUM column (OG-21063)

This release contains a resolution for this issue. The issue can be identified by encountering the error:
“Cannot insert the value NULL into column 'SERIALNUM', table 'accesscontrol_Dev.dbo.EVENTS_RESTORED'; column does not allow nulls. INSERT fails. The statement has been terminated.”

1.11. Performance issues with BADGELINK operations and DataExchange (OG-21138)

This release contains a resolution for this issue. When using the BADGELINK table in DataExchange (assigning access levels to badges), the performance has been increased.

1.12. Performance issues with BADGELINK operations and DataConduIT (OG-21139)

This release contains a resolution for this issue. The performance for assigning access levels to badges has been increased only if the user refresh threshold is increased. By default this is set at 1 minute. This ensures that user permissions are updated within a minute. However, if user permissions are not getting updated all the time for the DataConduIT user, then this can be bumped up to 15 or 30 minutes. To do this:
INSERT INTO LNLCONFIG SET LNLVALUE = 1800 WHERE LNLCONFIGID = 33
This value is specified in seconds. The above command sets it to 30 minutes. DataConduIT will need to be restarted for this to take affect.

2. Access Control

2.1. Selective Download is allowed but not reliable for Edge readers (OG-16177)

This release contains a resolution for this issue. Selective cardholder download is now allowed and reliable for HID VertX Edge reader. (This issue was incorrectly listed as resolved for OnGuard 2010.)

2.2. Access Levels for Edge readers not downloaded to hardware correctly (OG-19840)

This release contains a resolution for this issue. When downloading the access levels to an Edge reader, the access levels are now sorted so that access levels are downloaded to Edge readers first, followed by other access levels. The user is also prevented from configuring badges with more than eight access levels for a given Edge reader. The following message appears:
“Unable to add this access level, because doing so will exceed the eight access levels per badge limit of the HID controller.”

2.3. System Administration is slow to respond when saving a badge (OG-18626)

This release contains a resolution for this issue. There was an issue that caused System Administration to become slow to respond when saving a new or modified badge when the system was configured to check for unique PINs for badges.

2.4. Alarm Monitoring is slow to update panel status on startup when one or more Communication Servers is offline (OG-20435)

This release contains a resolution for this issue. Logging into Alarm Monitoring when one of the Communication Servers is offline will no longer slow down the entire system.

2.5. Communication Server closes unexpectedly when sending more than 126 intrusion points to a Intrusion Mask Group (OG-20584)

This release contains a resolution for this issue. If an intrusion mask group was created containing 127 or 128 points and then sent to an LNL panel, the Communication Server closed unexpectedly.

2.6. Alarm Monitoring closes unexpectedly if map has Global APB icon on it (OG-20685)

This release contains a resolution for this issue. Alarm Monitoring no longer closes unexpectedly when Global APB is enabled and you open a map that has a Global APB icon on it.

2.7. Performance - Bulk Access Level Removal - Actual removal takes ~ 23 hours to complete action for 16,504 cardholders (OG-20089)

This release contains a resolution for this issue. The time to do bulk access level operations has significantly improved. Downloading the changed badge to the panel is now done in the Linkage Server. The Linkage Server is required to be running when doing either bulk assignment or bulk removal of access levels.

2.8. Error occurs when modifying a Badge: “Datetime field overflow. Fractional second precision exceeds the scale specified in the parameter binding.” (OG-20720)

This release contains a resolution for this issue.

2.9. Reader Auxiliary Output loses status in Alarm Monitoring when an Aux Input is triggered (OG-20738)

This release contains a resolution for the following issue. If an Auxiliary Output on an LNL-2220 or LNL-3300 is activated and an Auxiliary Input belonging to an Intrusion Mask Group is activated and then secured, when Alarm Monitoring is logged out and back in, or the panel is queried for new hardware status it will incorrectly show that the Aux Output is no longer enabled.

2.10. When custom options feature is used, double options are displayed when right-clicking DataConduIT event (OG-20826)

This release contains a resolution for this issue.

2.11. Cannot assign disposable badges when a system-wide badge ID range is created (OG-20871)

This release contains a resolution for this issue.

2.12. HID EdgeReader firmware 2.2.7.47 issue - access granted, but Badge ID/Cardholder name not seen in Alarm Monitoring if only one card format is assigned to the reader (OG-21005)

This release contains a resolution for this issue. HID EdgeReader firmware 2.2.7.47 successfully reads 2K/2AA, 16K/2AA, 16K/16AA iCLASS cards encoded in HID Access Control (iCLASS) smart card format that are associated with any type of Wiegand Access Control card formats of 26 - 64 total bits on card, and correctly reports Card Name/Badge ID in Alarm Monitoring events screen when only one Wiegand format or multiple (8) Wiegand card formats are assigned to the reader.

2.13. Unchecking "User has internal account" clears password but leaves username intact (OG-21022)

This release contains a resolution for this issue. Now when disabling the internal account for a user the password will not be cleared out so when you re-enable the password it should remain as it was previously set.

2.14. Web applications allow users without internal or linked accounts to login (OG-21023)

This release contains a resolution for this issue. Web applications do not allow users without internal or linked accounts to login.

2.15. Can enable/disable and view current status of an action you don’t have segment permissions for (OG-21045)

This release contains a resolution for the following issue. If Segment A user adds an action Segment B user won’t be able to modify it but that Segment B user will be able to enable/disable and view the current status of the action. Now if you don't have segment permissions to modify an action you won't be able to enable/disable or view current status of the action.

2.16. Long login time for Alarm Monitoring with several cameras, device links, and maps (OG-21055)

This release contains a resolution for this issue. The login time has been decreased.

2.17. Copy PIN does not work when adding a second badge to the same cardholder (OG-21132)

This release contains a resolution for this issue. The Copy PIN feature is now working properly.

2.18. Editing a multi-segment custom alarm can result in loss of assigned events (OG-21152)

This release contains a resolution for this issue. Now the situation is prevented because the user will not be able to edit the alarm as a single segment user if the alarm has hardware from other segments.

2.19. Unable to get two LNL-2220 panels online at the same time when using hostname for communication (OG-21256)

This release contains a resolution for this issue. Panels are now able to get online.

2.20. Changes made in 6X-3517 can lead to the inability to print Visitor badges (OG-21313)

This release contains a resolution for this issue. After upgrading to 6.4, the user was no longer able to print their Visitor badges; they were presented with the following error:
“One or more fields were not found in the database. The fields and/or their data source names could have been renamed or removed from the database since the last time layout was edited with BadgeDesigner. (Imaging Error Code=0x6EB5.) Badge Layout in error: "Essential Personnel VIS" (ID=58). The following database fields are in error: BADGETYP.NAME.”
Now a Badge Layout for Visitors can include information regarding Badge information.

3. Digital Video

3.1. Daylight Savings Time (DST) issue (OG-21499)

This release contains a resolution for this issue. Customers using OnGuard video will observe a specific behavior when launching recorded video from an event (other video functions are unaffected). The video displayed will begin to play from a time 1 hour earlier than the time of the event requested (similar to having 1 hour of pre-roll). All video stored in the recorders is being maintained with the correct time.

3.2. Double Video on Alarm does not work with NetDVMS channels (OG-20601)

This release contains a resolution for this issue. The issue caused Double Video on Alarm to not work properly with NetDVMS channels.

3.3. During a reconnect of NetDVMS, the Communication Server may close unexpectedly (OG-20670)

This release contains a resolution for this issue. During a reconnect to a NetDVMS DVR, the Communication Server may throw an exception and close unexpectedly.

3.4. There are too many white balance options in the Video Sensor tab for the Axis Q1910 camera (OG-20845)

This release contains a resolution for this issue. The extra white balance/thermal setting has been removed.

3.5. Axis Q1910 Thermal Camera uses System Administration's white balance settings to control thermal palette (OG-20993)

The Axis Q1910 thermal camera color palettes can be adjusted by modifying the white balance settings in the OnGuard software. The white balance values correspond to the following palette settings:

- 0 - Atlantis
- 14 - Axis
- 29 - Black-hot
- 43 - Ice-and-Fire
- 57 - Nightvision
- 71 - Planck
- 86 - Rainbow
- 100 - White-hot

3.6. After upgrading to 6.4.500 HF 1 (1.0.112) the port field for the NetDVMS is 0 (OG-20947)

This release contains a resolution for this issue. The user interface now shows an empty port field after upgrading. The user should empty the field in order to start using the default. Blank ports are meant to represent the default port and in the case of NetDVMS, it is 8080.

3.7. AXIS 233D camera does not support PAL resolutions (OG-18376)

This release contains a resolution for this issue. The AXIS 233D camera now supports PAL and NTSC.

3.8. Daylight Saving Time should be disabled on goVision recorders (OG-20353/20547)

This release contains a resolution for this issue. Setting the clock now sets the DVR time zone time correctly.

3.9. Http video closes unexpectedly when Lnl.OG.WebService disabled anonymous authentication for single sign-on (OG-18141)

This release contains a resolution for this issue. The user is now able to view video in VideoViewer (Browser-based Client) and Area Access Manager (Browser-based Client), using normal login, single sign-on, and "Shift" to cancel single sign-on.

3.10. VideoViewer (Browser-based Client) stops responding if requested recorded video is not available (OG-20404)

This release contains a resolution for this issue. VideoViewer (Browser-based Client) stopped responding if using a date/time for recorded video that did not exist. The error only happened if any previously valid recorded video was played in the particular cell. VideoViewer (Browser-based Client) now displays a message that says that the video is not available, and continues playing live video.

3.11. VideoViewer/Alarm Monitoring displays frozen frame of video if camera goes offline and doesn't notify the user (OG-20561)

This release contains a resolution for this issue. Previously, the user received no indication that the video signal had been lost other than a frozen frame. This applied to both VideoViewer and Alarm Monitoring. Note: The resolution for this issue does not function properly when buffered reader is enabled for the live video clients. This will be addressed in a future release.

3.12. Buffer slider in live and recorded video does not show the buffered video (OG-20695)

This release contains a resolution for this issue.

3.13. Video Processing algorithms don't work on Hybrid LNVRs with Darim 408 or 444a cards (OG-20569)

This release contains a resolution for this issue. Video processing alarms are now seen in Alarm Monitoring from hybrid channels.

3.14. VideoViewer (Browser-based Client) login times are slow for large systems (OG-20711)

This release contains a resolution for this issue.

3.15. Axis Q7406 has problems reporting channel status in H.264 mode (OG-20722)

This release contains a resolution for this issue.

3.16. OnGuard 6.3.249 and above not indexing all the continuous archive files (OG-20734)

This release contains a resolution for this issue. If the user tried to access a video clip that was in a video file that did not index properly, it was reported as not found. The fractional second precision error message no longer appears in the log file or in the bottom pane when looking at the running archive server application.

3.17. LNVR fails to restart recording from MPEG4 or H.264 camera with an input after network connection to the camera is lost and then restored (OG-20762)

This release contains a resolution for the following issue. The LNVR fails to recover properly from a temporary network outage if an MPEG4 or H.264 camera has an input configured in OnGuard. This results in the LNVR not recording from that channel even after the network connection is restored. In addition, the LNVR does not report a communication error when the network is down so OnGuard keeps showing the channel as online.

3.18. Video client randomly pauses and never recovers (OG-20766)

This release contains a resolution for this issue.

3.19. Live video client stops responding watching Arecont 3130 cameras when they switch from Day-Night-Day (OG-20876)

This release contains a resolution for this issue.

3.20. Issues with playback of live video from LNVRs - ghosting, reduced frame rate, jitter, etc. (OG-20920)

This release contains a resolution for this issue.

3.21. Using Ctrl-C hotkey (versus menu option) to capture image from LNVR camera recorded playback may produce inconsistent results (OG-20943)

This release contains a resolution for this issue.

3.22. Capture Image may result in an incorrect or ghosted image while playing recorded H.264 video from LNVR camera with a relatively large GOV setting (OG-20984)

This release contains a resolution for this issue. Now when using the Ctrl + C option or the menu option on a high GOV H.264 camera, there is no ghosting when the capture image dialog appears.

3.23. Live buffered video (DVR-like capability) freezes for up to 15 minutes before resuming (OG-21102)

This release contains a resolution for the following issue. If the user is using the live buffered video capability, the live video will frequently freeze for up to 15 minutes before resuming.

4. Enterprise

4.1. Activity history (formerly Original Notes) is not displayed in Alarm Acknowledgement dialog for Enterprise systems (OG-15821)

This release contains a resolution for this issue. This was only an issue when Alarm Monitoring was logged into a database which was different from the database the Communication Server was connected to. For example, Alarm Monitoring logged into the Master or parent region for a child region Communication Server.

4.2. ID Allocation service does not attempt to reconnect to the database when connection is lost (OG-18574)

This release contains a resolution for this issue. There was an issue that caused the ID Allocation Service not to attempt to reconnect to the database when the connection was lost.

4.3. Need to expose the User Replication setting (USERS.LNL_DBID) through DataConduIT (OG-20765)

This release contains a resolution for the following issue. DataConduIT will add the OnGuard User with their Replication setting set to be local to the source of the record. This means that if you add the Users to the Enterprise Master they will not replicate to other sites. The setting is now exposed on the Lnl_User to allow clients to set it as desired while still defaulting to the local option. Please refer to the DataConduIT User Guide for more information.

4.4. Replicator will not move Enterprise transactions with a negative Badge ID (OG-20815)

This release contains a resolution for this issue.

4.5. Enterprise: On change of visitor to "local region only", delete transactions for other regions should include visit events (OG-20962)

This release contains a resolution for this issue.

4.6. Replicator generates unnecessary transactions which leads to higher volume of transactions at customer site (OG-20987)

This release contains a resolution for this issue.

4.7. Performance issues using new ‘intelligent’ MMOBJS replication (OG-21110)

This release contains a resolution for this issue. The performance has been improved.

4.8. Replicator - Changing a Cardholder from "All Regions" to "local region only" does not remove the Cardholder from sub-regions (OG-21193)

This release contains a resolution for this issue. Now when downloading, Replicator will check the Cardholder's replication setting. If the Cardholder’s replication setting does not belong at the target but it is already there the Cardholder will be removed. If the Cardholder is not at the target the transaction will simply be skipped. The modify transaction will be switched to a delete, and the transaction error text will display:
“Removed from destination based on Replication settings” to indicate that it was switched to a delete to remove the record from the destination since it did not belong.

4.9. Replicator - Removing a Cardholder Segment does not remove the Cardholder from regions (OG-21196)

This release contains a resolution for this issue.