LENEL:S2

HELUG 2023
OnGuard 8.2 Key Features Overview

July 2023 – Product Release

LenelS2 Product Management – Brian Tripp

OnGuard Evolution – How we talk to customers…

LENEL:S2

Core Software/Hardware

Released January 2021

OnGuard® 8.0

Allegion RU/RM
(Crash Bar – Remote Undog/Monitor)

End User - SUSP Notification
Cybersecurity and Hardening Updates
HTTPS for License Admin
Milestone – Video Tile 1.3 Support

Released June 2022

OnGuard® 8.1

Aperio® AH40 IP Hub – 64 Locks
Promotion of X-Series Controllers
Controller IP Client Support

Credential Factory Support Cumulus
Cybersecurity and Hardening Updates
API Auditing Improvements

milestone Deeper Integration for Unified Experience

Silent Installs / Rehydration

Released June 2023

OnGuard® 8.2

Badge Override – Locked
Honeywell PW7K

OpenAccess API Performance
Credentials – EV2 Diversified Keys
Acknowledgement UDF Support
Mobile Credentials NFC

Cloud Compatibility Chart

OnGuard 8.2 went to Partner Center the week of June 12th. Press Release on Tuesday June 20th.

2021 | 2022 | 2023 | 2024

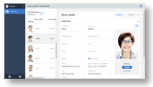
Browser Clients/Modules

'NEW' Reports v1.0

Monitor Maps & Milestone

Surveillance 1.3 Milestone

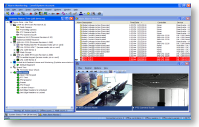
Magic Monitor for OnGuard


Credentials UI Refresh

Reports for ENT

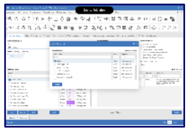
Visitor Updates

Magic Monitor for ENT

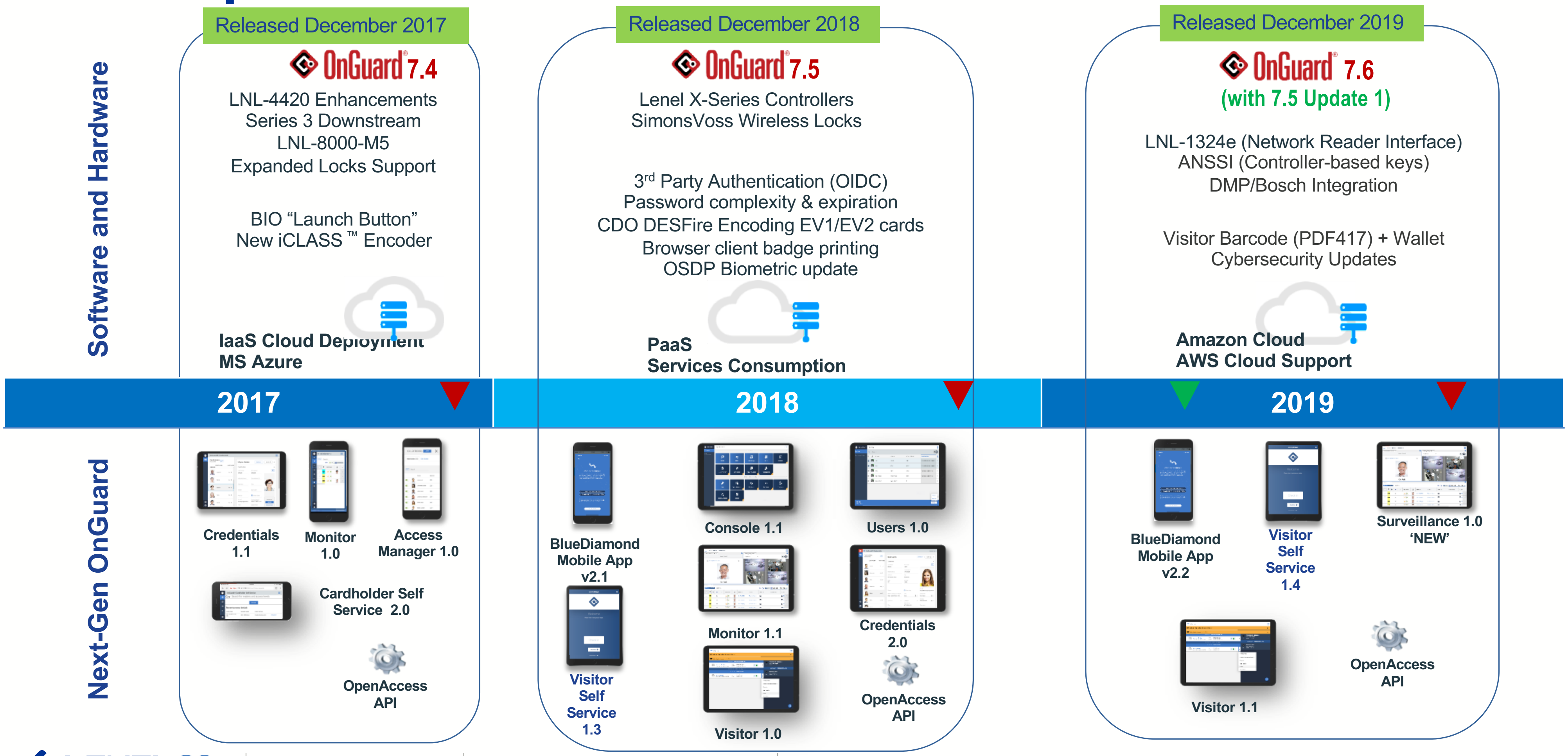

Windows Client UI Refresh

'New' OG Reports & Dashboards Client

Magic Monitor Updates


Windows Client Dialog Refresh

Roadmap – 2017 thru 2020



Software and Hardware

Released December 2017

OnGuard® 7.4

LNL-4420 Enhancements
Series 3 Downstream
LNL-8000-M5
Expanded Locks Support

BIO "Launch Button"
New iCLASS ™ Encoder

IaaS Cloud Deployment
MS Azure

Released December 2018

OnGuard® 7.5

Lenel X-Series Controllers
SimonsVoss Wireless Locks

3rd Party Authentication (OIDC)
Password complexity & expiration
CDO DESFire Encoding EV1/EV2 cards
Browser client badge printing
OSDP Biometric update

PaaS
Services Consumption

Released December 2019

OnGuard® 7.6
(with 7.5 Update 1)

LNL-1324e (Network Reader Interface)
ANSSI (Controller-based keys)
DMP/Bosch Integration

Visitor Barcode (PDF417) + Wallet
Cybersecurity Updates

Amazon Cloud
AWS Cloud Support

2017 | **2018** | **2019**

Next-Gen OnGuard

Credentials 1.1
Monitor 1.0
Access Manager 1.0
Cardholder Self Service 2.0
OpenAccess API

BlueDiamond Mobile App v2.1
Console 1.1
Users 1.0
Monitor 1.1
Credentials 2.0
Visitor Self Service 1.3
Visitor 1.0
OpenAccess API

BlueDiamond Mobile App v2.2
Visitor Self Service 1.4
Surveillance 1.0 'NEW'
Visitor 1.1
OpenAccess API

Browser ‘Client Navigation’ Changes

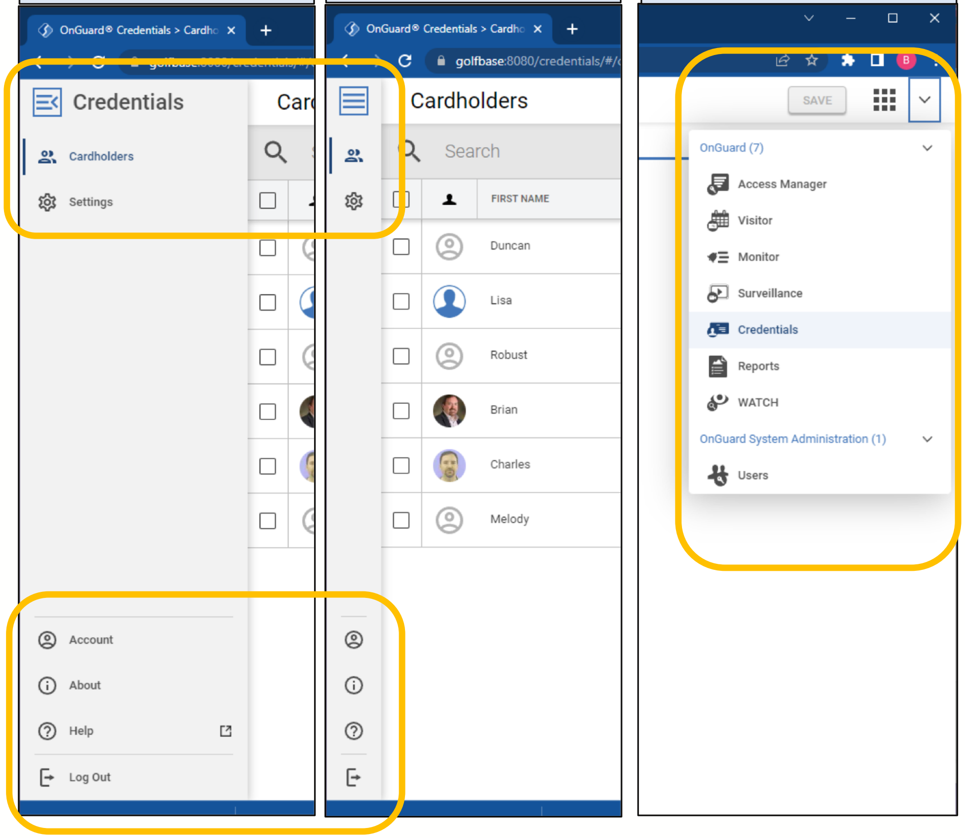
- Left Navigation
  - Open/Close reduces to an icon display
- Console ‘List’ Navigation
  - Responds to what you have on ‘My Console
- Account Pages
  - Account of the user (change password)
  - About
  - Help (automatically opens in a new tab)
  - Log Out ☺

- Supports accessibility and better user experience
- Visual changes and component refactoring
- No changes in the functionality expected

OPEN

CLOSED

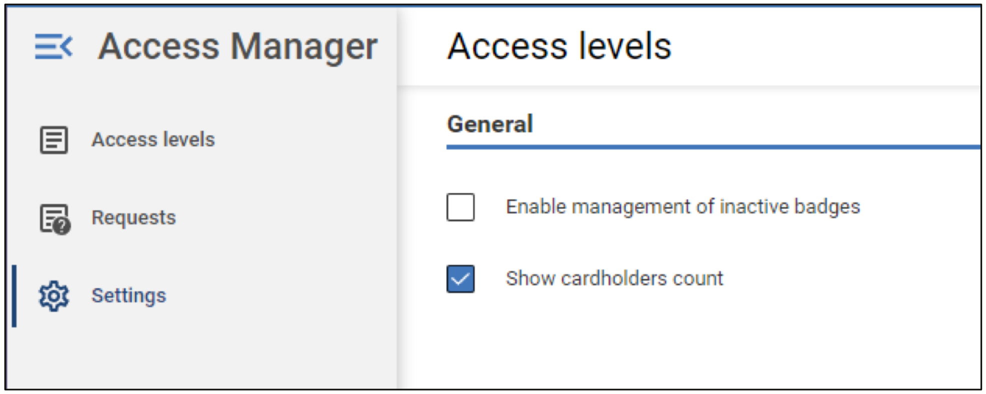
Console ‘List’



Continuing growth in browser clients…

Growing the support of OnGuard browser clients, brings their value to more customers and use cases…

- Access Manager client now supports visibility and assignment to 'Inactive' badges
- Credentials
  - Displays total searched cardholder counts
  - Supports improved WCAG accessibility
- Monitor client
  - Adds the ability to customize the Cardholder Verify display, for better visibility and screen/layout format
  - Click on Photo Thumbnail to see a larger photo of the cardholder involved in the event

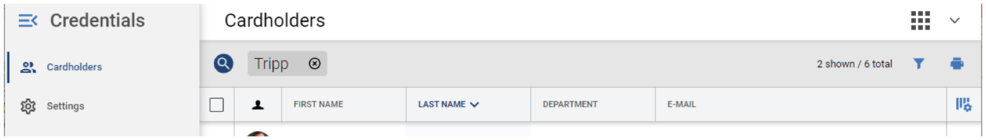


Access levels

General

□ Enable management of inactive badges

☑ Show cardholders count

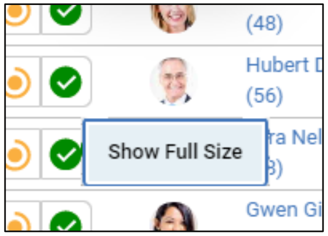


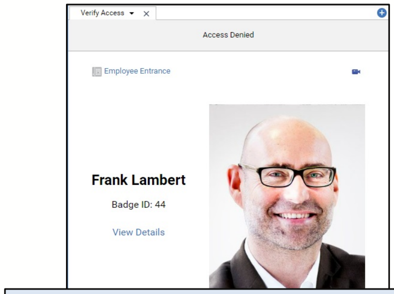
Cardholders

Tripp

2 shown / 6 total

□	FIRST NAME	LAST NAME	DEPARTMENT	E-MAIL





Access Denied

Employee Entrance

Frank Lambert

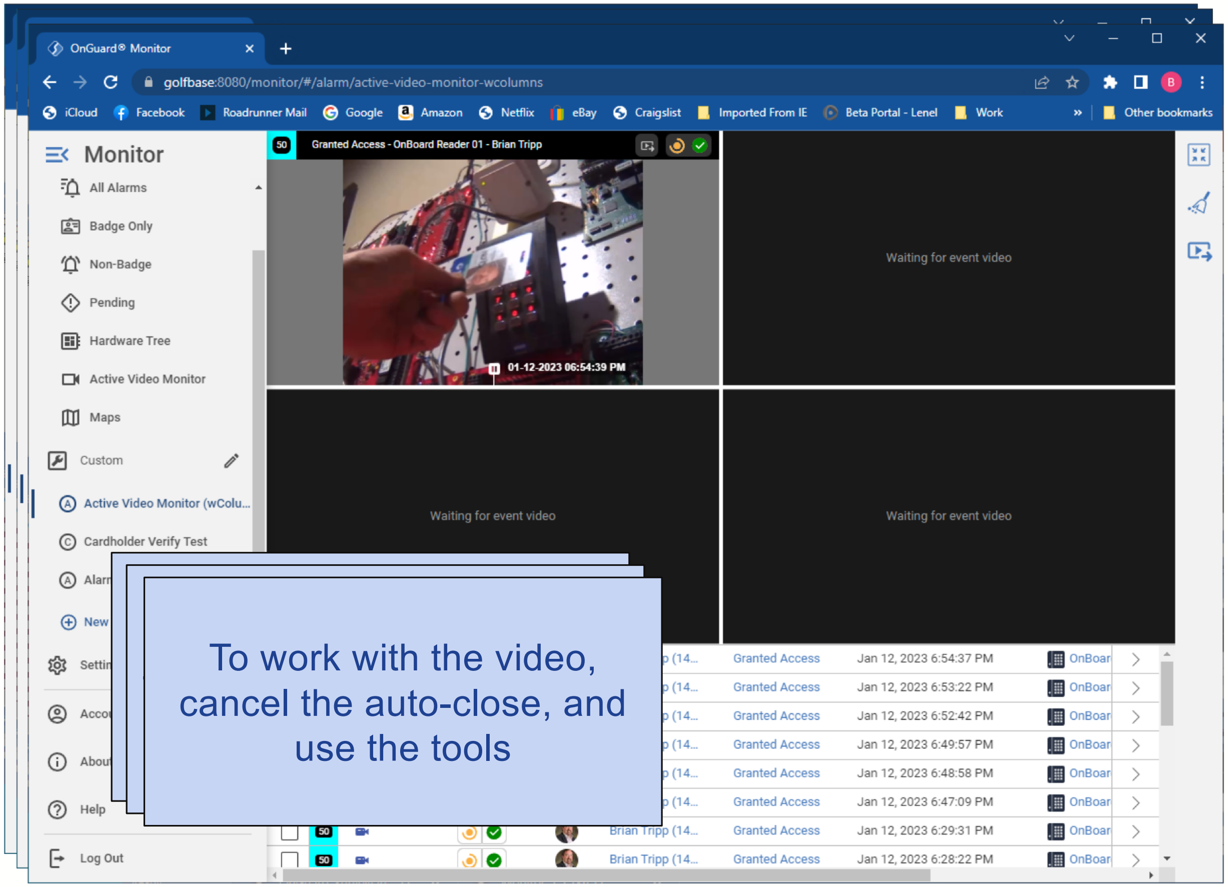
Badge ID: 44

View Details

Cardholder Verify example

OG Monitor: Added Support in Active Video Monitor

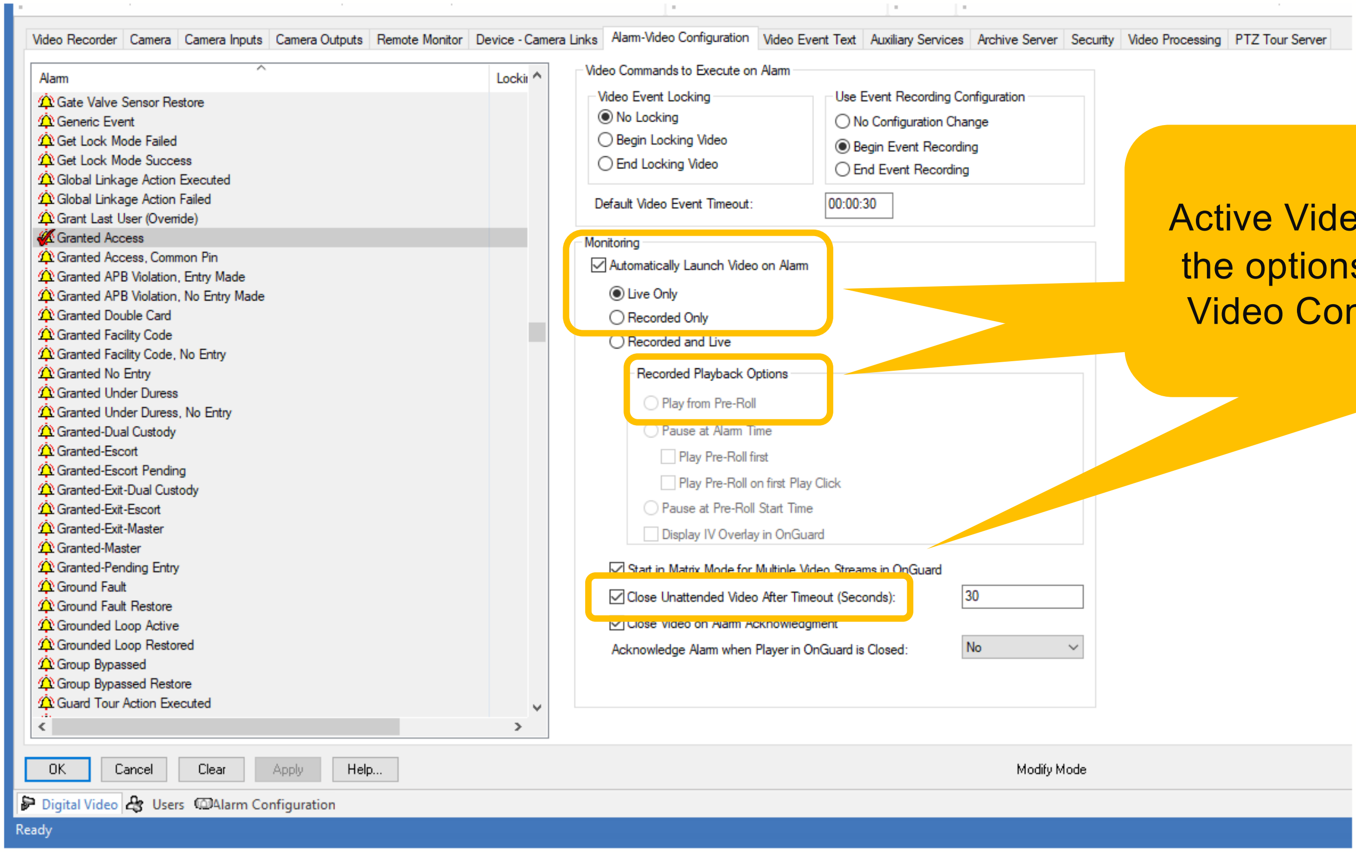
- Monitor: Pre-Roll support in Active Video Monitor
  - Configure Pre/Post roll for the camera
  - Configure Launch Live Video on an Alarm
- Monitor: Close video on timeout in Active Video Monitor
  - You can see the timeout countdown and cancel if needed



p (14...	Granted Access	Jan 12, 2023 6:54:37 PM	OnBoar
p (14...	Granted Access	Jan 12, 2023 6:53:22 PM	OnBoar
p (14...	Granted Access	Jan 12, 2023 6:52:42 PM	OnBoar
p (14...	Granted Access	Jan 12, 2023 6:49:57 PM	OnBoar
p (14...	Granted Access	Jan 12, 2023 6:48:58 PM	OnBoar
p (14...	Granted Access	Jan 12, 2023 6:47:09 PM	OnBoar
Brian Tripp (14...	Granted Access	Jan 12, 2023 6:29:31 PM	OnBoar
Brian Tripp (14...	Granted Access	Jan 12, 2023 6:28:22 PM	OnBoar

To work with the video, cancel the auto-close, and use the tools

Alarm-Video Configuration Support



Video Recorder | Camera | Camera Inputs | Camera Outputs | Remote Monitor | Device - Camera Links | Alarm-Video Configuration | Video Event Text | Auxiliary Services | Archive Server | Security | Video Processing | PTZ Tour Server

Alarm	Lockii
Gate Valve Sensor Restore	
Generic Event	
Get Lock Mode Failed	
Get Lock Mode Success	
Global Linkage Action Executed	
Global Linkage Action Failed	
Grant Last User (Override)	
Granted Access	
Granted Access, Common Pin	
Granted APB Violation, Entry Made	
Granted APB Violation, No Entry Made	
Granted Double Card	
Granted Facility Code	
Granted Facility Code, No Entry	
Granted No Entry	
Granted Under Duress	
Granted Under Duress, No Entry	
Granted-Dual Custody	
Granted-Escort	
Granted-Escort Pending	
Granted-Exit-Dual Custody	
Granted-Exit-Escort	
Granted-Exit-Master	
Granted-Master	
Granted-Pending Entry	
Ground Fault	
Ground Fault Restore	
Grounded Loop Active	
Grounded Loop Restored	
Group Bypassed	
Group Bypassed Restore	
Guard Tour Action Executed	

Video Commands to Execute on Alarm

Video Event Locking
- ● No Locking
- ○ Begin Locking Video
- ○ End Locking Video

Use Event Recording Configuration
- ○ No Configuration Change
- ● Begin Event Recording
- ○ End Event Recording

Default Video Event Timeout: 00:00:30

Monitoring

☑ Automatically Launch Video on Alarm
- ● Live Only
- ○ Recorded Only
- ○ Recorded and Live

Recorded Playback Options
- ○ Play from Pre-Roll
- ○ Pause at Alarm Time
  - □ Play Pre-Roll first
  - □ Play Pre-Roll on first Play Click
- ○ Pause at Pre-Roll Start Time
- □ Display IV Overlay in OnGuard

☑ Start in Matrix Mode for Multiple Video Streams in OnGuard

☑ Close Unattended Video After Timeout (Seconds): 30

☑ Close Video on Alarm Acknowledgment

Acknowledge Alarm when Player in OnGuard is Closed: No

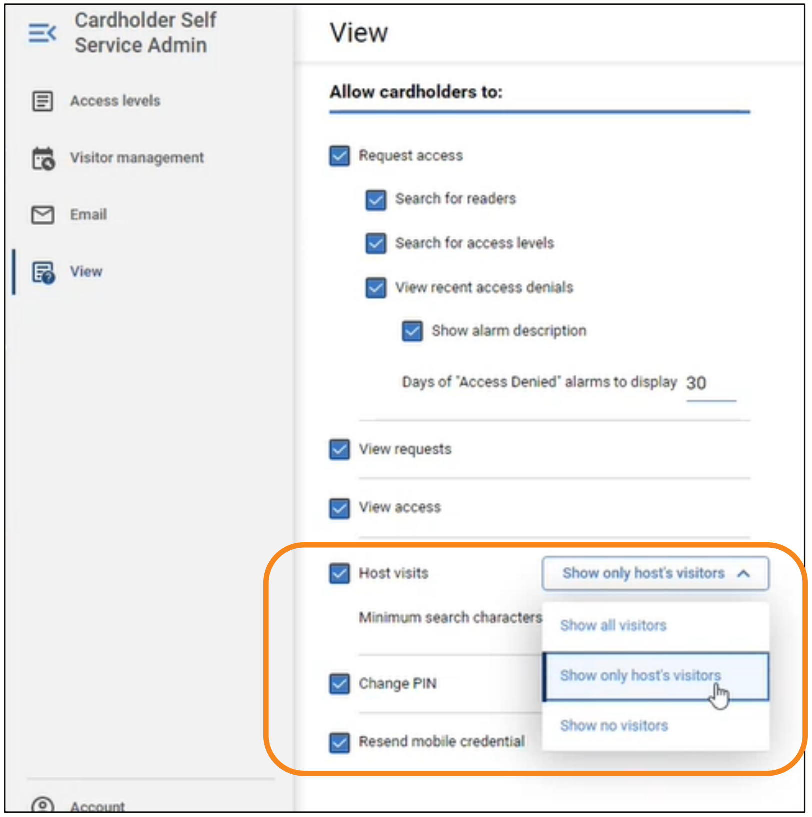
Active Video Monitor supports 4 of the options available from Alarm-Video Configuration / Monitoring

Cardholder Self Service – Visitor Host 'Privacy' Update

Provides a flexible tool for visitor check in, managing visitor badges and access levels, engaging groups, capturing visitor photos, and printing badges

- In support of global privacy concerns, CSS Visitor Host changes how Visitors are searched
- New 'Host Visits search options are available
  - Show all visitors
  - Show only host's visitors (default)
  - Show no visitors
  - Minimum search characters
    - Number of characters to type PRIOR to submitting search request

NOTE: Using the more restrictive options creates the opportunity for more duplication in Visitor records in OnGuard.



View

Allow cardholders to:

☑ Request access

☑ Search for readers

☑ Search for access levels

☑ View recent access denials

☑ Show alarm description

Days of 'Access Denied' alarms to display 30

☑ View requests

☑ View access

☑ Host visits — Show only host's visitors

Minimum search characters

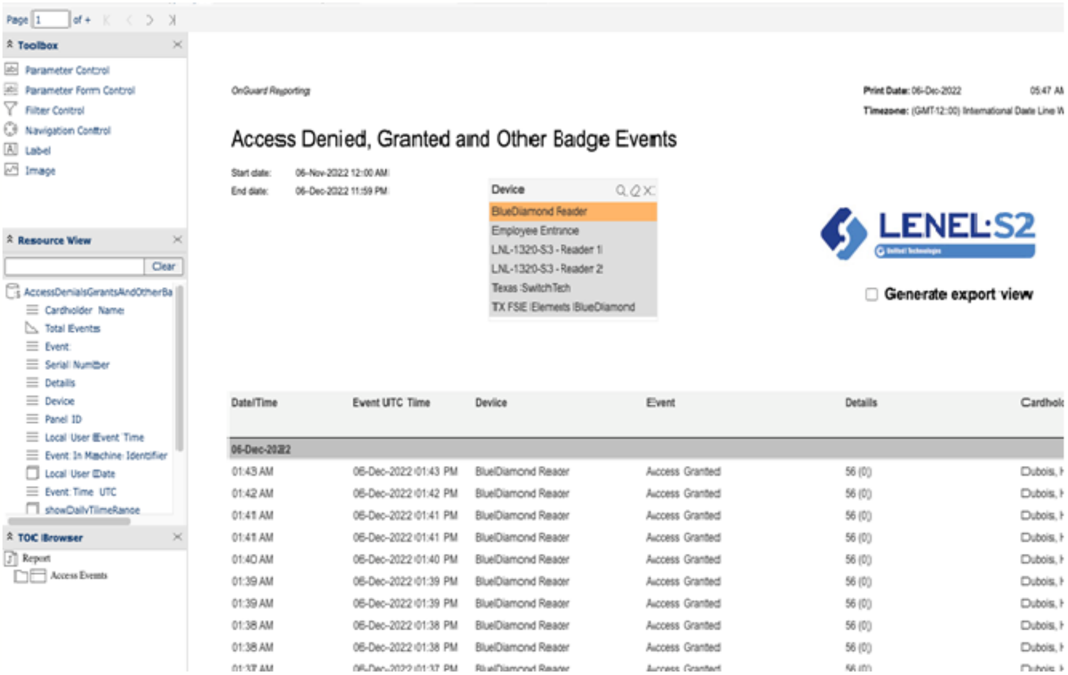
☑ Change PIN

☑ Resend mobile credential

Overview of OnGuard 8.2 Reporting & Dashboards

New Reports Client and updated LS Reporting Server support added customization and cybersecurity

- Replaced Logi Reports client with LenelS2 native client
  - Usability/Consistency
  - Accessibility
  - Localization (Partial)
- New "ToolBox" in Reports Studio (requires Advanced Reporting license)
  - Add text boxes and images to reports
  - Add interactive Filter and Parameter controls directly to the report
  - Add navigation controls



OnGuard Reporting

Print Date: 06-Dec-2022 05:47 AM

Timezone: (GMT-12:00) International Date Line W

Access Denied, Granted and Other Badge Events

Start date: 06-Nov-2022 12:00 AM

End date: 06-Dec-2022 11:59 PM

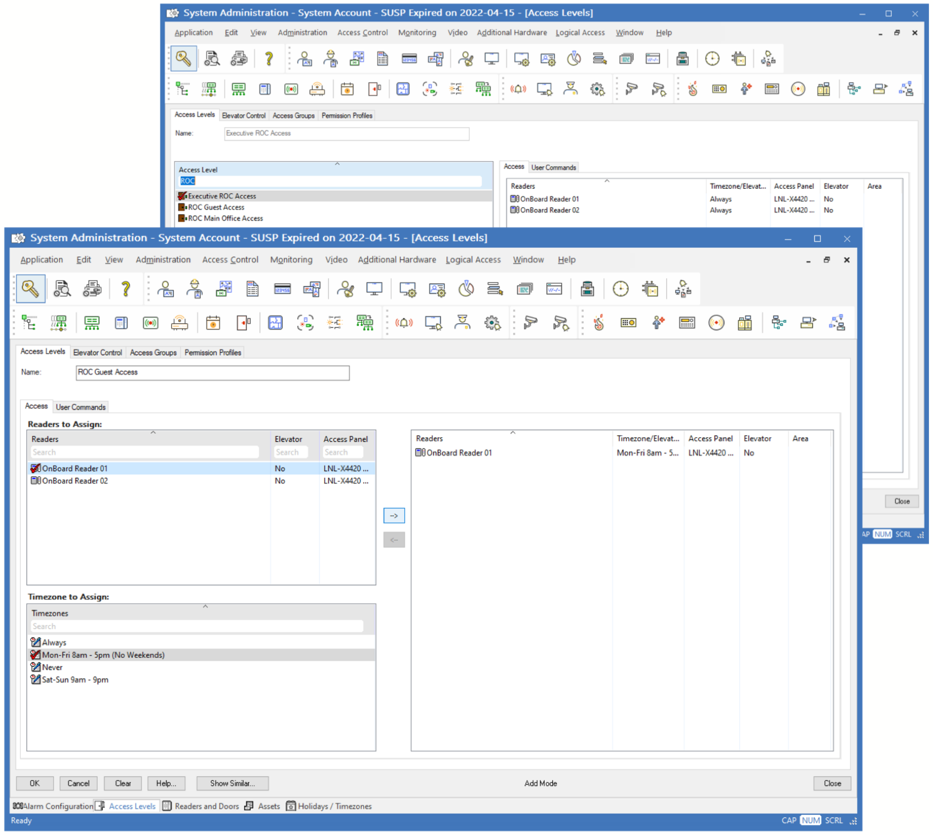
Date/Time	Event UTC Time	Device	Event	Details	Cardhol
06-Dec-2022					
01:43 AM	06-Dec-2022 01:43 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:42 AM	06-Dec-2022 01:42 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:41 AM	06-Dec-2022 01:41 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:41 AM	06-Dec-2022 01:41 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:40 AM	06-Dec-2022 01:40 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:39 AM	06-Dec-2022 01:39 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:39 AM	06-Dec-2022 01:39 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:38 AM	06-Dec-2022 01:38 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:38 AM	06-Dec-2022 01:38 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,
01:37 AM	06-Dec-2022 01:37 PM	BlueDiamond Reader	Access Granted	56 (0)	Dubois,

Reports edit screens with new tools

Windows Client Refresh

Bringing color back to Tool Icons, improving the usability of key dialogs for and filtering

- Bringing ‘accent color’ back to tool bar icons helps users who use color for tool identification
- Updated key dialogs to take better advantage of screen ‘space’
    - Access Levels, Timezones/Holidays, Alarm Definition, and Local IO
- Additions of filtered lists, allows users to easily focus on items in large systems



Name: Executive ROC Access

Access Level
ROC
Executive ROC Access
ROC Guest Access
ROC Main Office Access

Readers	Timezone/Elevat...	Access Panel	Elevator	Area
OnBoard Reader 01	Always	LNL-X4420 ...	No	
OnBoard Reader 02	Always	LNL-X4420 ...	No	

Name: ROC Guest Access

Readers to Assign:

Readers	Elevator	Access Panel
Search	Search	Search
OnBoard Reader 01	No	LNL-X4420 ...
OnBoard Reader 02	No	LNL-X4420 ...

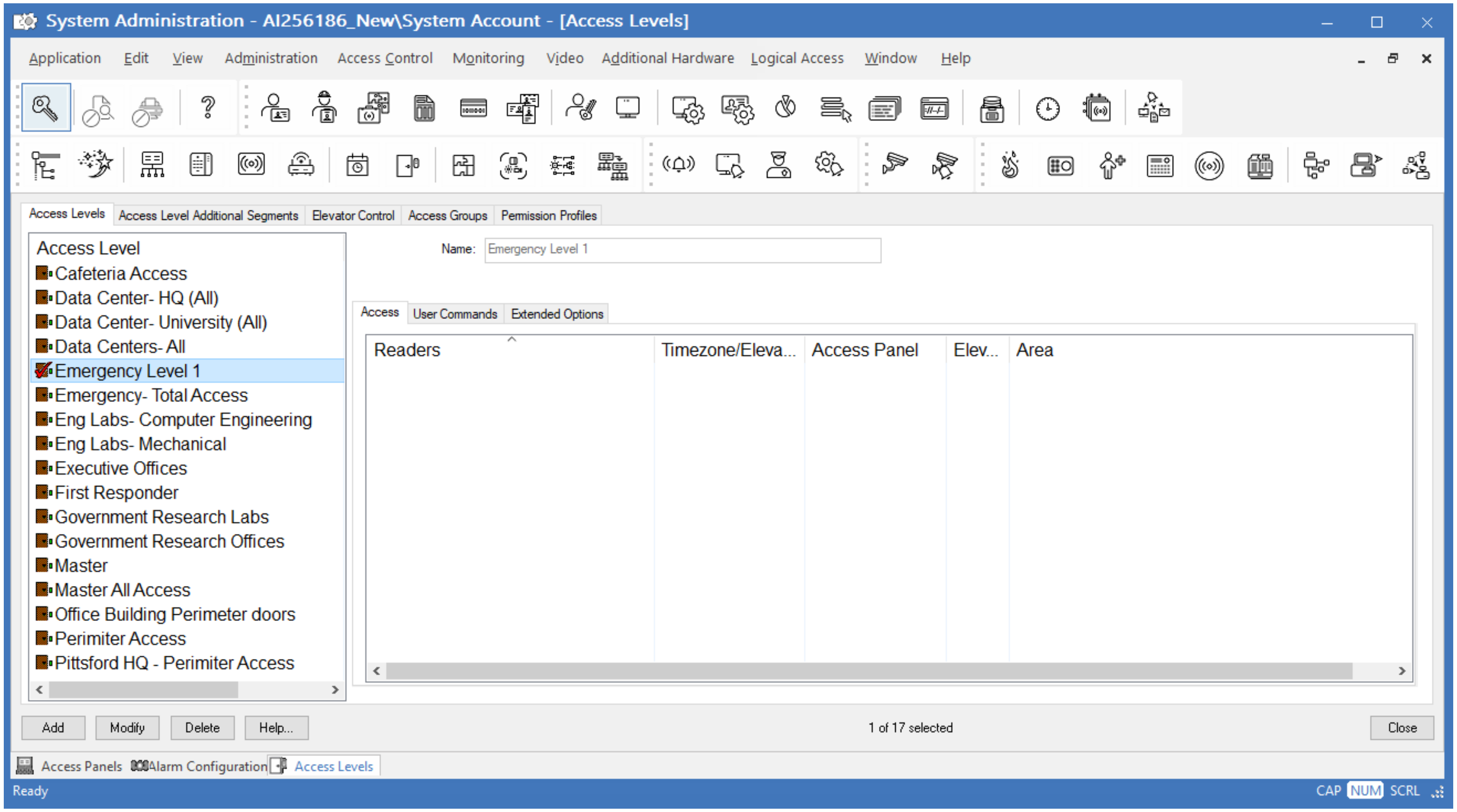
Readers	Timezone/Elevat...	Access Panel	Elevator	Area
OnBoard Reader 01	Mon-Fri 8am - 5...	LNL-X4420 ...	No	

Timezone to Assign:

Timezones
Search
Always
Mon-Fri 8am - 5pm (No Weekends)
Never
Sat-Sun 9am - 9pm

OnGuard 8.2 Access Levels Modify Dialog

OnGuard 8.1 Access Levels



System Administration - AI256186_New\System Account - [Access Levels]

Access Level

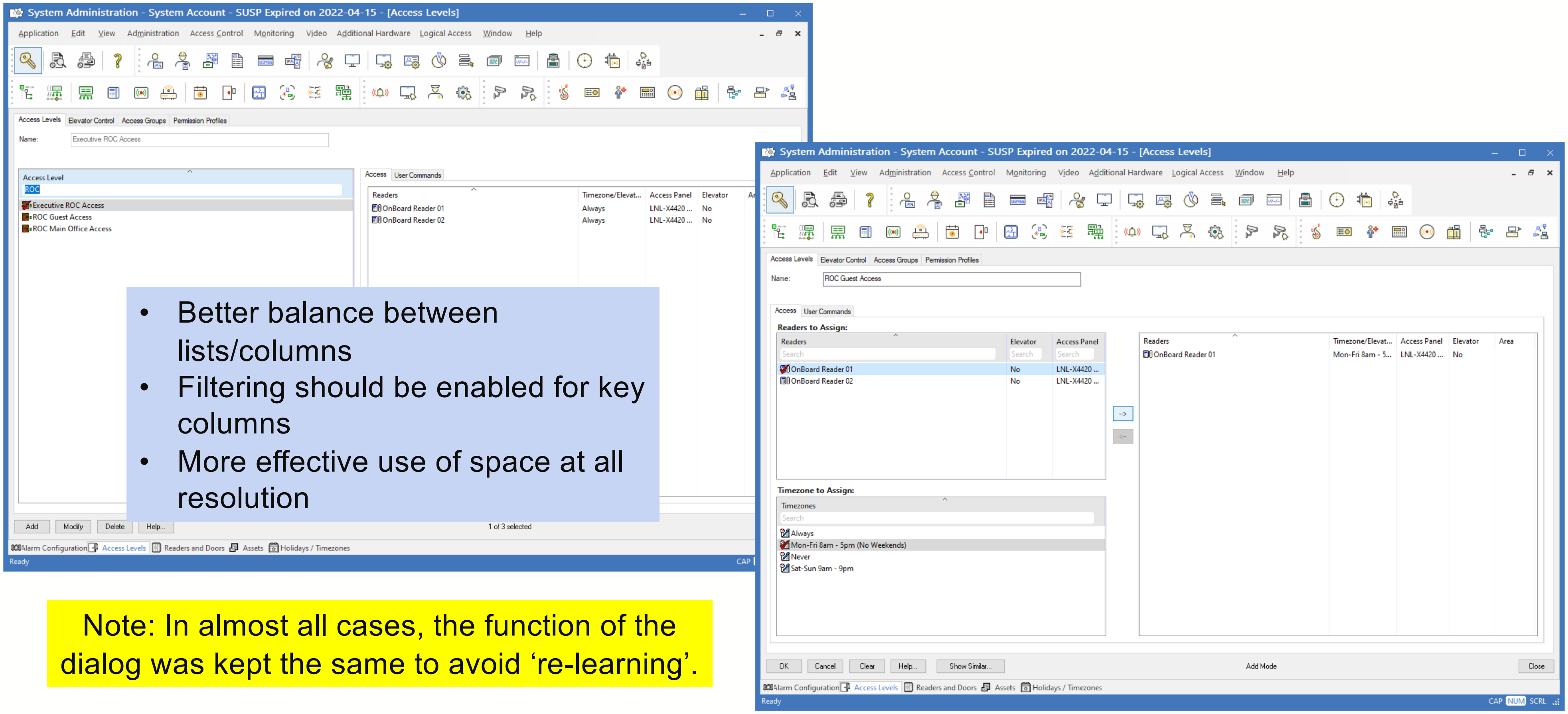
- Cafeteria Access
- Data Center- HQ (All)
- Data Center- University (All)
- Data Centers- All
- Emergency Level 1
- Emergency- Total Access
- Eng Labs- Computer Engineering
- Eng Labs- Mechanical
- Executive Offices
- First Responder
- Government Research Labs
- Government Research Offices
- Master
- Master All Access
- Office Building Perimeter doors
- Perimiter Access
- Pittsford HQ - Perimiter Access

Name: Emergency Level 1

Readers	Timezone/Eleva...	Access Panel	Elev...	Area

1 of 17 selected

OnGuard 8.2 Access Levels



Name: Executive ROC Access

Access Level
ROC
Executive ROC Access
ROC Guest Access
ROC Main Office Access

Readers	Timezone/Elevat...	Access Panel	Elevator
OnBoard Reader 01	Always	LNL-X4420 ...	No
OnBoard Reader 02	Always	LNL-X4420 ...	No

1 of 3 selected

Name: ROC Guest Access

Readers to Assign:

Readers	Elevator	Access Panel
OnBoard Reader 01	No	LNL-X4420 ...
OnBoard Reader 02	No	LNL-X4420 ...

Timezone to Assign:

Timezones
Always
Mon-Fri 8am - 5pm (No Weekends)
Never
Sat-Sun 9am - 9pm

Readers	Timezone/Elevat...	Access Panel	Elevator	Area
OnBoard Reader 01	Mon-Fri 8am - 5...	LNL-X4420 ...	No	

Add Mode

- Better balance between lists/columns
- Filtering should be enabled for key columns
- More effective use of space at all resolution

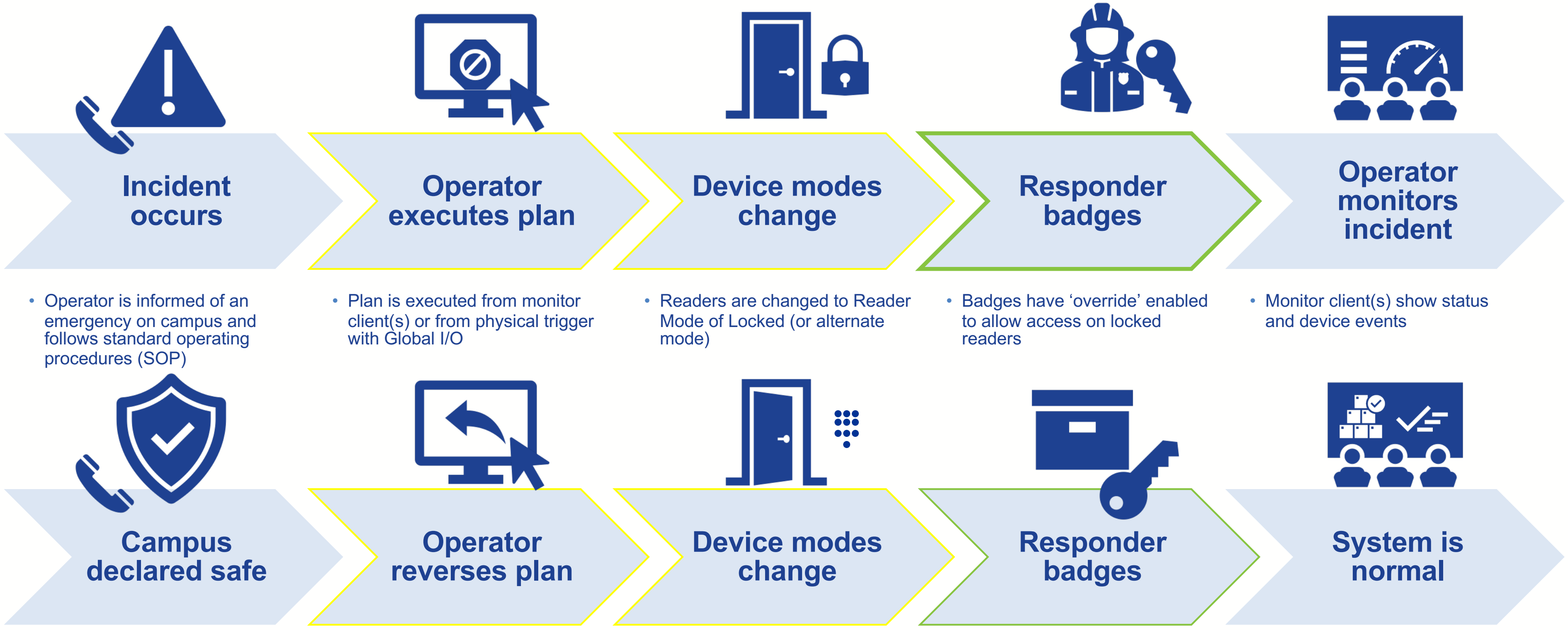
Note: In almost all cases, the function of the dialog was kept the same to avoid ‘re-learning’.

Badge Override of Locked Reader Mode

- Why?
  - At certain times, the system admin must change reader mode to locked
  - Some badges need to be able to continue to gain access through locked readers
  - Badge Override of Locked Reader Mode allows this functionality
- Works with online readers controlled by Mercury Hardware
- Requirements
  - Badge must have Lock Override Attribute enabled
  - Badge must have Active Access Level for Locked Reader
- Benefit
  - Emergency response improved

Incident Response and Resolution (Restore)

* Reminder from earlier discussions



Incident occurs

- Operator is informed of an emergency on campus and follows standard operating procedures (SOP)

Operator executes plan

- Plan is executed from monitor client(s) or from physical trigger with Global I/O

Device modes change

- Readers are changed to Reader Mode of Locked (or alternate mode)

Responder badges

- Badges have 'override' enabled to allow access on locked readers

Operator monitors incident

- Monitor client(s) show status and device events

Campus declared safe

- Operator receives all clear and follows SOP to return to normal operations

Operator reverses plan

- Plan is reversed from monitor client(s) or special trigger

Device modes change

- Readers are returned to their normally configured modes

Responder badges

- No changes to badges are required

System is normal

- Monitor client(s) show system is in typical operation
- Reporting and Auditing show who executed action plans

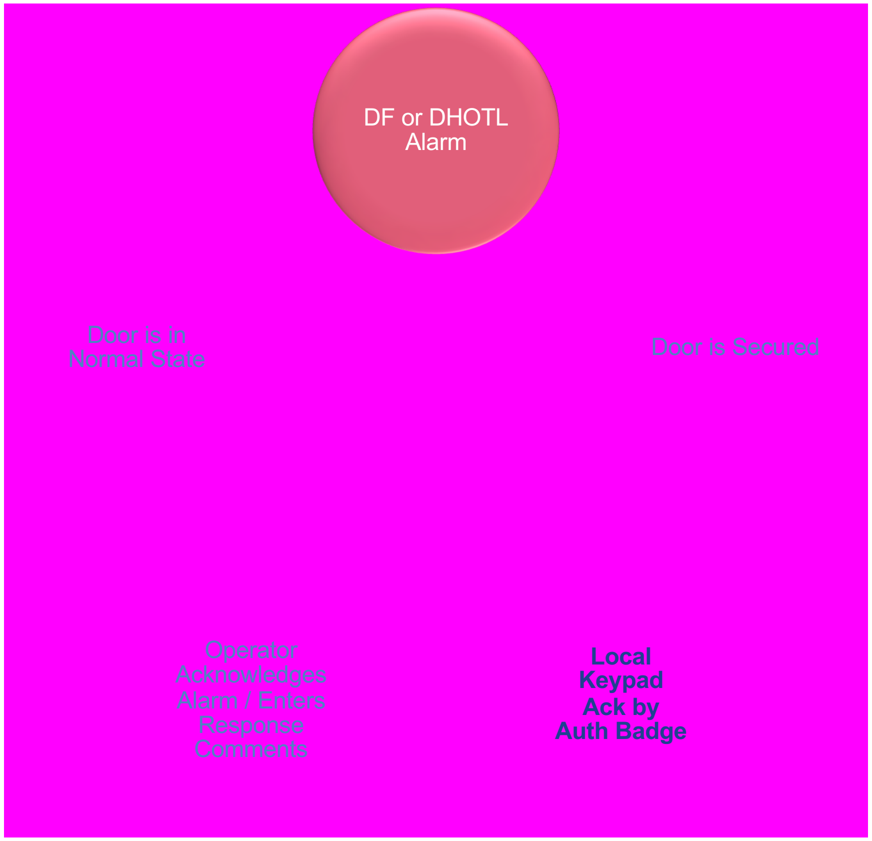
What is Action Plans (Lockdown) going to be…

- Main Operational component will be Device Groups for Readers
  - Provides a logical grouping of associated readers
  - Many customers already have groups of readers created in support of current efforts
- Reader Groups will have options to configure Lockdown
- Alarm Monitoring Device Groups will allow Activate/Restore of the Lockdown
  - Groups will also show Status of the Lockdown
- Specific Permissions will be created for Operators to Activate / Restore
  - Similar to Operator permissions for other ‘pairs’ to allow better control pf who can trigger these actions
    - Like; Mask / UnMask or Arm / Disarm

Keypad Alarm Response Required - Option

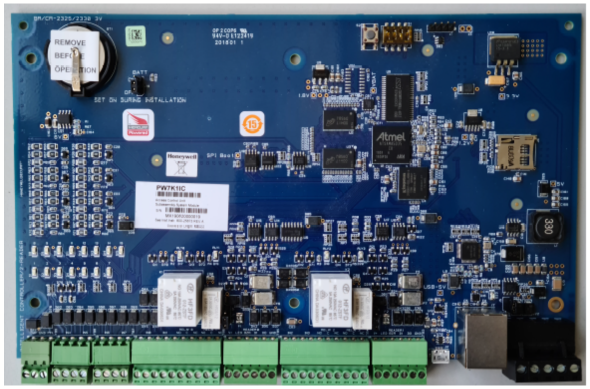
- Different Alarm Acknowledgement workflow available for doors that have keypad readers for
  - Door Forced Alarms
  - Door Held Open Too Long Alarms
- Acknowledge flow
  - Door Forced Alarm or Door Held Open Too Long Alarm occurs
  - Door is physically re-secured
  - Locally acknowledged (thru reader Keypad code) with authorized badge
  - Then Operator can acknowledge alarm in Alarm Monitoring Client (Thick or Thin)

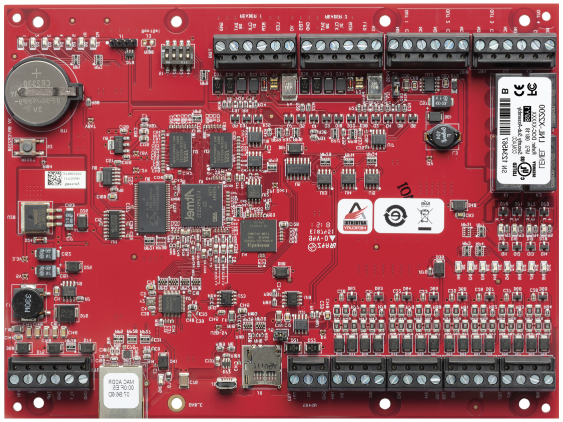
Audit trail of who locally acknowledged that the alarmed door was re-secured


DF or DHOTL Alarm
Door is in Normal State
Door is Secured
Operator Acknowledges Alarm / Enters Response Comments
Local Keypad Ack by Auth Badge

Support for Honeywell PW7000 Controllers and SIOs

- PW7K Controller = LNL-X2220 Controller
- PW7K SIOs = Series 3 SIOs
- Requirements:
  - Software Option License SWG-1640 is required for communications, it enables bi-lingual DLL
  - Proper OEM Mask, to allow Honeywell OEM Coded boards to communicate with OnGuard
- Benefits
  - Allows Honeywell hardware users to migrate to the OnGuard platform, preserving their investment in Honeywell hardware





Longer Descriptions for Aux Inputs and Aux Outputs

- Descriptions for Auxiliary Inputs and Outputs have been extended from 32 characters to 64 characters
- This change applies to Auxiliary Inputs and Outputs on Controllers and Reader Interface Boards
- Description definition in System Admin UI
- Displaying the longer descriptions in all Alarm Monitoring Clients & Reports

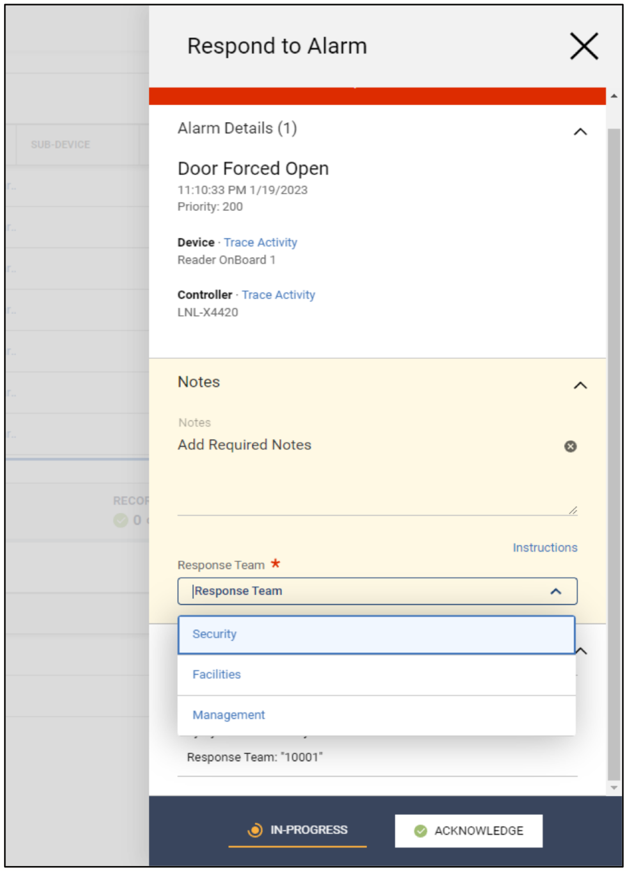
Extended descriptions can provide more context for operators and system admins.
Leads to increased responsiveness in operation, and understanding in historical reporting

User-Defined Fields for Alarm Response (ACK)

Allows Admins to define specific and predictable fields within their Alarm Response (Acknowledgement) process

- Customers wanted to include their own data fields in the Response/ACK process
  - Simple - what 'team' was dispatched in response to an Alarm
  - Specific – numeric or 'coded' fields to support their reporting or response metrics
- ACK UDF fields are displayed in Alarm Monitoring or OnGuard Monitor, on the same screens where you see ACK Notes
  - Use the 'Advanced Acknowledgement Report' to add your UDF's to the report (Advanced Reporting License required)
- Fields can be updated during In Progress or Acknowledgement
  - Required UDF Fields only affect the Acknowledgement

Reminder: UDF's are added to OnGuard using FormsDesigner and a FULL FormsDesigner License is required to do so.



Respond to Alarm

Alarm Details (1)

Door Forced Open
11:10:33 PM 1/19/2023
Priority: 200

Device · Trace Activity
Reader OnBoard 1

Controller · Trace Activity
LNL-X4420

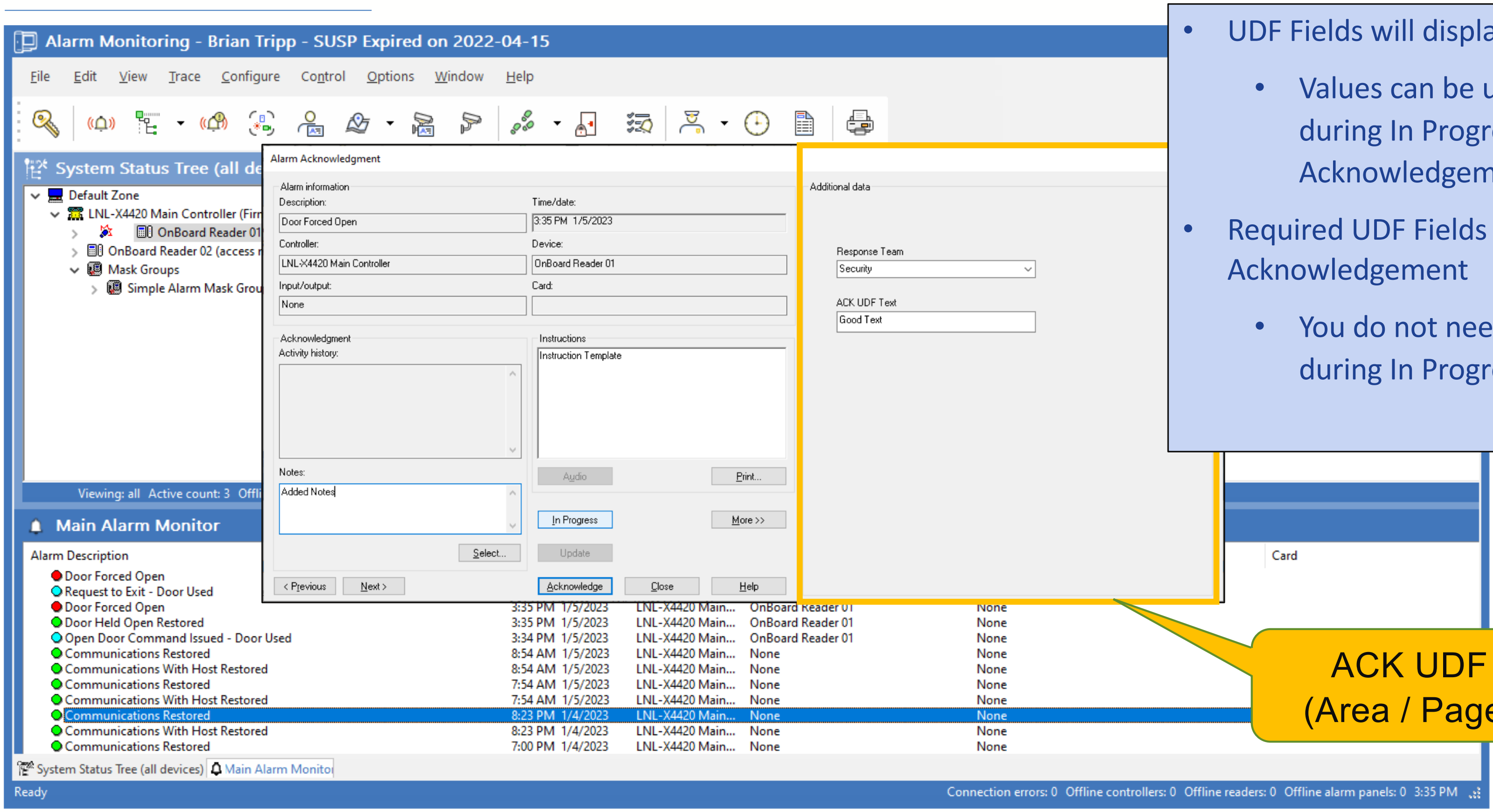
Notes

Notes: Add Required Notes

Response Team *: Response Team

Response Team: "10001"

Using ACK UDF Fields in Alarm Monitoring



Alarm Monitoring - Brian Tripp - SUSP Expired on 2022-04-15
File Edit View Trace Configure Control Options Window Help
System Status Tree (all de
Default Zone
LNL-X4420 Main Controller (Firr
OnBoard Reader 01
OnBoard Reader 02 (access r
Mask Groups
Simple Alarm Mask Grou
Viewing: all Active count: 3 Offli
Main Alarm Monitor
System Status Tree (all devices)
Main Alarm Monitor

Alarm Acknowledgment

Alarm information

Description: Door Forced Open

Time/date: 3:35 PM 1/5/2023

Controller: LNL-X4420 Main Controller

Device: OnBoard Reader 01

Input/output: None

Card:

Acknowledgment

Activity history:

Notes: Added Notes

Instructions

Instruction Template

Audio
Print...
Select...
In Progress
More >>
Update
< Previous
Next >
Acknowledge
Close
Help

Additional data

Response Team: Security

ACK UDF Text: Good Text

Alarm Description					Card
Door Forced Open					
Request to Exit - Door Used					
Door Forced Open	3:35 PM 1/5/2023	LNL-X4420 Main...	OnBoard Reader 01	None	
Door Held Open Restored	3:35 PM 1/5/2023	LNL-X4420 Main...	OnBoard Reader 01	None	
Open Door Command Issued - Door Used	3:34 PM 1/5/2023	LNL-X4420 Main...	OnBoard Reader 01	None	
Communications Restored	8:54 AM 1/5/2023	LNL-X4420 Main...	None	None	
Communications With Host Restored	8:54 AM 1/5/2023	LNL-X4420 Main...	None	None	
Communications Restored	7:54 AM 1/5/2023	LNL-X4420 Main...	None	None	
Communications With Host Restored	7:54 AM 1/5/2023	LNL-X4420 Main...	None	None	
Communications Restored	8:23 PM 1/4/2023	LNL-X4420 Main...	None	None	
Communications With Host Restored	8:23 PM 1/4/2023	LNL-X4420 Main...	None	None	
Communications Restored	7:00 PM 1/4/2023	LNL-X4420 Main...	None	None	

Ready

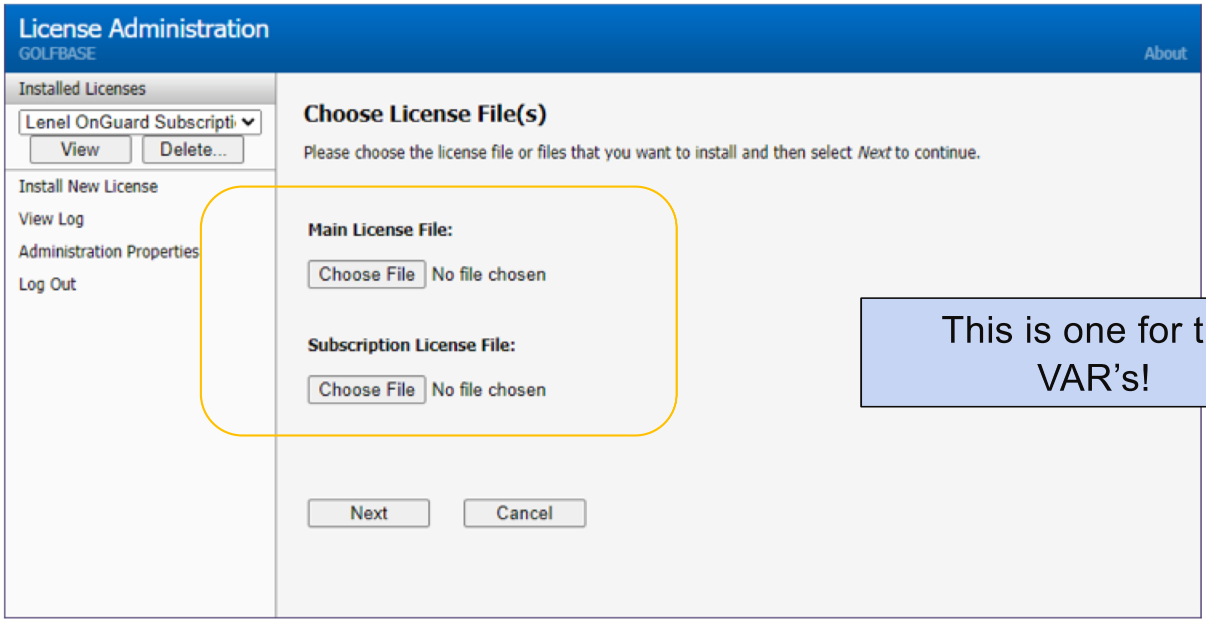
Connection errors: 0 Offline controllers: 0 Offline readers: 0 Offline alarm panels: 0 3:35 PM

- UDF Fields will display the latest value
  - Values can be updated/changed during In Progress, Update, or Acknowledgement
- Required UDF Fields only affect the Acknowledgement
  - You do not need to mark them during In Progress

ACK UDF
(Area / Page)

License Administration Updates

- License Administration now includes the ability to load BOTH the OnGuard Main and Subscription license files at the same time.
  - The screen where you browse to the license file now includes fields for selection of both
  - You do not have to load both, you can still do one or the other as well



Choose License File(s)

Please choose the license file or files that you want to install and then select *Next* to continue.

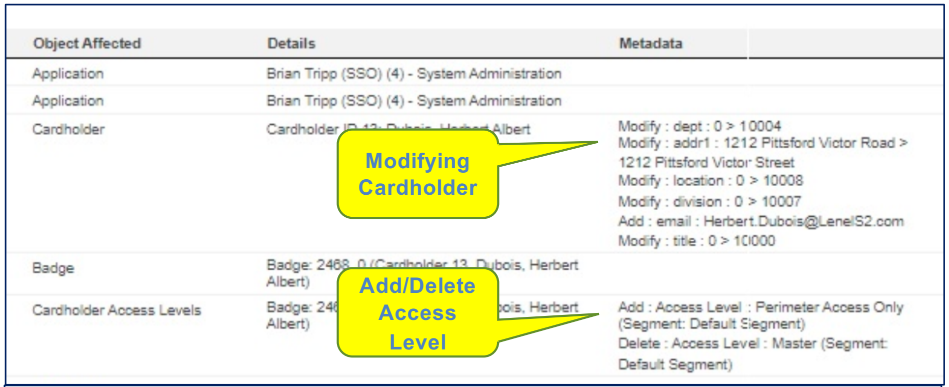
This is one for the VAR's!

Updates to User Transaction Auditing & Reporting

‘Core’ OnGuard pre/post auditing for the API is extended to include Badge Details

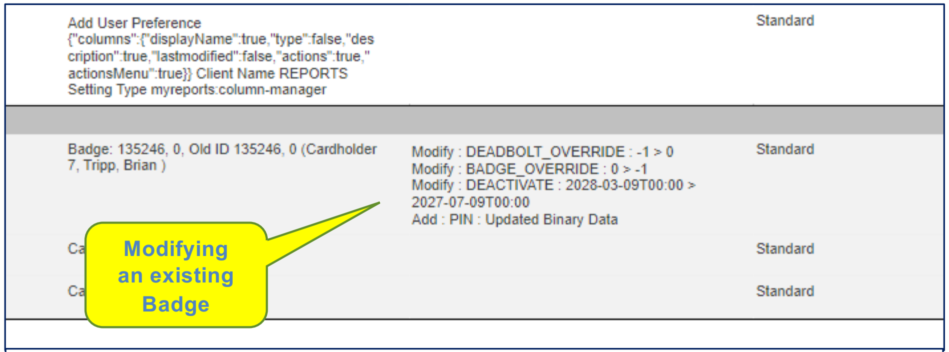
- Building on the 8.1 API Transaction effort
- Support for Badge Details added to ‘human readable’ metadata
- Audited fields [1] :
  - Cardholder Details
  - Badge Details
  - Access Level assignment
  - Access Level modifications
  - User Access Level assignments (for AAM)

[1]: While these user transaction updates were focused on transactions thru the API, these specific areas were updated thru the installed clients as well.



Object Affected	Details	Metadata	
Application	Brian Tripp (SSO) (4) - System Administration		
Application	Brian Tripp (SSO) (4) - System Administration		
Cardholder	Cardholder ID 13: Dubois, Herbert Albert	Modify : dept : 0 > 10004 Modify : addr1 : 1212 Pittsford Victor Road > 1212 Pittsford Victor Street Modify : location : 0 > 10008 Modify : division : 0 > 10007 Add : email : Herbert.Dubois@LenelS2.com Modify : title : 0 > 10000	
Badge	Badge: 2468, 0 (Cardholder 13, Dubois, Herbert Albert)		
Cardholder Access Levels	Badge: 246 ois, Herbert Albert)	Add : Access Level : Perimeter Access Only (Segment: Default Segment) Delete : Access Level : Master (Segment: Default Segment)	

Expanded User Transactions Report – Cardholder Example



Add User Preference {"columns":{"displayName":true,"type":false,"description":true,"lastmodified":false,"actions":true,"actionsMenu":true}} Client Name REPORTS Setting Type myreports:column-manager		Standard
Badge: 135246, 0, Old ID 135246, 0 (Cardholder 7, Tripp, Brian)	Modify : DEADBOLT_OVERRIDE : -1 > 0 Modify : BADGE_OVERRIDE : 0 > -1 Modify : DEACTIVATE : 2028-03-09T00:00 > 2027-07-09T00:00 Add : PIN : Updated Binary Data	Standard
Ca		Standard
Ca		Standard

Expanded User Transactions Report – Badge Example

3^{rd} Party Authentication – Client Credentials Flow

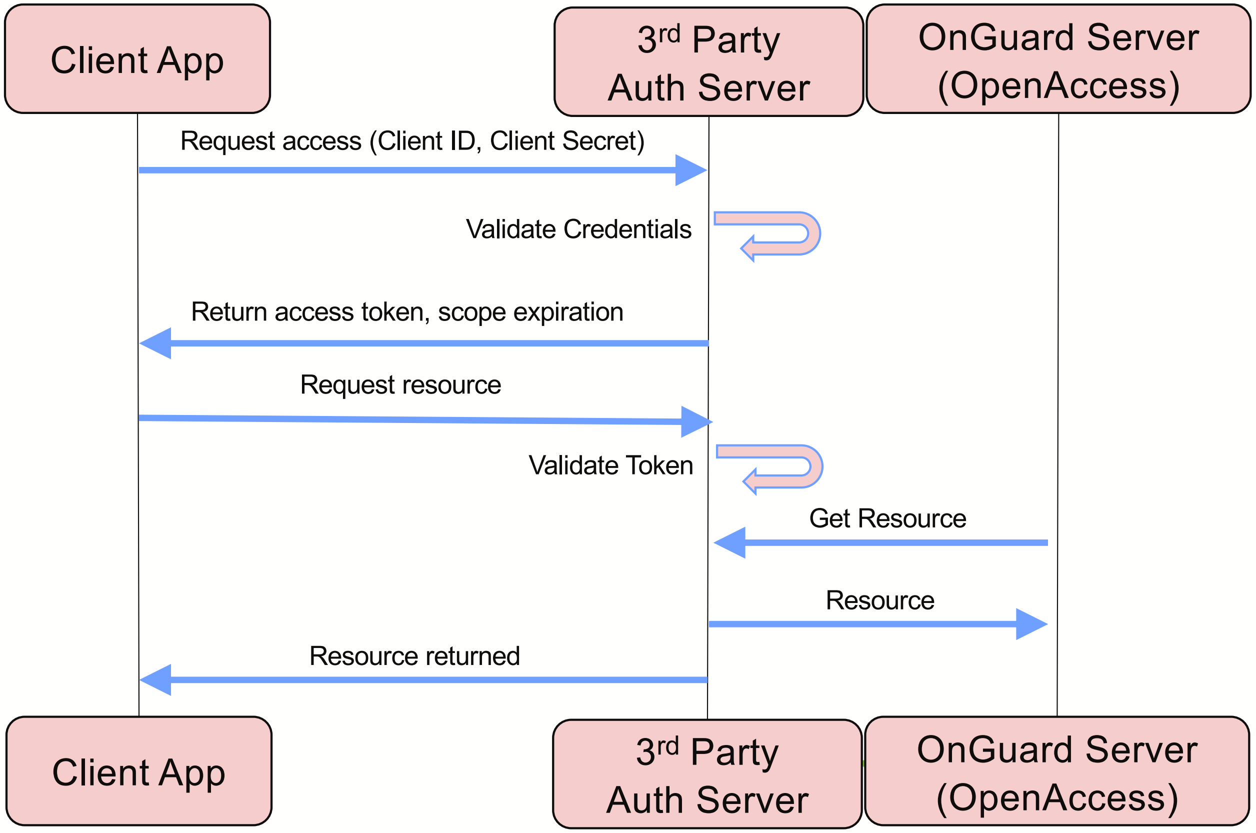
- What did we do?
  - Addressed the question: How does a 'service' log into OnGuard using 3^{rd} Party Authentication?
  - Added an OAuth option for this called 'Client Credentials Flow' to 3^{rd} Party Authentication

- Why did we do this?
  - Customers and Partners have the need for their integrations to be able to authenticate, and customers are pushing to have this authentication be done thru a 3^{rd} Party Provider
  - The current 3^{rd} Party Auth in OnGuard is very 'user centric' in that the browser goes out to the provider and the user enters their User/Pass there.
    - And a service cannot take that path

Support/Limitations – This option requires more support from the 3^{rd} Party Provider, and as with our OIDC support, not all providers will support the Client Credentials Flow. Validation for this support focused on Okta and Azure AD.

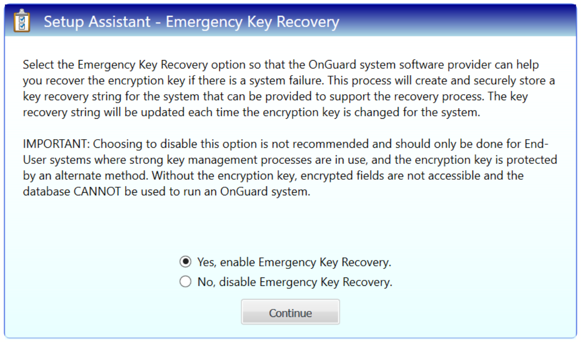
Client Credentials Flow

- This diagram is the basic flow of the process
- Credentials from the Partner App are validated by the 3rd Party
  - The login with them first
- When the token is sent to OnGuard for the request
  - We can validate the token using the 'Introspect Endpoint'
  - We can validate the token locally (harder to setup)
- After validation, the Client ID is used to connect the request to an OnGuard User Account



Cybersecurity Updates and Process

- Hardening Guide Updates for OnGuard 8.2
  - Now includes Revision History for the list of changes
  - Updates for TLS 1.3, Identified Ports, and more…
- OnGuard 8.2 has recent versions of NGINX, RabbitMQ/Erlang, Java OpenJDK
- Emergency Key Recovery option for 8.2 (& 8.1 Update 1)
  - Extends the Key Management/Encryption done in 8.1
  - Enabling this option allows LenelS2 (as the manufacturer) to assist with key recovery when NO OTHER OPTIONS are available
- TLS 1.3 support starts in OnGuard 8.2 for specific areas
  - Browser-based client delivery (supported by the NGINX web service)
  - LS Message Broker service (using RabbitMQ).
  - Some areas of OnGuard remain supported at TLS 1.2
  - Access Controllers support TLS 1.2 or 1.1 based on model



Setup Assistant - Emergency Key Recovery

Select the Emergency Key Recovery option so that the OnGuard system software provider can help you recover the encryption key if there is a system failure. This process will create and securely store a key recovery string for the system that can be provided to support the recovery process. The key recovery string will be updated each time the encryption key is changed for the system.

IMPORTANT: Choosing to disable this option is not recommended and should only be done for End-User systems where strong key management processes are in use, and the encryption key is protected by an alternate method. Without the encryption key, encrypted fields are not accessible and the database CANNOT be used to run an OnGuard system.

● Yes, enable Emergency Key Recovery.

○ No, disable Emergency Key Recovery.

TLS 1.3 changes provide better performance and stronger security, thru changes like a faster TLS handshake and more secure cipher suites.

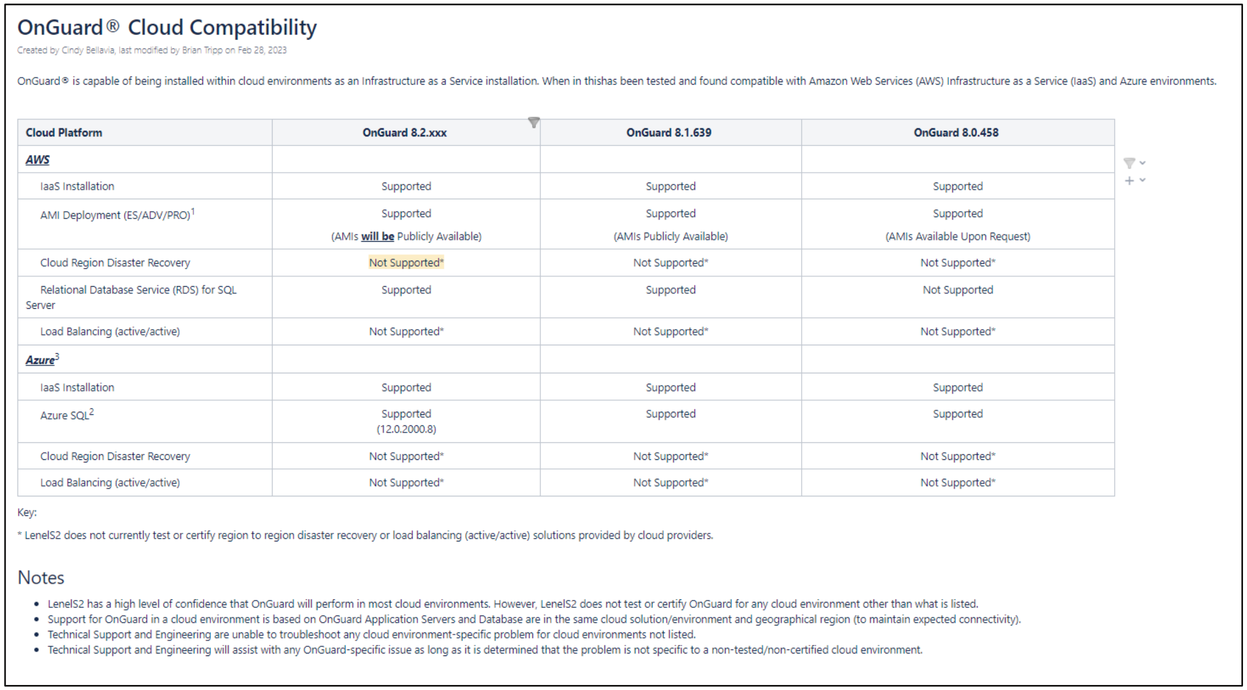
Cloud Platform Compatibility

- As we go thru the Beta, we will be looking to preview/review the upcoming Compatibility Chart for Cloud Platforms

- Listed compatibility for…
  - Azure
  - Azure SQL
  - AWS
  - Amazon RDS
    - Relational Database Service

Key notes and epxectations how OnGuard would be used in cloud environments

*Additional guidance would be included in the OnGuard Deployment Guide



OnGuard® Cloud Compatibility

Created by Cindy Bellavia, last modified by Brian Tripp on Feb 28, 2023

OnGuard® is capable of being installed within cloud environments as an Infrastructure as a Service installation. When in thishas been tested and found compatible with Amazon Web Services (AWS) Infrastructure as a Service (IaaS) and Azure environments.

Cloud Platform	OnGuard 8.2.xxx	OnGuard 8.1.639	OnGuard 8.0.458
AWS			
IaaS Installation	Supported	Supported	Supported
AMI Deployment (ES/ADV/PRO)[1]	Supported (AMIs **will be** Publicly Available)	Supported (AMIs Publicly Available)	Supported (AMIs Available Upon Request)
Cloud Region Disaster Recovery	Not Supported*	Not Supported*	Not Supported*
Relational Database Service (RDS) for SQL Server	Supported	Supported	Not Supported
Load Balancing (active/active)	Not Supported*	Not Supported*	Not Supported*
Azure[3]			
IaaS Installation	Supported	Supported	Supported
Azure SQL[2]	Supported (12.0.2000.8)	Supported	Supported
Cloud Region Disaster Recovery	Not Supported*	Not Supported*	Not Supported*
Load Balancing (active/active)	Not Supported*	Not Supported*	Not Supported*

Key:

* LenelS2 does not currently test or certify region to region disaster recovery or load balancing (active/active) solutions provided by cloud providers.

Notes

- LenelS2 has a high level of confidence that OnGuard will perform in most cloud environments. However, LenelS2 does not test or certify OnGuard for any cloud environment other than what is listed.
- Support for OnGuard in a cloud environment is based on OnGuard Application Servers and Database are in the same cloud solution/environment and geographical region (to maintain expected connectivity).
- Technical Support and Engineering are unable to troubleshoot any cloud environment-specific problem for cloud environments not listed.
- Technical Support and Engineering will assist with any OnGuard-specific issue as long as it is determined that the problem is not specific to a non-tested/non-certified cloud environment.

Documentation Topic

- OnGuard ‘Combined Compatibility Guide’ concept is being evaluated
  - VARs have requested that this become one guide
- From our POV this is a great suggestion/option to help Customers and VARs easily find what they need
- Benefits
  - Easier to download one document
  - Table of Contents as a guide
  - Standard organization of topics in the file…
    - OnGuard System, Hardware, Video, etc.
  - Search all the charts in one ‘Ctrl-f’ for what you need

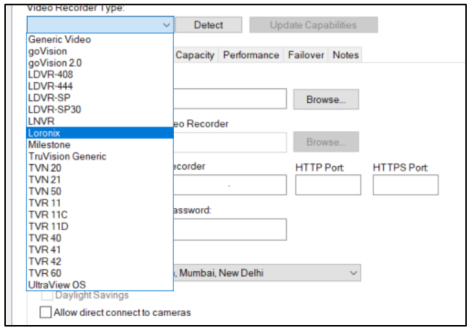
LENEL:S2

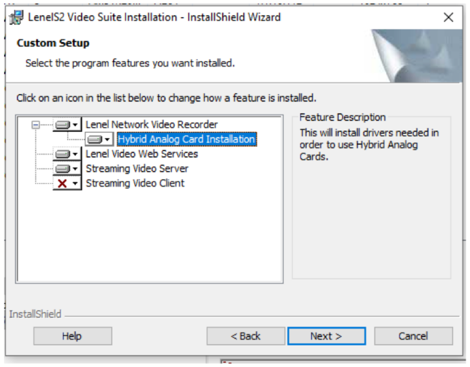
OnGuard®

OnGuard Compatibility Guide

EOL Video components

- Removing the following outdated and obsolete recorders
  - LDVR
  - Loronix
  - HNVR (Hybrid LNVR units aka "HVR")
- Removal of the standalone SKU for the card and LNVR that used them
  - Relevant PNs for these products are prefixed with:
    - “A16” 16-channel encoder
    - “A32” 32-channel encoder
- Removal of WVV and Intelligent Video
  - Web Video Viewer (the 2011 ISS Based Version)
  - Intelligent Video Server / Intelligent Video Application Server




LenelS2 Video Suite Installation - InstallShield Wizard

Custom Setup

Select the program features you want installed.

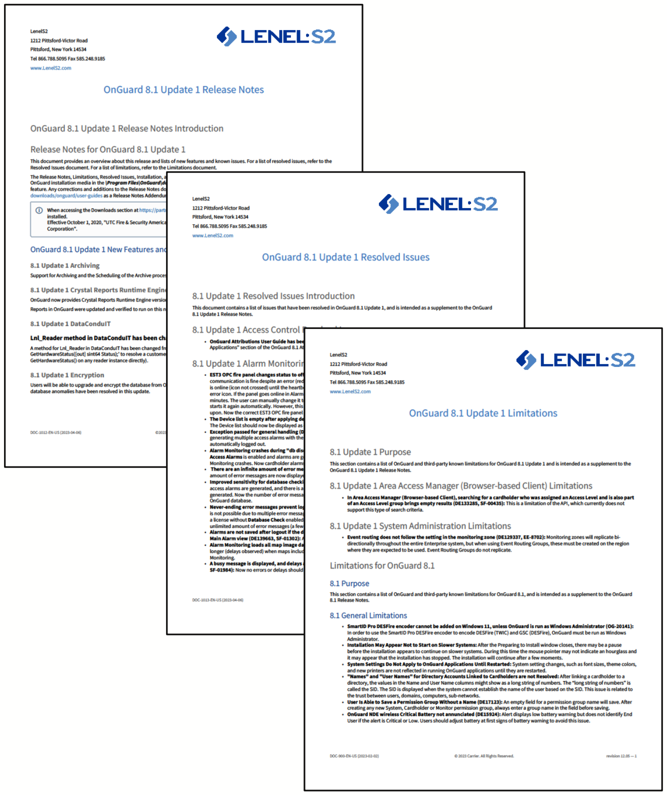
Click on an icon in the list below to change how a feature is installed.

Feature Description

This will install drivers needed in order to use Hybrid Analog Cards.

OnGuard 8.1 Update 1

- Finished our Health Check (gate) Review 4/18
- Currently in process to Partner Center
  - Release Memo up 4/24
  - Software Expected on our about 4/26
- Release Notes, Resolved Issues can be provided
  - SQL Azure Archiving (to DB)
  - Updated Crystal Reports
  - Emergency Key Recovery (Encrypted Fields)
  - OpenAccess from 8.2
    - Lnl_Cardholder paging
    - New Lnl_Badge.ModifyAccessLevelAssignment
  - 3rd Party Auth for SVCS (OAuth2 Client Credentials)
  - Custom Reports Service location
  - New NGINX, RabbitMQ, and Erlang



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

OnGuard 8.1 Update 1 Release Notes

OnGuard 8.1 Update 1 Release Notes Introduction

Release Notes for OnGuard 8.1 Update 1

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

The Release Notes, Limitations, Resolved Issues, Installation, a
OnGuard installation media in the \Program Files\OnGuard\d
feature. Any corrections and additions to the Release Notes do
downloads/onguard/user-guides as a Release Notes Addendu

ⓘ When accessing the Downloads section at https://part
installed.
Effective October 1, 2020, "UTC Fire & Security America
Corporation".

OnGuard 8.1 Update 1 New Features and

8.1 Update 1 Archiving

Support for Archiving and the Scheduling of the Archive proce

8.1 Update 1 Crystal Reports Runtime Engin

OnGuard now provides Crystal Reports Runtime Engine versio

Reports in OnGuard were updated and verified to run on this n

8.1 Update 1 DataConduIT

Lnl_Reader method in DataConduIT has been ch

A method for Lnl_Reader in DataConduIT has been changed fr
GetHardwareStatus([out] sint64 Status);' to resolve a custome
GetHardwareStatus() on any reader instance directly).

8.1 Update 1 Encryption

Users will be able to upgrade and encrypt the database from O
database anomalies have been resolved in this update.

DOC-1012-EN-US (2023-04-06) ©2023

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

OnGuard 8.1 Update 1 Resolved Issues

8.1 Update 1 Resolved Issues Introduction

This document contains a list of issues that have been resolved in OnGuard 8.1 Update 1, and is intended as a supplement to the OnGuard 8.1 Update 1 Release Notes.

8.1 Update 1 Access Control

- **OnGuard Attributions User Guide has bee**
  Applications" section of the OnGuard 8.1 A

8.1 Update 1 Alarm Monitorin

- **EST3 OPC fire panel changes status to of**
  communication is fine despite an error (red
  is online (icon not crossed) until the heartb
  error icon. If the panel goes online in Alarm
  minutes. The user can manually change it t
  starts it again automatically. However, this
  upon. Now the correct EST3 OPC fire panel
- **The Device list is empty after applying de**
  The Device list should now be displayed as
- **Exception passed for general handling (D**
  generating multiple access alarms with the
  automatically logged out.
- **Alarm Monitoring crashes during "db dis**
  Access Alarms is enabled and alarms are g
  Monitoring crashes. Now cardholder alarms
- **There are an infinite amount of error me**
  amount of error messages are now display
- **Improved sensitivity for database checki**
  access alarms are generated, and there is a
  generated. Now the number of error messa
  OnGuard database.
- **Never-ending error messages prevent log**
  is not possible due to multiple error messag
  a license without **Database Check** enabled
  unlimited amount of error messages (a few
- **Alarms are not saved after logout if the d**
  Main Alarm view (DE139663, SF-01302): A
- **Alarm Monitoring loads all map image da**
  longer (delays observed) when maps includ
  Monitoring.
- **A busy message is displayed, and delays a**
  SF-01984): Now no errors or delays should

DOC-1013-EN-US (2023-04-06)

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

OnGuard 8.1 Update 1 Limitations

8.1 Update 1 Purpose

This section contains a list of OnGuard and third-party known limitations for OnGuard 8.1 Update 1 and is intended as a supplement to the OnGuard 8.1 Update 1 Release Notes.

8.1 Update 1 Area Access Manager (Browser-based Client) Limitations

- **In Area Access Manager (Browser-based Client), searching for a cardholder who was assigned an Access Level and is also part of an Access Level group brings empty results (DE133285, SF-00435):** This is a limitation of the API, which currently does not support this type of search criteria.

8.1 Update 1 System Administration Limitations

- **Event routing does not follow the setting in the monitoring zone (DE129337, EE-8702):** Monitoring zones will replicate bi-directionally throughout the entire Enterprise system, but when using Event Routing Groups, these must be created on the region where they are expected to be used. Event Routing Groups do not replicate.

Limitations for OnGuard 8.1

8.1 Purpose

This section contains a list of OnGuard and third-party known limitations for OnGuard 8.1, and is intended as a supplement to the OnGuard 8.1 Release Notes.

8.1 General Limitations

- **SmartID Pro DESFire encoder cannot be added on Windows 11, unless OnGuard is run as Windows Administrator (OG-20141):** In order to use the SmartID Pro DESFire encoder to encode DESFire (TWIC) and GSC (DESFire), OnGuard must be run as Windows Administrator.
- **Installation May Appear Not to Start on Slower Systems:** 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.
- **System Settings Do Not Apply to OnGuard Applications Until Restarted:** System setting changes, such as font sizes, theme colors, and new printers are not reflected in running OnGuard applications until they are restarted.
- **"Names" and "User Names" for Directory Accounts Linked to Cardholders are not Resolved:** After linking a cardholder to a directory, the values in the Name and User Name columns might show as a long string of numbers. The "long string of numbers" is called the SID. 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.
- **User Is Able to Save a Permission Group Without a Name (DE17123):** An empty field for a permission group name will save. After creating any new System, Cardholder or Monitor permission group, always enter a group name in the field before saving.
- **OnGuard NDE wireless Critical Battery not annunciated (DE15924):** Alert displays low battery warning but does not identify End User if the alert is Critical or Low. Users should adjust battery at first signs of battery warning to avoid this issue.

DOC-900-EN-US (2023-02-02) © 2023 Carrier. All Rights Reserved. revision 12.05 — 1

Questions and Answers

?? Q&A ??

My Questions to you as OnGuard Users…

1. **What problems are you trying to solve?**

2. **What are your thoughts on our Release Timing?**
   - Major Releases?
   - Update 1 – at 6 months
   - Update 2 - at 9 months (15 total)
   - Update 3 – at 9 months (24 total)
   - End of Support – at 3 Years from Release

3. **When do you remove a Cardholder?**
   - What qualities of that Cardholder indicate you can take them out of OnGuard?

LENEL·S2

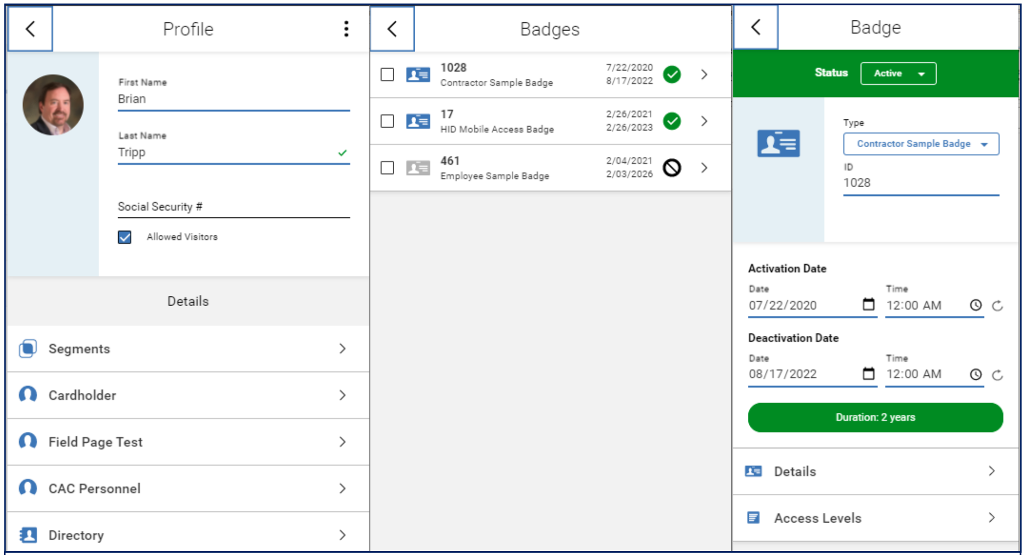
Thank you for your attention!

(And for having me back again ☺)

Credentials Refresh

Our ‘oldest’ browser client refreshed with our ‘latest’ user experience, includes enhanced support and usability/accessibility updates for a better user experience

- New Search Methods
- Improved support of cardholder segmentation (Primary / Additional)
- Action to bulk change segments
- Updated editing commands in Photo Capture
- Local Printer Management
- Improvements to accessibility (AD 508), clarity, and usability



First Name: Brian
Last Name: Tripp ✓
Social Security #
☑ Allowed Visitors

□	1028 Contractor Sample Badge	7/22/2020 8/17/2022	✓	>
□	17 HID Mobile Access Badge	2/26/2021 2/26/2023	✓	>
□	461 Employee Sample Badge	2/04/2021 2/03/2026	⦸	>

Status: Active
Type: Contractor Sample Badge
ID: 1028

Activation Date
Date: 07/22/2020 Time: 12:00 AM

Deactivation Date
Date: 08/17/2022 Time: 12:00 AM

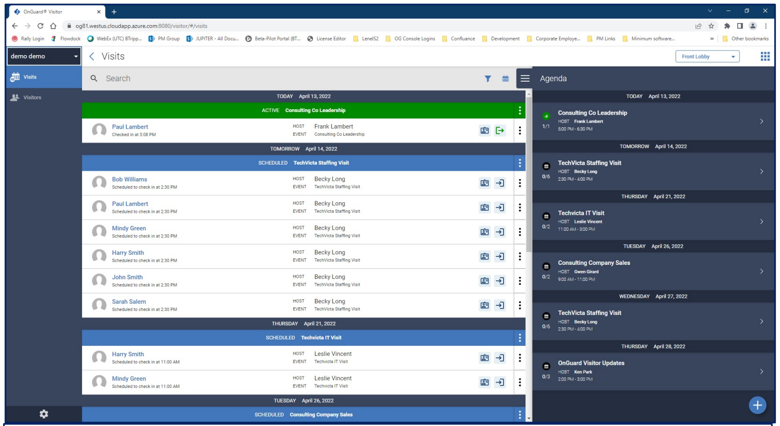
Duration: 2 years

Detail screens allow the operator to ‘go as deep as needed’ to understand and adjust the cardholders record in the system

Visitor

Provides a flexible tool for checking in visitors, managing visitor badges and access levels, engaging groups, capturing visitor photos, and printing badges

- Manage of Visitor Badges and Access Levels
- Bulk Visitor enrollment
- Export Visitor Accepted / Viewed documents
- Alignment of Visit Status between Visitor and 'Thick' Visitor Management
- Printer assignments management
- Usability / consistency enhancements
- Control of visitor system settings



Visits

TODAY April 13, 2022

ACTIVE Consulting Co Leadership

Visitor		
Paul Lambert Checked in at 3:08 PM	HOST EVENT	Frank Lambert Consulting Co Leadership

TOMORROW April 14, 2022

SCHEDULED TechVicta Staffing Visit

Visitor		
Bob Williams Scheduled to check in at 2:30 PM	HOST EVENT	Becky Long TechVicta Staffing Visit
Paul Lambert Scheduled to check in at 2:30 PM	HOST EVENT	Becky Long TechVicta Staffing Visit
Mindy Green Scheduled to check in at 2:30 PM	HOST EVENT	Becky Long TechVicta Staffing Visit
Harry Smith Scheduled to check in at 2:30 PM	HOST EVENT	Becky Long TechVicta Staffing Visit
John Smith Scheduled to check in at 2:30 PM	HOST EVENT	Becky Long TechVicta Staffing Visit
Sarah Salem Scheduled to check in at 2:30 PM	HOST EVENT	Becky Long TechVicta Staffing Visit

THURSDAY April 21, 2022

SCHEDULED Techvicta IT Visit

Visitor		
Harry Smith Scheduled to check in at 11:00 AM	HOST EVENT	Leslie Vincent Techvicta IT Visit
Mindy Green Scheduled to check in at 11:00 AM	HOST EVENT	Leslie Vincent Techvicta IT Visit

TUESDAY April 26, 2022

SCHEDULED Consulting Company Sales

Agenda

TODAY April 13, 2022
- 1/1 Consulting Co Leadership — HOST Frank Lambert — 5:00 PM - 6:30 PM

TOMORROW April 14, 2022
- 0/6 TechVicta Staffing Visit — HOST Becky Long — 2:30 PM - 4:00 PM

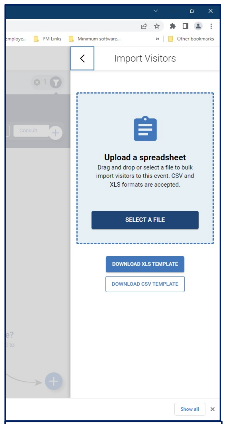
THURSDAY April 21, 2022
- 0/2 Techvicta IT Visit — HOST Leslie Vincent — 11:00 AM - 3:00 PM

TUESDAY April 26, 2022
- 0/2 Consulting Company Sales — HOST Gwen Girard — 9:00 AM - 11:00 PM

WEDNESDAY April 27, 2022
- 0/6 TechVicta Staffing Visit — HOST Becky Long — 2:30 PM - 4:00 PM

THURSDAY April 28, 2022
- 0/3 OnGuard Visitor Updates — HOST Ken Park — 2:00 PM - 3:00 PM

Visit Status and Agenda by Sign-In Location help plan the front desk attendants day…

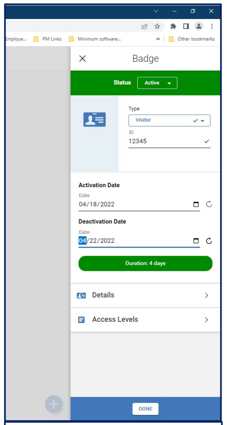


Import Visitors

Upload a spreadsheet

Drag and drop or select a file to bulk import visitors to this event. CSV and XLS formats are accepted.

Bulk Import Process



Badge

Status: Active

Type: Visitor

ID: 12345

Activation Date

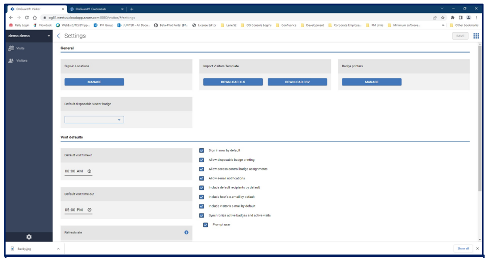
Date: 04/18/2022

Deactivation Date

Date: 04/22/2022

Duration: 4 days

Badge Detail Screen



Settings

General

Sign-in Locations

Import Visitors Template

Badge printers

Default disposable Visitor badge

Visit defaults

Default visit time-in: 08:00 AM

Default visit time-out: 05:00 PM

Refresh rate

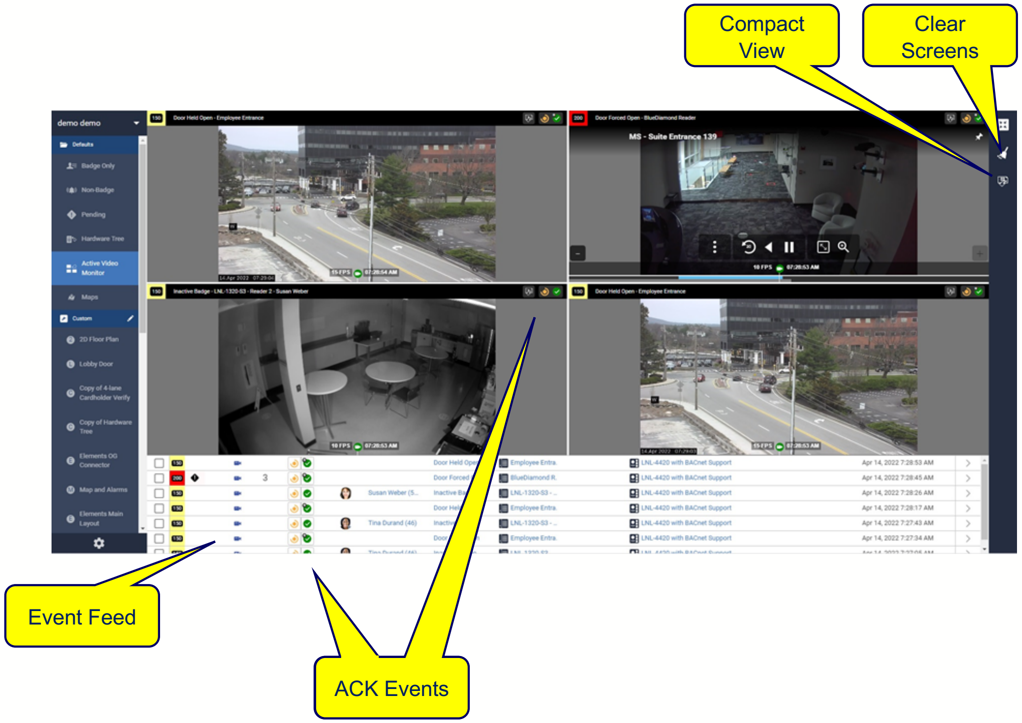
- ☑ Sign in now by default
- ☑ Allow disposable badge printing
- ☑ Allow access control badge assignments
- ☑ Allow e-mail notifications
- ☑ Include default recipients by default
- ☑ Include host's e-email by default
- ☑ Include visitor's e-mail by default
- ☑ Synchronize active badges and active visits
  - ☑ Prompt user

Visitor settings offer key administration options within the browser client

Monitor: Active Video Monitor (Video Hot Tile)

Interactive display and management of incoming video linked to priority alarms for improved visualization & responsiveness

- Active Video Monitor allows quick access to view video of active alarms and events.
- Dedicated page for viewing event video only
  - Event video is pushed to the viewer first in first out.
  - Acknowledge in the video tile of event feed
  - Pre-configured widget or build custom layouts



□	150					Door Held Ope	Employee Entra.	LNL-4420 with BACnet Support	Apr 14, 2022 7:28:53 AM
□	200		3			Door Forced	BlueDiamond R.	LNL-4420 with BACnet Support	Apr 14, 2022 7:28:45 AM
□	150				Susan Weber (5...	Inactive Ba	LNL-1320-S3 - ...	LNL-4420 with BACnet Support	Apr 14, 2022 7:28:26 AM
□	150					Door Hel	Employee Entra.	LNL-4420 with BACnet Support	Apr 14, 2022 7:28:17 AM
□	150				Tina Durand (46)	Inactiv	LNL-1320-S3 - ...	LNL-4420 with BACnet Support	Apr 14, 2022 7:27:43 AM
□	150					Door	Employee Entra.	LNL-4420 with BACnet Support	Apr 14, 2022 7:27:34 AM

Compact View

Clear Screens

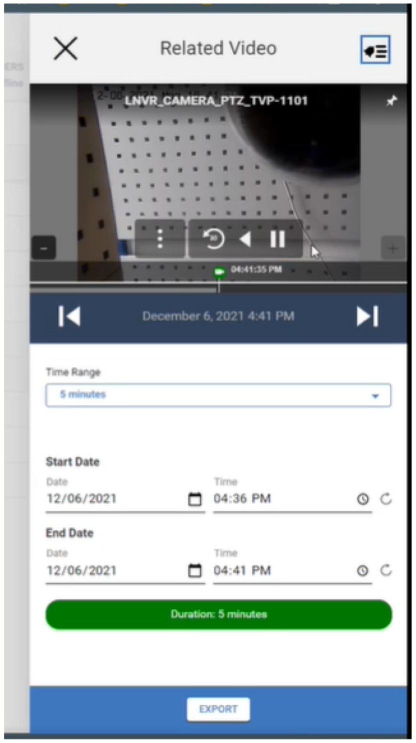
Event Feed

ACK Events

Monitor: Video Export

Quickly and easily share video clips with others inside or outside of the security environment

- Video is exported to browser in MP4 format
- Download up to 4 clips simultaneously
- Clip duration can be custom set or use value from the pulldown menu
- Maximum clip duration is 1 hour
- Export from several different screens, Hardware tree, Widget, Active Video Monitor



Time Range: 5 minutes

Start Date
Date: 12/06/2021
Time: 04:36 PM

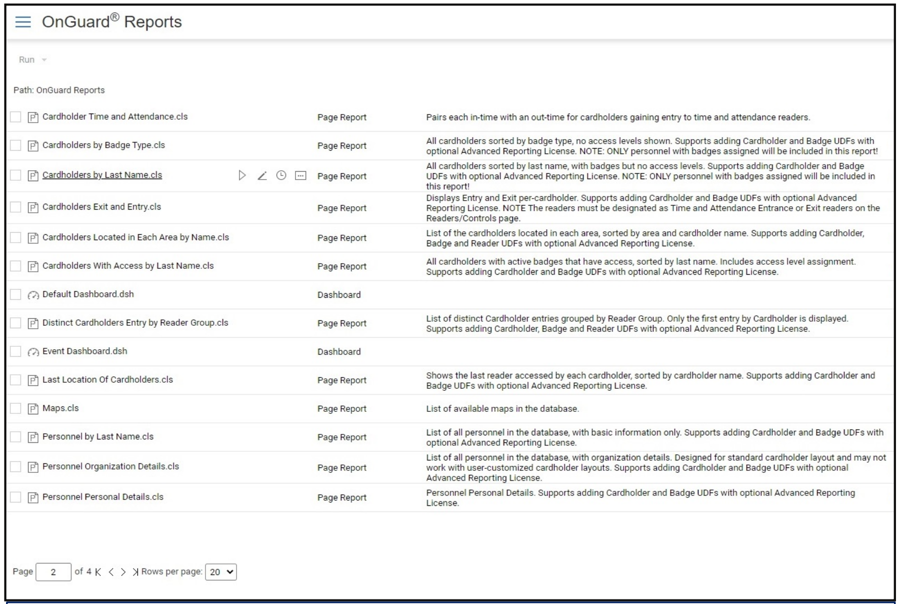
End Date
Date: 12/06/2021
Time: 04:41 PM

Duration: 5 minutes

Reporting and Dashboards Enhancements

More Enterprise users can now move from Crystal Reports and take advantage of browser-based reporting

- Support available for Enterprise systems
  - Can be used at the Region or Global ('Master') Servers
- Extended and Enhanced Reports and Dashboards
  - 20+ new reports (based on Crystal equivalents)
  - Several totally new reports
  - Most existing 8.0 reports have been updated
  - New and updated dashboards



OnGuard® Reports

Path: OnGuard Reports

□ Cardholder Time and Attendance.cls	Page Report	Pairs each in-time with an out-time for cardholders gaining entry to time and attendance readers.
□ Cardholders by Badge Type.cls	Page Report	All cardholders sorted by badge type, no access levels shown. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License. NOTE: ONLY personnel with badges assigned will be included in this report!
□ Cardholders by Last Name.cls	Page Report	All cardholders sorted by last name, with badges but no access levels. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License. NOTE: ONLY personnel with badges assigned will be included in this report!
□ Cardholders Exit and Entry.cls	Page Report	Displays Entry and Exit per-cardholder. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License. NOTE The readers must be designated as Time and Attendance Entrance or Exit readers on the Readers/Controls page.
□ Cardholders Located in Each Area by Name.cls	Page Report	List of the cardholders located in each area, sorted by area and cardholder name. Supports adding Cardholder, Badge and Reader UDFs with optional Advanced Reporting License.
□ Cardholders With Access by Last Name.cls	Page Report	All cardholders with active badges that have access, sorted by last name. Includes access level assignment. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
□ Default Dashboard.dsh	Dashboard	
□ Distinct Cardholders Entry by Reader Group.cls	Page Report	List of distinct Cardholder entries grouped by Reader Group. Only the first entry by Cardholder is displayed. Supports adding Cardholder, Badge and Reader UDFs with optional Advanced Reporting License.
□ Event Dashboard.dsh	Dashboard	
□ Last Location Of Cardholders.cls	Page Report	Shows the last reader accessed by each cardholder, sorted by cardholder name. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
□ Maps.cls	Page Report	List of available maps in the database.
□ Personnel by Last Name.cls	Page Report	List of all personnel in the database, with basic information only. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
□ Personnel Organization Details.cls	Page Report	List of all personnel in the database, with organization details. Designed for standard cardholder layout and may not work with user-customized cardholder layouts. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
□ Personnel Personal Details.cls	Page Report	Personnel Personal Details. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.

Page 2 of 4 Rows per page: 20

Reports list and added descriptions make it much easier to select the reports suited to the operator's needs.

- New "Export View" for many reports to deliver 1 record/row and 1 row/record in Excel or CSV
- No report replication – custom reports can be manually copied

Slide from our 8.1 Beta/Pilot Effort

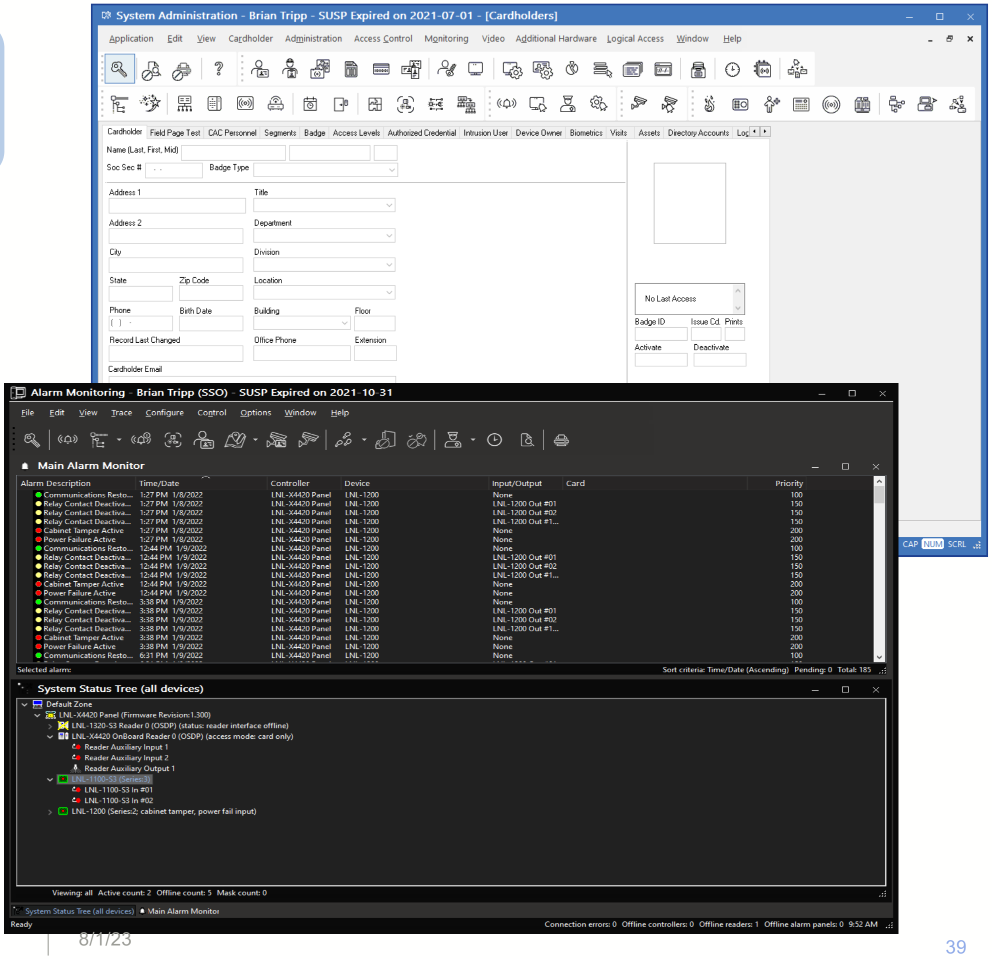
Examples of ‘new’ reports in OnGuard

Name	Type	Description
Active Badges Without Access Level Assignments	Page Report	Listing of each Access Level by Segment, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded to each segment. This report only works on a system using Segmentation. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
Advanced Badges Report	Page Report	Primarily designed for systems with the Advanced Reporting license. List of Badges for Cardholders and/or Visitors with Badge Type, Status and Activate and Deactivate Dates. Landscape layout with an empty space to allow adding more columns. Supports adding Cardholder, Visitor and Badge UDFs with optional Advanced Reporting License.
Advanced Visitor Report	Page Report	Primarily designed for systems with the Advanced Reporting license. List of Visitors sorted alphabetically with last visit information. Supports adding Visitor UDFs with optional Advanced Reporting License.
Advanced Visits Report	Page Report	Primarily designed for systems with the Advanced Reporting license. List of visits by date, newest first, with visit details. Supports adding Visit, Visitor, Host (Cardholder) and Badge UDFs with optional Advanced Reporting License.
Badge Expiration Report	Page Report	List of Badges expiring in less than specified number of days before and after today's date. Can be used to determine which Badges may need to be updated or purged based on recent or upcoming expiration. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
Badges Not Used In X Days Or More	Page Report	List of Badges not used in more than specified number of days before today's date. Can be used to determine which Badges may need to be updated or purged based on lack of use. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
Cardholder Record Activity Report	Page Report	List of Cardholder records inactive for more than specified number of days. Can be used to determine which Cardholder records may need to be purged based on days of inactivity. Supports adding Cardholder and Badge UDFs with optional Advanced Reporting License.
Distinct Cardholders Entry by Reader Group	Page Report	List of distinct Cardholder entries grouped by Reader Group. Only the first entry by Cardholder is displayed. Supports adding Cardholder, Badge and Reader UDFs with optional Advanced Reporting License. Supports adding Cardholder, Badge and Readers UDFs with optional Advanced Reporting License.
User Transaction Log (Expanded) by User ID	Page Report	Chronological log of all transactions performed, grouped by User ID, includes additional details, transaction grouping, and metadata.
User Transaction Log (Expanded)	Page Report	Chronological log of all transactions performed on the system by users, includes additional details, transaction grouping, and metadata.
Visitor Record Activity Report	Page Report	List of Visitor records inactive for more than specified number of days. Can be used to determine which Visitor records may need to be purged based on days of inactivity. Supports adding Visitor UDFs with optional Advanced Reporting License.
Cardholder Dashboard	Dashboard	Displays cardholder record and badge record activity, low usage access levels, and badges expiring soon.

Windows Client Refresh

Modernized user interfaces reduce eye strain and enhance energy efficiency

- Familiar functionality with updated look-and-feel require no operator re-training
- Refreshed User Experience for Alarm Monitoring and System Administration
- Common changes to Colors, Shapes, Icons, Borders and Toolbars
    - No changes to 'Device/Status' Icons
- Addition of 'Dark Mode' to Alarm Monitoring


System Administration - Brian Tripp - SUSP Expired on 2021-07-01 - [Cardholders]
Application Edit View Cardholder Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
Cardholder Field Page Test CAC Personnel Segments Badge Access Levels Authorized Credential Intrusion User Device Owner Biometrics Visits Assets Directory Accounts Log
Name (Last, First, Mid)
Soc Sec #
Badge Type
Address 1
Title
Address 2
Department
City
Division
State
Zip Code
Location
Phone
Birth Date
Building
Floor
Record Last Changed
Office Phone
Extension
Cardholder Email
No Last Access
Badge ID
Issue Cd.
Prints
Activate
Deactivate
CAP NUM SCRL
Alarm Monitoring - Brian Tripp (SSO) - SUSP Expired on 2021-10-31
File Edit View Trace Configure Control Options Window Help

Main Alarm Monitor

Alarm Description	Time/Date	Controller	Device	Input/Output	Card	Priority
🟢 Communications Resto...	1:27 PM 1/8/2022	LNL-X4420 Panel	LNL-1200	None		100
🟡 Relay Contact Deactiva...	1:27 PM 1/8/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #01		150
🟡 Relay Contact Deactiva...	1:27 PM 1/8/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #02		150
🟡 Relay Contact Deactiva...	1:27 PM 1/8/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #1...		150
🔴 Cabinet Tamper Active	1:27 PM 1/8/2022	LNL-X4420 Panel	LNL-1200	None		200
🔴 Power Failure Active	1:27 PM 1/8/2022	LNL-X4420 Panel	LNL-1200	None		200
🟢 Communications Resto...	12:44 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		100
🟡 Relay Contact Deactiva...	12:44 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #01		150
🟡 Relay Contact Deactiva...	12:44 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #02		150
🟡 Relay Contact Deactiva...	12:44 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #1...		150
🔴 Cabinet Tamper Active	12:44 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		200
🔴 Power Failure Active	12:44 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		200
🟢 Communications Resto...	3:38 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		100
🟡 Relay Contact Deactiva...	3:38 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #01		150
🟡 Relay Contact Deactiva...	3:38 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #02		150
🟡 Relay Contact Deactiva...	3:38 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	LNL-1200 Out #1...		150
🔴 Cabinet Tamper Active	3:38 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		200
🔴 Power Failure Active	3:38 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		200
🟢 Communications Resto...	6:31 PM 1/9/2022	LNL-X4420 Panel	LNL-1200	None		100

Selected alarm:

Sort criteria: Time/Date (Ascending) Pending: 0 Total: 185

System Status Tree (all devices)

```
Default Zone
  LNL-X4420 Panel (Firmware Revision:1.300)
    LNL-1320-S3 Reader 0 (OSDP) (status: reader interface offline)
    LNL-X4420 OnBoard Reader 0 (OSDP) (access mode: card only)
      Reader Auxiliary Input 1
      Reader Auxiliary Input 2
      Reader Auxiliary Output 1
    LNL-1100-S3 (Series:3)
      LNL-1100-S3 In #01
      LNL-1100-S3 In #02
    LNL-1200 (Series:2; cabinet tamper, power fail input)
```

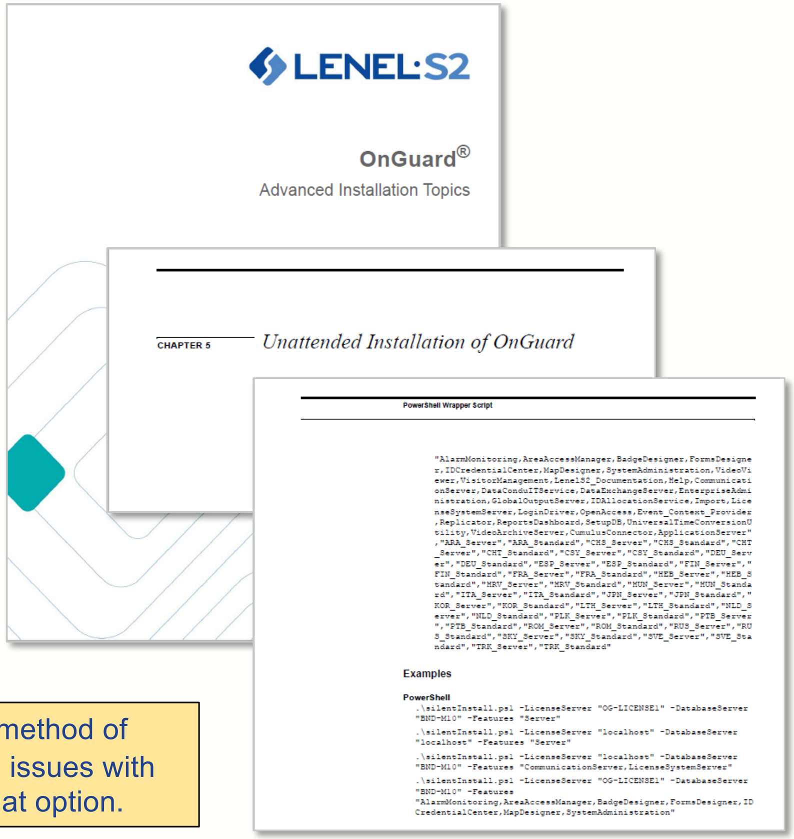
Viewing: all Active count: 2 Offline count: 5 Mask count: 0

Connection errors: 0 Offline controllers: 0 Offline readers: 1 Offline alarm panels: 0 9:52 AM

Silent / Scripted Server or Client Installation

Allows OnGuard to be installed using more IT-centric methodologies

- Allows the OnGuard Server to be installed without user interaction
  - Adds to Silent Client installation enabled in 8.0
- Key to automating cloud-based installations
- Includes sample Powershell scripts
- Replaces the ‘Client Update’ process that used to be in the Advanced Installation Guide



LENEL:S2

OnGuard®
Advanced Installation Topics

CHAPTER 5 *Unattended Installation of OnGuard*

PowerShell Wrapper Script

```
"AlarmMonitoring,AreaAccessManager,BadgeDesigner,FormsDesigne
r,IDCredentialCenter,MapDesigner,SystemAdministration,VideoVi
ewer,VisitorManagement,LenelS2_Documentation,Help,Communicati
onServer,DataConduITService,DataExchangeServer,EnterpriseAdmi
nistration,GlobalOutputServer,IDAllocationService,Import,Lice
nseSystemServer,LoginDriver,OpenAccess,Event_Content_Provider
,Replicator,ReportsDashboard,SetupDB,UniversalTimeConversionU
tility,VideoArchiveServer,CumulusConnector,ApplicationServer"
,"ARA_Server","ARA_Standard","CHS_Server","CHS_Standard","CHT
_Server","CHT_Standard","CSY_Server","CSY_Standard","DEU_Serv
er","DEU_Standard","ESP_Server","ESP_Standard","FIN_Server","
FIN_Standard","FRA_Server","FRA_Standard","HEB_Server","HEB_S
tandard","HRV_Server","HRV_Standard","HUN_Server","HUN_Standa
rd","ITA_Server","ITA_Standard","JPN_Server","JPN_Standard","
KOR_Server","KOR_Standard","LTH_Server","LTH_Standard","NLD_S
erver","NLD_Standard","PLK_Server","PLK_Standard","PTB_Server
","PTB_Standard","ROM_Server","ROM_Standard","RUS_Server","RU
S_Standard","SKY_Server","SKY_Standard","SVE_Server","SVE_Sta
ndard","TRK_Server","TRK_Standard"
```

Examples

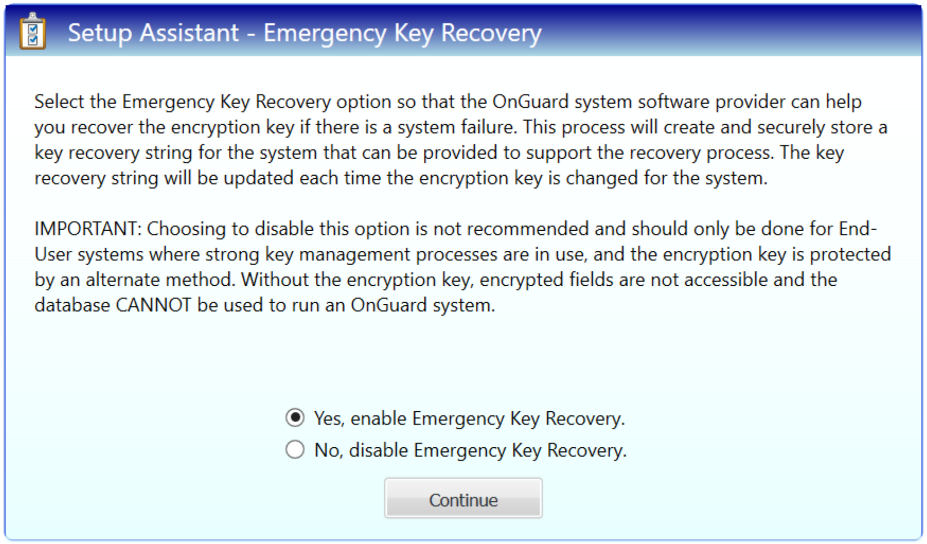
PowerShell

```
.\silentInstall.ps1 -LicenseServer "OG-LICENSE1" -DatabaseServer
"BND-M10" -Features "Server"

.\silentInstall.ps1 -LicenseServer "localhost" -DatabaseServer
"localhost" -Features "Server"

.\silentInstall.ps1 -LicenseServer "localhost" -DatabaseServer
"BND-M10" -Features "CommunicationServer,LicenseSystemServer"

.\silentInstall.ps1 -LicenseServer "OG-LICENSE1" -DatabaseServer
"BND-M10" -Features
"AlarmMonitoring,AreaAccessManager,BadgeDesigner,FormsDesigner,ID
CredentialCenter,MapDesigner,SystemAdministration"
```

Deployment Note: As part of 8.1 installation effort, the ‘Client Update Service’ method of installation was removed. While this worked for some few customers, continued issues with the certificate security model and permissions concerns made us discontinue that option.

Emergency Key Recovery (Installation)

- Following on from the Encryption Key Management in 8.1, customers can now choose to have their encryption key recoverable by LenelS2.
- You will see this option in the following places:
  - During Encryption Key Generation
    - Database Setup > Re-encrypt my database
    - Setup Assistant for new installations and upgrades jumping over 8.1
  - Setup Assistant upgrades from 8.1 to anything going forward
  - Login Driver application > Edit > Manage Encryption Key



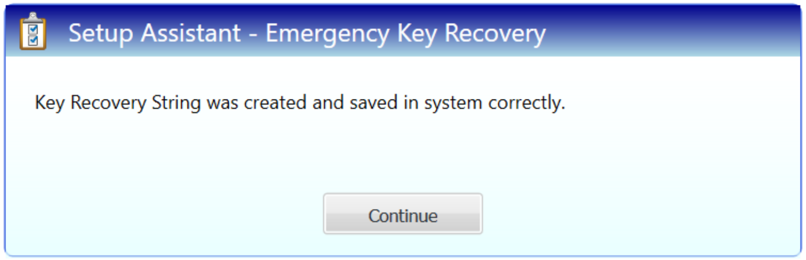
Setup Assistant - Emergency Key Recovery

Select the Emergency Key Recovery option so that the OnGuard system software provider can help you recover the encryption key if there is a system failure. This process will create and securely store a key recovery string for the system that can be provided to support the recovery process. The key recovery string will be updated each time the encryption key is changed for the system.

IMPORTANT: Choosing to disable this option is not recommended and should only be done for End-User systems where strong key management processes are in use, and the encryption key is protected by an alternate method. Without the encryption key, encrypted fields are not accessible and the database CANNOT be used to run an OnGuard system.

● Yes, enable Emergency Key Recovery.

○ No, disable Emergency Key Recovery.



Setup Assistant - Emergency Key Recovery

Key Recovery String was created and saved in system correctly.