MAKE THE WORLD SEE

Milestone Systems

XProtect Access for OnGuard

Manual



Contents

Copyright, trademarks, and disclaimer	6
Introduction	7
General description	7
Whats new in version 4.4?	7
Solution overview	8
Planning your installation	9
Different installation scenarios (explained)	9
Single system scenario	10
Multiple single systems	10
Milestone XProtect Federated Architecture with OnGuard Enterprise	11
Distributed Event Server system design	13
System architecture diagram for distributed Event Server:	13
Installation and configuration of the Event Server:	14
Firewall on the XProtect Event Server and SQL Server	14
Distributed deployment options	15
Single system with integration server	16
Milestone XProtect clustered with single clustered OnGuard	16
Milestone XProtect Management Server redundancy solutions with OnGuard	17
Technical Considerations	19
Software version compatibility	19
Hardware support	19
Scalability	20
FIPS-140-2 compatibility	20
OnGuard segments explained	20
Configuring segments within OnGuard	22
Mapping OnGuard users to segments	22
XProtect Access and SSO authentication (explained)	23
Secure communications explained	24
Applying secure communications between XProtect and the OnGuard XProtect Access Service	25
Applying secure communications between the OnGuard XProtect Access Service and OpenAccess	27

Prerequisites	30
Time synchronization	30
.NET framework for OnGuard	30
Milestone XProtect license	30
Event Server DNS name resolution	30
Smart Client profile settings explained	30
OnGuard license options PLEASE CONSULT CARRIER FOR LICENSING	31
Required OnGuard services	31
Generate software events	32
Create directory in OnGuard	32
Create user in OnGuard	34
Installation	
Installation program (explained)	39
Step 1: Installing OnGuard XProtect Access Service	40
Step 2: Installing OnGuard XProtect Access MipPlugin	42
Integration version upgrades	44
Upgrading from DataCondulT	46
Uninstalling the integration	48
XProtect Management Client Configuration	49
XProtect Access instance creation wizard	49
XProtect Access instance status & properties	51
Personalized login explained	55
Enabling or disabling personalized login	55
Logging into Smart Client with personalized login	56
Refreshing personalized login	58
Commands explained	58
Supported commands reference	59
Administrative Configuration	62
Door & camera association	62
Categorize events	62
Access control event categories	65
Access request notifications	67

	Searching for cardholders explained	69
	Client profiles & Roles explained	. 70
	Managing client profiles & Roles	70
s	mart Client Features	. 71
	Access control workspace explained	71
	Access control workspace events	. 71
	Access control workspace doors	. 73
	Access control workspace cardholders	. 75
	OnGuard web admin link	. 75
	Access Monitor	. 76
	Maps	77
	Map icon hardware and status details	79
	Overlay buttons & commands	80
	Alarm acknowledgment explained	83
	Acknowledge alarms in XProtect	. 85
	Checking alarm acknowledgment status in OnGuard	86
	Changing alarm acknowledgment behavior	07
		07
	Smart Client access control options	
N		88
N	Smart Client access control options	88 90
N	Smart Client access control options	88 90 90
	Smart Client access control options Iobile Client XProtect Mobile application	88 90 90 90
	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile	88 90 90 90 92
	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon	88 90 90 90 92
	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon Service tray icon (explained)	88 90 90 90 92 92
S	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon Service tray icon (explained) Using the Select Certificate menu	88 90 90 90 92 92 92
S	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon Service tray icon (explained) Using the Select Certificate menu Using the log viewer application	88 90 90 92 92 92 93 96
S	Smart Client access control options	88 90 90 92 92 92 92 93 96 96
S	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon Service tray icon (explained) Using the Select Certificate menu Using the log viewer application Iugin Settings File Working with the PluginSettings.json configuration file	88 90 90 92 92 92 92 93 96 97
S P K	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon Service tray icon (explained) Using the Select Certificate menu Using the log viewer application Iugin Settings File Working with the PluginSettings.json configuration file nown Issues	88 90 90 92 92 92 92 93 96 97 97
S P K	Smart Client access control options	88 90 90 92 92 92 92 93 96 97 97 98
S P K	Smart Client access control options Iobile Client XProtect Mobile application Using the access control tab in XProtect Mobile ervice Tray Icon Service tray icon (explained) Using the Select Certificate menu Using the log viewer application Iugin Settings File Working with the PluginSettings.json configuration file nown Issues Limitations roubleshooting Guide	88 90 90 92 92 92 92 93 93 96 97 97 98 98

OnGuard	
OnGuard loses communication with access control hardware	100
Integration version downgrades	
XProtect 2021 R1 and R2 shows no error if OpenAccess - password is incorrect.	101
Access control rules stop working after upgrade to 4.0 or newer.	
OnGuard XProtect Access Service: MipPlugin post-install verification	
Cardholder search data fields are missing, or out of order	106
Not receiving cardholder or badge changes	108
XProtect Access integration flooding OnGuard user transaction report	108
OnGuard XProtect Access instance not displayed in the XProtect Management Client	
LS OpenAccess service automatically stops seconds after starting	109
I/Os connected to OSDP readers are no longer detected	109
LS OpenAccess events fail in OnGuard Enterprise systems	109
XProtect Access developer tabs (explained)	109
Enabling developer tabs	110
Developer tabs (reference)	110
All other support issues	114
Version Notes	115
Current document version	115
Appendix A: Create CA Certificate script	
Appendix B: Create Server SSL Certificate script	117

Copyright, trademarks, and disclaimer

Copyright © 2024 Milestone Systems A/S

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

Introduction

General description

This document describes the XProtect Access integration between Milestone XProtect video management system (VMS) and the OnGuard access control (AC) system. This integration supports the following standard XProtect Access features:

- · Retrieve and refresh configuration from the OnGuard AC system, e.g. doors and event types
- · Receive AC event streams and hardware status changes from the OnGuard system
- · Display and search cardholder information both data and images
- · Create alarms in XProtect alarm manager based on AC events
- Synchronization of alarm status between XProtect and OnGuard
- Association of access control events to cameras for simultaneous display of events and video
- · Association of access control hardware to cameras for simultaneous display of doors and video
- · Select and categorize events from the OnGuard system to view and work with events in groups
- Trigger system actions based on AC hardware events. For example: start recording, go to PTZ preset, display access request, triggered by door forced, access granted, and access denied
- · Personalized login to support segmented database systems
- · AC hardware status display and command interaction on VMS client map user interface
- · Create customized access reports based on search queries in XProtect Smart Client
- Smart Client pop-up access request notifications
- · AC hardware interaction via XProtect web and mobile clients
- · Connect to the OnGuard web administration interface from the XProtect Smart Client

Whats new in version 4.4?

The most prominent changes to version 4.4 of the OnGuard XProtect Access integration are listed below.

Features & User Experience:

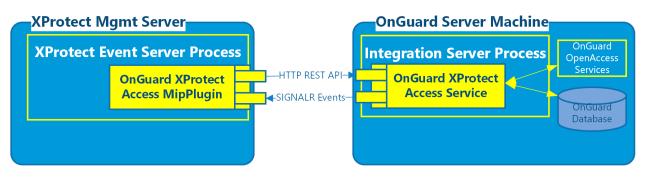
 Durable Event Subscription - increased resiliency and reliability for event stream connection between OnGuard and XProtect.

- Additional logging of API calls and privilges.
- Testing and documentation for Distributed Event Server system design on page 13.
- Support for Categorize events on page 62. (requires version 4.4 CU1)

Solution overview

The solution provided has two components:

- 1. OnGuard XProtect Access Service Typically installed in the OnGuard environment.
- 2. OnGuard XProtect Access MipPlugin Installed in the XProtect environment.



Planning your installation

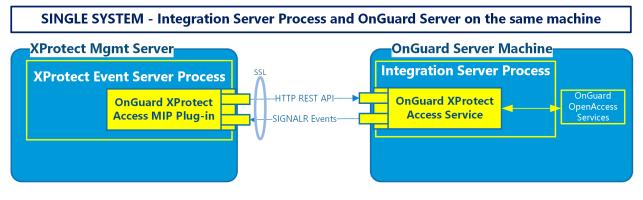
Different installation scenarios (explained)

There are different ways to integrate XProtect with the OnGuard access control system. This section is a guide to help you figure out which deployment options you should consider.

Milestone and LenelS2 have created a technical deployment guide which documents design recommendations, performance thresholds, and architectural guidance within one short document. The XProtect Access OnGuard integration is covered in this deployment guide. Download and read the guide.

Installation scenario	Use case
Single system	You have a single XProtect system (one event server per system) and a single OnGuard system (one OnGuard database per system).
Multiple single systems	You have multiple single XProtect/OnGuard system pairs. The customer just wants each pair to behave independently of each other.
XProtect Federated Architecture with OnGuard Enterprise	You have a federated XProtect system and an OnGuard Enterprise system that need pairing. The customer needs centralized configuration and alarms.
Distributed XProtect Event Server scenario	XProtect Event Server installed on an isolated host environment to accommodate increased alarm and event throughput.
Single system - Integration Server and OnGuard Server on separate machines	There is a need to run the required integration software components on a different machine than the OnGuard Server.
XProtect Clustered with OnGuard Clustered	You have a XProtect clustered environment connecting to an OnGuard clustered environment.

Single system scenario

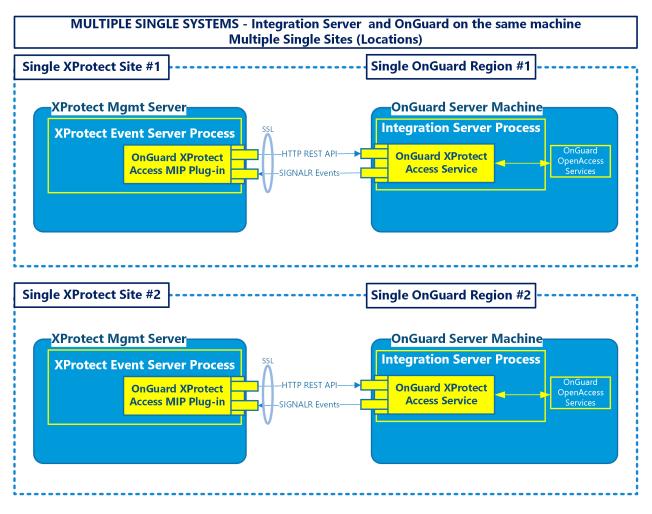


For most systems, this is the recommended installation scenario.

- First install the OnGuard XProtect Access Service on the OnGuard server
- Second install the OnGuard XProtect Access MipPlugin on the XProtect server

Multiple single systems

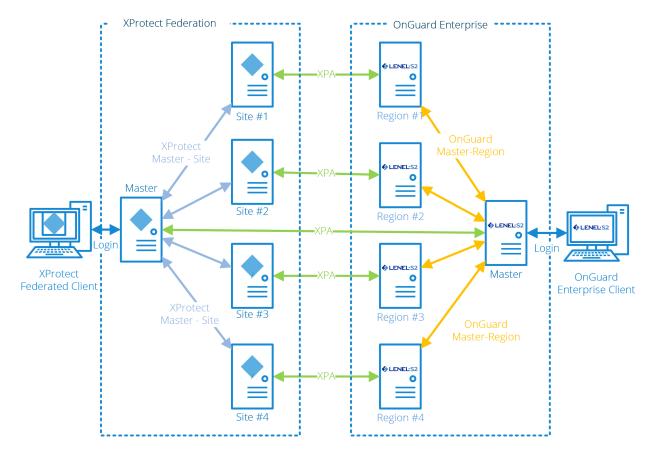
Scaling the default scenario means adding more OnGuard systems and XProtect systems in a 1:1 ratio. The OnGuard and XProtect systems are independent of each other, keeping the OnGuard XProtect Access Service process on the OnGuard machine. The customer is NOT interested in centralized configuration or alarms, the integrated XProtect/OnGuard systems are independent of each other.



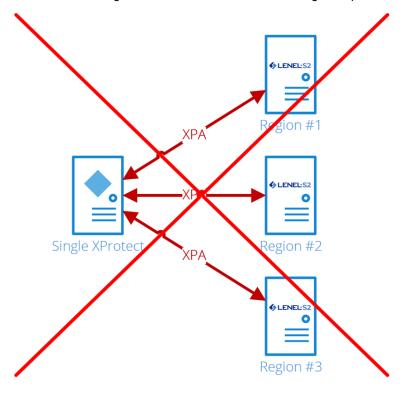
Site #1 and site #2 are independent of each other and not communicating with each other, or commonly managed. The same is true for both the XProtect and the OnGuard systems in this scenario.

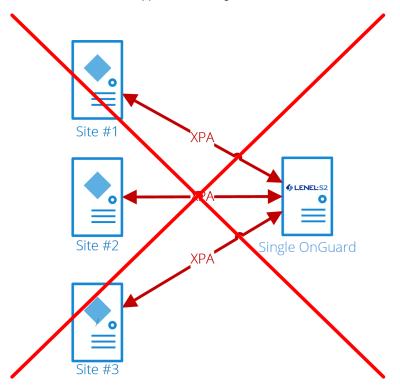
Milestone XProtect Federated Architecture with OnGuard Enterprise

This scenario has many uses. It is recommended for large scale deployments. This is the default scenario when the customer has an Enterprise deployment of OnGuard and wants to integrate with XProtect. Also, it is recommended when the customer wants centralized alarm and configuration management for both systems.



Milestone DOES NOT support connecting a single XProtect site to many different OnGuard regions. We do not recommend running more than one XProtect Access integration per event server, for performance reasons.





Milestone DOES NOT support connecting more than one XProtect site to a single OnGuard region.

Each XPA line in these diagrams represents the HTTP/SignalR connection between the Event Server in XProtect and the OnGuard XProtect Access Service on the OnGuard server. There are some scenarios where the OnGuard XProtect Access Service may not live on the same OnGuard server, see <u>Distributed deployment options on page 15</u> for details.

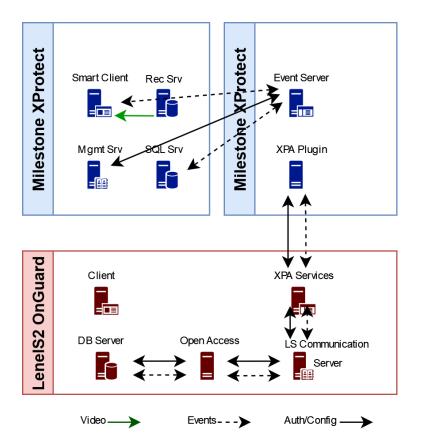
Distributed Event Server system design

Video management systems engineered for increased event throughput will commonly include a distributed XProtect Event Server. This is a system design scenario which places the XProtect Event Server in a standalone host server environment, which is specifically outside of the Management Server and/or Recording Server host environments.

Below are the required system design details for integrating and configuring the system to support a distributed Event Server configuration. These include the system design diagrams and data flow, service account requirements, and firewall port requirements.

System architecture diagram for distributed Event Server:

The XProtect Access Plugin for XProtect should be installed on the Event Server. As in all other XProtect Access system design scenarios, the versions of the plugin on the XProtect system and the OnGuard system must match.



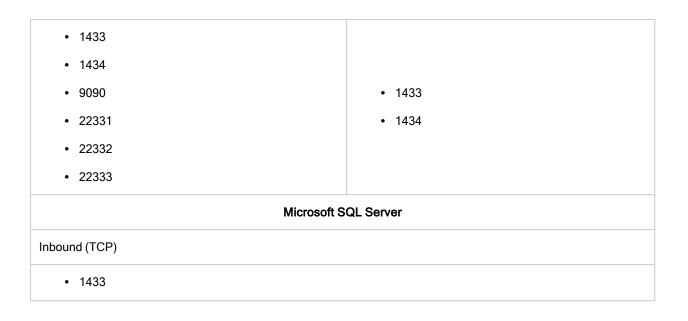
Installation and configuration of the Event Server:

All services for XProtect on both the Management Server and Event Server need to be logged on and running as the same account. Testing confirmed that in a domain environment an account with administrative privileges on the XProtect system worked, and the default Network Service account on a Work Group environment worked.

Firewall on the XProtect Event Server and SQL Server

Most of the ports in the list below are opened automatically by the standard XProtect installation programs. To note, firewall TCP port 1433 must be manually opened on the XProtect Event Server host machine. This port facilitates communication between the Event Server and the Microsoft SQL Server.

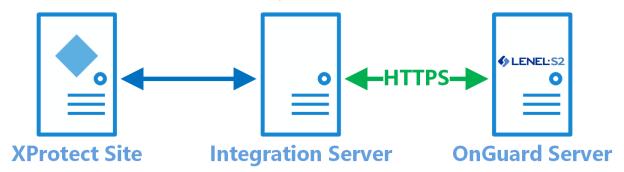
XProtect Event Server				
Inbound (TCP) Outbound (TCP)				
• 1234	• 80			
• 1235	• 443			



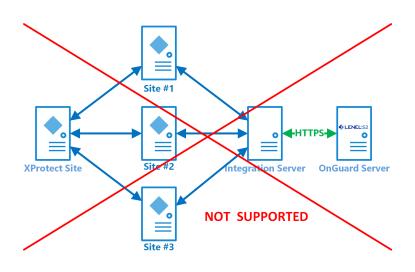
To learn more about why specific ports need to be opened, and which other ports are required for all XProtect services, read this knowledge base article.

Distributed deployment options

It's possible to have the "integration" server on a different machine than the XProtect server or the OnGuard server. This option provides segmentation of OnGuard hardware and events to individual XProtect sites, and the distributed scenario helps support OnGuard clustering.

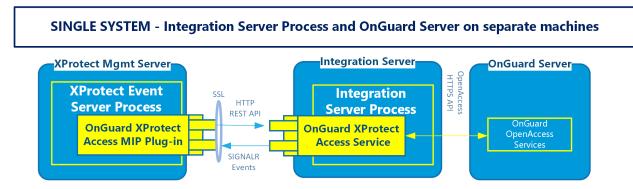


For design, scaling, and performance reasons, Milestone doesn't support connecting multiple XProtect sites to the same Integration Server instance.



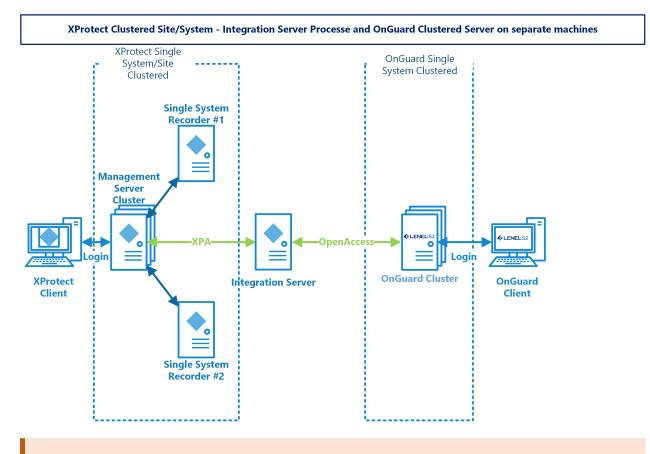
Single system with integration server

This is the recommended system design to run the OnGuard XProtect Access Service on a different machine than the OnGuard server.



Milestone XProtect clustered with single clustered OnGuard

When server clusters are used for redundancy, the OnGuard XProtect Access Service requires a separate Integration Server - distributed from both the XProtect and OnGuard server. Below is the suggested architecture if both XProtect and OnGuard use server clusters:



Before configuring XProtect Access with OnGuard on a system that is using clustered XProtect Management Server Failover which includes a clustered XProtect Event Server, it is required to add all of the clustered Event Server nodes to the Registered Services within XProtect. Please refer to KB 33314 for more details on using XProtect Access with clustering. Refer to KB 34505 for additional information about XProtect in a clustered environment.

Milestone XProtect Management Server redundancy solutions with OnGuard

Both of the XProtect Management Server redundancy solutions are tested and supported to work with the OnGuard XProtect Access integration.

- 1. Microsoft Clustered Server solution
- 2. XProtect Management Server Failover solution

Both XProtect Management Server redundancy solutions offer data resilience and availability for many XProtect system components. As such integrations which rely on XProtect experience high availability and resilient video access. During failover events, interruption in service still occurs. In particular, the connection to the XProtect Event Server and integration plug-ins or services hosted in the same server environment experience disruption. Tests show the connection to XProtect Access services, and connections to OnGuard re-establish with little or no loss of data, and full system operation restores within minutes.

Find more information about these redundancy solutions for XProtect here:

XProtect Management Server Failover

Clustering XProtect Management Servers

Technical Considerations

Software version compatibility

Integration with OnGuard access control system is supported for all XProtect VMS products that support MIP integrations. To find a list of supported versions of the following software components, read the most recent compatibility information.

- OnGuard access control software
- XProtect video management software
- OnGuard XProtect Access integration software

Please verify the version of OnGuard is compatible. Milestone recommends the latest versions of both OnGuard and XProtect.

Hardware support

The following OnGuard panels are tested and supported by Milestone Technical Support. More hardware models are compatible.

Panel Model	Description
LNL-500	Intelligent System Controller
LNL-1100	Input Control Module
LNL-1200	Output Control Module
LNL-1300	Single Reader Interface Module
LNL-1320	Dual Reader Interface Module
LNL-2210	Intelligent Single Door Controller
LNL-2220	Intelligent Dual Reader Controller
LNL-3300	Intelligent System Controller
LNL-4420	Advanced Dual Reader Controller

Scalability

This section details the size of the test system at the LenelS2 certification labs and lists the maximum documented performance.

The software interface between Milestone and OnGuard is optimized for throughput of events and system status messages. Server components and computer hardware resources can still limit total throughput.

Device Type	Count
Panel	1925
Door	1024
Reader	1028
IO Module	14
Input	2074
Output	2055
Card Holders	400,000

Event	Events/sec
OpenAccess	100
OpenAccess - Peak	300+

FIPS-140-2 compatibility

This integration is compatible with operating systems that are running in FIPS mode, it is fully tested and supported in these environments. This integration is not officially FIPS-140-2 compliant. XProtect and OnGuard are individually both FIPS-140-2 compliant.

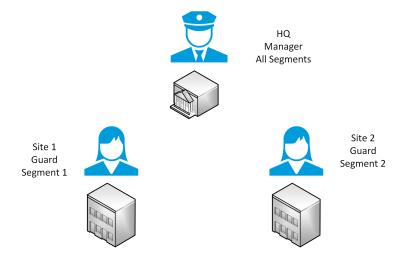
OnGuard segments explained

Personalized login can control which devices, events, and alarms users can view in the Smart Client when integrated with segmented OnGuard systems. A segmented OnGuard system uses logical groupings, known as segments, to define which access panels, readers, cardholders, and users work together.

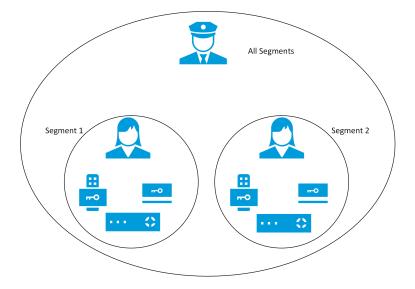
Creating a segmented system within OnGuard shouldn't be a part of installing the XProtect Access OnGuard integration. It's recommended to consult with an authorized OnGuard representative before configuring segments.

For example, an organization with facilities in many locations can use segments within their OnGuard system so users have access to view and manage the devices at the facilities relevant to their job.

Illustrated below is an organization with three sites, a head quarters, site 1, and site 2.



Using segments, the guard user at site 1 can see readers, panels, and cardholders from segment 1, and the guard user from site 2 can see the devices and information from segment 2. The manager can see all devices and information, since they're in the default "All Segments" segment.



Configuring segments within OnGuard

The following process shows where the information about existing segments is found within an OnGuard system. Please consult with your LenelS2 representative before adding segments to an operational OnGuard system.

- 1. Go to the Segments sub-menu in the Administration menu of the OnGuard System Administration application.
- 2. The Segment Options tab contains options to enable segmentation.

🚯 Segments			×			
Segment Options Segments Segment G	oups					
Enable segmentation						
Segment card formats						
Segment badges via badge type	3					
Segment cardholders						
Segment visitors						
Allow segments to belong to more	than one segment group					
I Allow access levels to be configured as assignable by users in other segments						
Segment non-system List Builder lists						
			-1			
Add Modify Delete	Help	Clo	se			

3. The Segments tab contains the segments configured within OnGuard.

egment Options Segments Seg	gment Groups										
Segment	Name:										
Default Segment	Default Segment										
Segment 1	Hardware Settings	Anti-Passback	Biometrics	User Co	mmands	Visits	Access	l evels /	Assets	Runawa *	F
Segment 2	Hardware limits					Tione		2010107		Thanking	
		Maxi	mum holidays	255	· · ·						
		Maxim	um timezones	255	· ·						
		Maximum	access levels	255	*						
	h	faximum badge r	number length	9	*						
		Maximum exter	nded id length	0	*						
	Max	imum number of e	elevator floors	64	\sim						
	Ma	aximum number ol	f card formats	8	\sim						
	Maximum acces	s level assignmer			_						
			Tota	6	× v						
x >		With no ac	tivation dates	6	*						

Mapping OnGuard users to segments

- 1. Go to the Users sub-menu in the Administration menu of the OnGuard System Administration application.
- 2. Click Modify.
- 3. Select the Segment Access sub-tab.

4. In the Segment listing window, select the segment(s) the user has access to.

🊽 Users			
Users Search System Permission Groups	Cardholder Permission Grou	ups Monitor Permission Groups	s Report Permission Groups Field/Page Permission Groups
Name RAdio State Control (Control (Contro) (Contro) (Contro) (Contro) (Contro) (Contro) (Cont		Cardholder Cardholde Admin Cardholde Bdge Operator Cardholde Admin (All Permissions) Cardholder User	Mon Mon Mon Mon Mon Mon Mon Mon
OK Cancel Clear	H	leip	Modify Mode Close

5. Click **OK** to save the changes.

It's recommended to map users logically from your domain, to XProtect, to OnGuard and to their segment. This lets SSO in XProtect work with the personalized log-in feature, and with segments within OnGuard, to simplify the log-in experience, while also customizing and controlling the integrated Smart Client.

You can map OnGuard users to a domain user within XProtect in the **Directory Accounts** subtab of the **Users** sub-menu of the **Administration** menu in the OnGuard System Administration application.

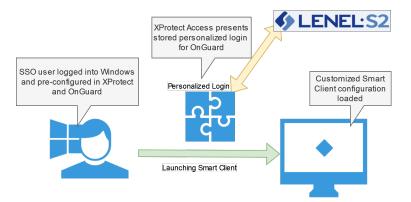
	System System Admin	Cardholder Cardholder Admin	Moni	Segment Access General Directo	Area Access M ry Accounts	Manager Levels Mor Internal Account	nitor Zone Assign Permission Gro
Blow, Joe System Account, System Account	System Badge Operator System Admin (All Permissions) System User		Moni (All P Moni	Name	User Name mjt	Directory	
Hide users whose access to this system is Hide users that have been automatically of			,			Link	Unlink

XProtect Access and SSO authentication (explained)

XProtect single sign-on (SSO) doesn't delegate SSO to the OnGuard system. XProtect SSO uses the logged in Windows user, and it can't automatically present that same user to OnGuard for authentication. The personalized login feature of XProtect Access is how XProtect presents unique credentials for authentication with OnGuard.

These personalized login credentials can match a user with SSO in OnGuard. They can even be the same user logged into Windows who is launching the Smart Client. The credentials must be entered at the first login of the Smart Client, and re-entered if the credentials are changed in OnGuard. Then a user can log into Windows, launch the Smart Client,

which automatically authenticates with XProtect via SSO. At this point the stored credentials for the personalized login user that matches the XProtect user are presented to OnGuard and the OnGuard user's configuration is loaded into the Smart Client. This can all be done without manually presenting any credentials to XProtect or OnGuard.



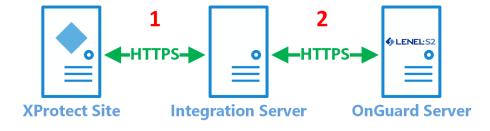
This is the closest to a true SSO user experience that the XProtect Access integration offers. It requires using the personalized login feature. If this feature isn't used, all authentication to OnGuard from XProtect Access uses the same user credentials that the OnGuard XProtect Access Service uses to refresh and fetch the configuration from OnGuard. To use this partial SSO user experience with customized privileges, it's important to link XProtect users and roles directly to the appropriate SSO users within OnGuard.

Secure communications explained

XProtect Access integrations can be configured to use encrypted communications. The XProtect Access integration with OnGuard can encrypt communications between the XProtect Access service and the XProtect Event Server, and between the XProtect Access service and OpenAccess service.

Please note: the instructions in this document are for generating self-signed certificates. It's possible to get certificates from a trusted third-party provider. For more information please read the XProtect VMS certificates guide

The process of securing communications between OnGuard and XProtect should start after the integration has been installed and configured. There are two different processes required.



- 1. Certificate generation, distribution, and configuration supporting secure communications between XProtect and the OnGuard XProtect Access Service.
- 2. Certificate extraction, distribution, and configuration supporting secure communications between OpenAccess and the OnGuard XProtect Access Service. This process (#2) is required when the OnGuard XProtect Access Service isn't installed on the OpenAccess host machine.

Applying secure communications between XProtect and the OnGuard XProtect Access Service

In versions 4.2 and higher of the XProtect Access OnGuard integration, there is a tool built into the XProtect Access service to help users manage certificates. This process shows the steps required to generate, distribute, and configure the solution to secure communications between XProtect and the OnGuard XProtect Access Service.

The process included below is for self-signed certificates. If you are using a third party certificate, from a commercial certificate provider, please skip ahead to step number ten below. Refer to the XProtect Certificate Guide for any questions on dealing with certificates.

1. On a server with restricted access, open PowerShell as an administrator and run the script in Appendix A, to create a CA certificate.

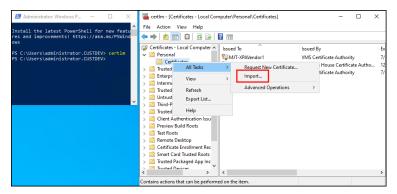
🏪 🛃 📙 🖛 Local Disk	(C:)	-	D X
File Home Share	View		~ 🕐
\leftarrow \rightarrow \checkmark \Uparrow $\stackrel{\bullet}{=}$ \Rightarrow This	s PC → Local Disk (C:)	5 V	Q
CCURE_9000_ * ^	Name	Date modified	Туре
Certificates	SWinREAgent	7/12/2022 8:09 PM	File folder
logs	inetpub	5/23/2022 11:30 AM	File folder
Zips & Installers	milestone	10/5/2021 4:22 PM	File folder
This PC	PerfLogs	5/8/2021 3:20 AM	File folder
	Program Files	7/18/2022 2:07 PM	File folder
3D Objects	Program Files (x86)	7/18/2022 1:44 PM	File folder
🔮 C on USLT-MJT-(ProgramData	5/23/2022 3:10 PM	File folder
E Desktop	Sql	5/19/2022 1:18 PM	File folder
🗄 Documents	sysprep	5/18/2022 1:42 PM	File folder
👆 Downloads	Users	5/23/2022 11:30 AM	File folder
🛒 K on USLT-MJT-(Windows	5/23/2022 2:42 PM	File folder
Music	🔄 root-authority-public	7/18/2022 3:12 PM	Security Ce
Pictures			
🔮 Q on USLT-MJT-			
S on USLT-MIT-C	<		>
12 items 1 item selected	863 bytes		

- By default the script places the new root certificate in the C:\ file location. Move the certificate to the XProtect server.
- On the XProtect server right-click the certificate and select Install Certificate to begin the certificate installation wizard.
- 4. Choose to place the certificate in the Store Location of the Local Machine.

- 5. Browse and import the certificate in to the Trusted Root Certification Authorities folder.
- 6. Complete the wizard.
- Go back to the server with restricted access where you generated the root certificate, open PowerShell and enter the script in Appendix B, to generate a new client certificate to install on the server hosting the OnGuard XProtect Access Service.
- The script requires input: the DNS name of the server hosting the OnGuard XProtect Access Service, the IP address of the server, and a certificate password of your own choosing - enter this information and complete the script.
- 9. By default the script generates the certificate at the C:\ file location. Copy the file and move it to the server hosting the OnGuard XProtect Access Service.

🏪 🕑 📙 🚽 Local Disk	(C:)	_	
File Home Share	View		~ ?
\leftarrow \rightarrow \checkmark \Uparrow \blacksquare \rightarrow Thi	s PC > Local Disk (C:) >	5 ~	Q,
CCURE_9000_ * ^	Name	Date modified	Туре
Certificates	\$WinREAgent	7/12/2022 8:09 PM	File folder
logs	inetpub	5/23/2022 11:30 AM	File folder
Zips & Installers	milestone	10/5/2021 4:22 PM	File folder
This PC		5/8/2021 3:20 AM	File folder
		7/18/2022 2:07 PM	File folder
📜 3D Objects	Program Files (x86)	7/18/2022 1:44 PM	File folder
🔮 C on USLT-MJT-(ProgramData	5/23/2022 3:10 PM	File folder
E Desktop	📙 Sql	5/19/2022 1:18 PM	File folder
Documents	sysprep	5/18/2022 1:42 PM	File folder
🕹 Downloads	Users	5/23/2022 11:30 AM	File folder
K on USLT-MJT-(Windows	5/23/2022 2:42 PM	File folder
b Music	MJT-XPAVendor1	7/18/2022 3:26 PM	Personal
Pictures			
🔮 Q on USLT-MJT-			
S on USLT-MIT-C	<		>
12 items 1 item selected	3.61 KB		:==

10. Go to the server hosting the OnGuard XProtect Access Service and run the certificates snap-in for the local machine. Right-click the **Certificate** store within the **Personal** folder and choose to **Import** a new certificate.



11. Import the certificate into the store of the local machine. Choose the certificate file that you copied to the local server. Enter the password chosen during the script. Browse to the personal folder of the certificate store to choose that as the location for the certificate. Complete the import wizard

- 12. Open the OnGuard XProtect Access Service service tray icon and choose the certificate to use. It should match the hostname of the OnGuard server. The service restarts once the configuration is saved.
- Now apply encryption for the OnGuard XProtect Access instance in the XProtect Management Client. There are three options to use for secured communication for the integration. This process enables use of XProtect Access Service - SSL Certificate Validation, option A below.

Integration plug-in:	LenelS2 OnGuard (Version: 4.
Last configuration refresh:	9/14/2022 3:49 PM
	Refresh Configuration
Operator login required:	
XProtect Access Service - Host:	MJT-LNLS2
XProtect Access Service - Port:	8443
XProtect Access Service - SSL Certificate Validation:	✓ A
OpenAccess - Host:	MJT-LNLS2
OpenAccess - Port:	8080
OpenAccess - SSL Certificate Validation:	✓ B
OpenAccess - User:	administrator
OpenAccess - Password:	Enter current password
OpenAccess - Directory:	custdev.us
Options - OnGuard Web Administration URL:	
Options - Disable Commands:	\checkmark
Options - States polling interval (seconds):	900
Options - [Legacy] OnGuard SQL Server hostname:	
Options - [Legacy] Connection Profile:	
Options - Enable performance metrics (diagnostics):	

Applying secure communications between the OnGuard XProtect Access Service and OpenAccess

In versions 4.2 and higher of the XProtect Access OnGuard integration, encrypted communication is fully supported. This process shows the steps required to extract and distribute the required certificates and configure the solution to enable secure communications between the OnGuard XProtect Access Service and OpenAccess.

The process below isn't needed when the OnGuard XProtect Access Service runs on the OnGuard server that hosts the OpenAccess service. In integrated systems where the OnGuard XProtect Access Service and the OpenAccess service are co-located encrypted communication can be enabled with no extra configuration.

1. Go to the OpenAccess server, open PowerShell and run the following script to extract the CA certificate.

```
$cert = Get-ChildItem 'Cert:\LocalMachine\LS Certificate Store' |`
Where-Object{$_.Subject -like "*cn=$ENV:COMPUTERNAME*"}
if ($cert) {$match = Select-String "CN=(.*?),"`
-InputObject $cert.Issuer
$issuer = $match.Matches.groups[1].Value
$RootCert = Get-ChildItem 'Cert:\LocalMachine\Root'`
|Where-Object{$_.Subject -like "CN=$issuer*"}
if ($RootCert) {Export-Certificate -Cert $RootCert -FilePath ".\LenelCert.cer"}`
else{write-host "Could not find $Issuer Certificate." -foregroundcolor Red}}`
else{write-host "Could not find $env:Computername Certificate in LS Certificate
Store."`
-foregroundcolor Red}
```

- 2. By default the script exports the extracted root certificate to the current directory. Copy the certificate and move it to the OnGuard XProtect Access Service server.
- On the OnGuard XProtect Access Service host server right-click the certificate and select Install Certificate to begin the certificate installation wizard.
- 4. Choose to place the certificate in the Store Location of the Local Machine.
- 5. Browse and import the certificate in to the Trusted Root Certification Authorities folder.
- 6. Complete the wizard.
- 7. Now apply encryption for the OnGuard XProtect Access instance in the XProtect Management Client. This process enables use of **OpenAccess SSL Certificate Validation**, option B below.

Integration plug-in:	LenelS2 OnGuard (Version: 4.
Last configuration refresh:	9/14/2022 3:49 PM
	Refresh Configuration
Operator login required:	
XProtect Access Service - Host:	MJT-LNLS2
XProtect Access Service - Port:	8443
XProtect Access Service - SSL Certificate Validation:	✓ A
OpenAccess - Host:	MJT-LNLS2
OpenAccess - Port:	8080
OpenAccess - SSL Certificate Validation:	✓ B
OpenAccess - User:	administrator
OpenAccess - Password:	Enter current password
OpenAccess - Directory:	custdev.us
Options - OnGuard Web Administration URL:	
Options - Disable Commands:	✓
Options - States polling interval (seconds):	900
Options - [Legacy] OnGuard SQL Server hostname:	
Options - [Legacy] Connection Profile:	
Options - Enable performance metrics (diagnostics):	

Prerequisites

Time synchronization

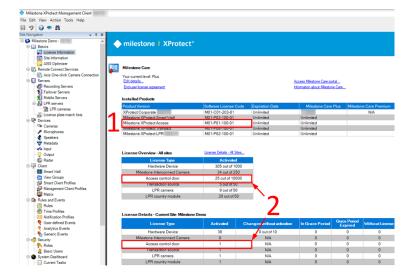
All OnGuard and XProtect servers must be time-synchronized to within a couple of minutes.

.NET framework for OnGuard

.NET Framework 4.7.2 is a requirement for the integration on the OnGuard server machine (NDP472-KB4054530-x86-x64-AllOS-ENU.exe). This note applies for older OS editions; any OS newer than Windows 10 (April 2018 Update) and Windows Server version 1803 have it installed. Milestone recommends that you use Microsoft Windows Server Editions of the OS.

Milestone XProtect license

The customer must have XProtect Access enabled (1) and the appropriate number of doors (2) in their XProtect SLC. See the Management Client license screen for more details.



Event Server DNS name resolution

The server hosting the Milestone XProtect Event Server must have network name resolution. It must resolve the computer name of the OnGuard Server. The OnGuard Server must also resolve the XProtect Event Server.

Smart Client profile settings explained

If you customize or create new Smart Client profiles in XProtect and the users assigned to those profiles need to receive access request notification pop-up alerts, you need to include the following setting.

• Access Control > Show access request notifications = Yes

This is the default setting for all Smart Client profiles. All Smart Client profiles in use need to have this setting configured if system users need to view or interact with access control notifications.

OnGuard license options – PLEASE CONSULT CARRIER FOR LICENSING

To enable the integration the following license options are required in the OnGuard license:

Connection	OnGuard License Options Needed
	OpenAccess Integration (ITM-MLST-001) enabled with an expiration date
OpenAccess	Partner Integration (IPC-311-MLST01) enabled with an expiration date

For XProtect Access version 3.5 and up, the supported connection mode is OpenAccess. The OnGuard license must have the OpenAccess license options for the integration to function. If you are upgrading from version 3.4 with a DataCondulT license, please refer to Milestone Knowledge Base article 33277.

Required OnGuard services

The following Windows services must run on the OnGuard machine:

OnGuard Windows Service Name	Description
LS Communication Server	Required to send and receive status and events between hardware devices and software.
LS Event Context Provider	Required to send events from the OnGuard system.
LS Login Driver	Manages the database password for client login for OnGuard.
LS Message Broker	Required to receive real-time data from the OnGuard system.
LS OpenAccess	Required to interface the OnGuard system web service-based API OpenAccess

	(REST/JSON web service).
LS Web Event Bridge	Required to receive events from the OnGuard system.
LS Web Service	Required to interface the OnGuard system web-service-based events with OpenAccess (SignalR).

Generate software events

In the OnGuard System Administration app, go to the Administration menu, and select System Options:

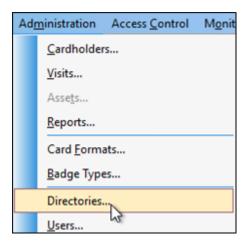
- 1. For OnGuard versions greater than or equal to 7.4 using OpenAccess, check the **OpenAccess host** and **Generate software events** checkbox.
- 2. Set the Linkage Server host to the OnGuard server's machine name.
- 3. Set the Message Broker Service host to the OnGuard server's machine name.

Log on authorization warning None Vert	FIPS mode FIPS mode controller encryption
DataConduIT service	Configuration Download Service host
	Message Broker Service host MJT-0G82.CUSTOMDEVELOP
Monitoring 3 Image: Specify monitor zone assignments	OpenAccess host MJT-OG82.CUSTOMDEVELOPMENT.MILESTO Browse Image: Selencate software events Browse
Linkage Server host OG82.CUSTOMDEVELOPMEN Browse Browse	Default Badge Printing Service host Browse
Reporting and Dashboards Service Host Browse Browse	Port number for IP Client connection 3001
Cumulus Service URL https://identity.cumulus.s2sys.com Link	

Create directory in OnGuard

These instructions are not meant to replace the knowledge of a trained LenelS2 system administrator. They are here to enable the basic setup of an authentication directory and user, so the integration can connect to the OnGuard system.

1. Using the OnGuard System Administration app, go to the Administration menu and select Directories.



For an OnGuard Enterprise system, create directories from the master server.

2. Choose the directory type, either Windows Local Account or domain user account.

For Windows Local Account support, the single sign-on account MUST be a Windows Local Account .	For Domain User Account support, the single sign-on account MUST Allow manual single sign-on as shown below.
Decidoles Name [*] Type Catheritication Name [*] Catheritication Name [*] Administra Windows Local Accounts Marcesoft Active Directory Type: Windows Local Accounts Hostname: Hostname: Estable single sign on	Directories Name [®] Type Image: Constraints Microsoft Active Directory Operative Image: Constraints Operative Image: Constraints Image: Constraints

If you are creating a Directory of a type other than **Windows Local Accounts** (e.g. LDAP, Active Directory), verify the user is a member of the Local Administrators group.

Create user in OnGuard

These instructions are not meant to replace the knowledge of a trained LenelS2 system administrator. They are here to enable the basic setup of an authentication directory and user so the integration can connect to the OnGuard system.

1. Go to the Administration menu and select Users...

Adg	<u>m</u> inistration	Access Control	M <u>o</u> nit
	<u>C</u> ardholder	S	
	<u>V</u> isits		
	Asse <u>t</u> s		
	<u>R</u> eports		
	Card <u>F</u> orma	ats	
	<u>B</u> adge Type	25	
	Directories.		
	Users		
	Wadutatio		

2. Add a new user, or modify a user from the list of internal system users.

Kruger, Scott Syst System Account, System Account (All User, Segment1 Syst	istem Admin II Permissions) Istem Admin	(All Permissions) Cardholder Admin (All Permissions) Cardholder Admin	Monitor Admin (All Permissions)	(All Permissions) <full access=""> (All Permissions)</full>	(All Permissions) View/Edit All Fields	4	X	General Directory Accounts Internal Account Permission Groups First name:		
System Account, System Account (All User, Segment1 Syst	Il Permissions) Istem Admin	(All Permissions)	(All Permissions)		View/Edit All Fields					
User, Segment1 Syst	stem Admin							System Account		
		Cardholder Admin			(All Permissions)	-1				
User, Segment2 Syst	istem Admin		Monitor Admin	<full access=""></full>	View/Edit All Fields	5	SE	Last name:		
		Cardholder Admin	Monitor Admin	<full access=""></full>	View/Edit All Fields	6	SE	System Account		
								Notes:		
								Created Lat dragod P172000 5946 JAN [9172000 1928 PA [9172000 1928 PA]9172000 1928 PA [9172000 1928 PA]9172000 1926 PA]91720000 1926 PA]91720000 1926 PA]9172000000000000000000000000000000000000		
							1			
Hide users whose access to this system is disal										
Hide users that have been automatically create	ted									

3. On the General tab Access to this system is disabled should NOT be selected.

General	Directory Accounts	Internal Account
First name:	-	
Lynn		
Last name:		,
En'Gard		
Notes:		
		~
		~
Created:	Last changed:	
1/12/2021 11:01:	33 AM	
Last Successful Lo	igin:	
	UL 1981 us	er
Access to this	system is disabled	
Automatically c	reated user	

4. On the **Directory Accounts** tab click **Link** to associate the user to the directory user (or local account user) from the directory created in this topic: Create directory in OnGuard on page 32.

General	Directory Accounts	Internal Account	Permission Groups
Name	User Name	Directory	^
		Link	Unlink

5. In the Select Account dialog select the directory from the Directory list. Click Search and select a user in Accounts then click OK.

Select Account				×
Directory:				
IP-0A00183F				~
Field:	Condition:		Value:	
Name ~	contains	~		~
Accounts:				Search
Name	User Name			
🛃 Administrator	Administrator			
🖸 DefaultAccount	DefaultAccour	x /		
🛃 Guest	Guest			
🛃 LenelAdmin	LenelAdmin			
Local Cystem	LocalSystem			
Lynn L. En'Gard	LOG			
😰 cond 🖸 WDAGUtilityAccount	WDAGUtilityA	chount		
			OK	Cancel

6. Once selected, the OnGuard user account is linked to the corresponding Directory account.

General	Directory Accounts		Internal Account	
Name	User Name	Directory	^	
🞻 Lynn L. En'Gard	LOG	IP-0A00183	3F	
		Lin	k	Unlink

7. On the Internal Account tab, make sure that the User has internal account option is selected. Next, enter the account credentials.

General	Directory Accounts	Internal Account
🗹 User has interna	al account	
User name:		
LOG		
Password:		
•••••		
Confirm password:		

- 8. On the **Permission Groups** tab assign the following permission groups:
- System = System Admin
- Cardholder = Cardholder Admin
- Monitor = Monitor Admin
- Reports = Full Access
- Field/page = View/Edit All Fields

General	Directory Accounts	Internal Account	Permission Groups
System:			
System A	dmin		~
Cardholde	r:		
Cardholde	er Admin		~
Monitor:			
Monitor A	dmin		~
Reports:			
<full acc<="" td=""><td>ess></td><td></td><td>~</td></full>	ess>		~
Field/page	e:		
View/Edit	t All Fields		~
SA del	egate (SA permissions)		

Installation

Installation program (explained)

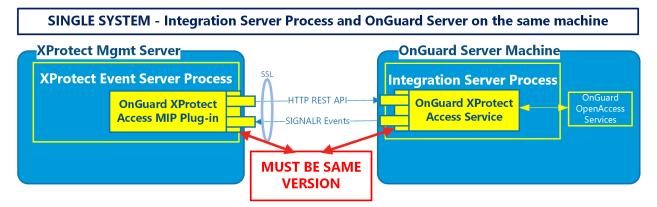
Download the OnGuard XProtect Access installation program.

The installation package consists of one context sensitive installer program:

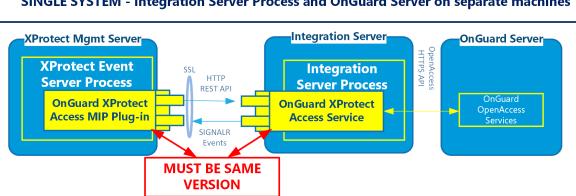
XProtectAccess.OnGuard.msi

This program detects which server it's running on (OnGuard or XProtect), and installs the following software components:

- 1. OnGuard XProtect Access Service Installed on the OnGuard Server machine, or its own integration server.
- 2. OnGuard XProtect Access MipPlugin Installed on the XProtect Event Server machine, or on a standalone Milestone XProtect Management Server.



OR



SINGLE SYSTEM - Integration Server Process and OnGuard Server on separate machines

It's required that the exact same versions of the OnGuard XProtect Access integration software components are installed on both the XProtect and OnGuard machines.

Step 1: Installing OnGuard XProtect Access Service

- 1. Double-click the XProtectAccess.OnGuard.msi file to begin.
- 2. The installation wizard launches. Click Next to continue.

🖟 Milestone OnGuard XProtect	Access Setup	—		×
🔶 milestone	Welcome to the Mileston XProtect Access Setup V		uard	
	The Setup Wizard will install XProtect Access on your com continue or Cancel to exit the	puter. Cli	ck Next to	
	Back N	ext	Cano	el

 The context sensitive wizard offers to install the required components for the OnGuard XProtect Access Service. Click Next to continue.

😥 Milestone OnGuard XProtect Access Setup	– 🗆 X
Custom Setup Select the way you want features to be in	stalled. $igodoldsymbol{\phi}$ milestone
Click the icons in the tree below to change	e the way features will be insta
WProtect Access Service	Install OnGuard XProtect Access Service files on this computer. This feature requires 34MB on your hard drive.
Location: C:\Milestone OnGuard X	Protect Access Service\
Reset	Back Next Cancel

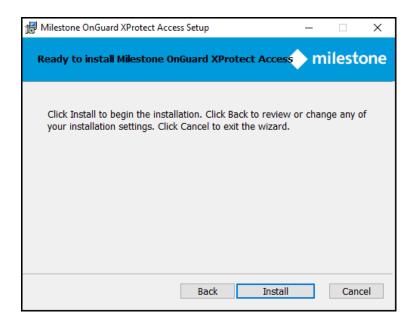
4. Optionally, expand the server icon menu to view installation options. The **Reset** button returns the wizard to all default options.

搅 Milestone OnGuard XProtect Access Setup 🛛 —		×
Custom Setup Select the way you want features to be installed.	ilesto	ne
Click the icons in the tree below to change the way features will	be insta	
Will be installed on local hard drive Entire feature will be installed on local hard drive	otect on this	
Entire feature will be unavailable your naru unve.	34MB or	I
Location: C:\Milestone OnGuard XProtect Access Service	l.	
Reset Back Next	Cance	el

5. Choose the account used to run the OnGuard XProtect Access Service. The wizard selects the LocalSystem account by default. Click Next.

Milestone OnGuard XProt	ect Access Setup	×
XProtect Access Serv Enter credentials for the	rice RunAs Credentials he service	milestone
Run as LocalSyst	em	
<u>D</u> omain:	MJT-WIPE	
<u>U</u> ser Name:		
Password:		
Confirm Password:		
	Back	Next Cancel

6. The ready to install step confirms the wizard can begin installation. Click Install.

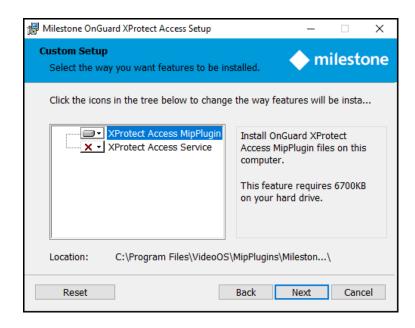


7. Installation is complete. Click Finish.

🖟 Milestone OnGuard XProtect	Access Setup	🖟 Milestone OnGuard XProtect Access Setup 🦳 🗌		Х
♦ milestone	Completed the Milestone XProtect Access Setup W	e OnGu /izard	ard	
	Click the Finish button to exit	the Setur) Wizard.	
	De ek Fin	ich	(
	Back Fir	iish	Cano	er

Step 2: Installing OnGuard XProtect Access MipPlugin

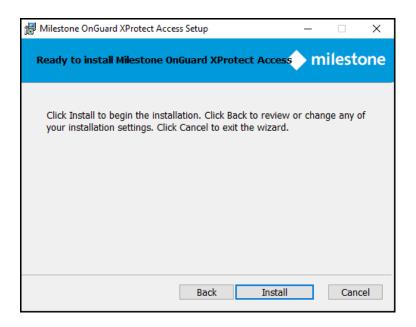
- 1. Place the XProtectAccess.OnGuard.msi file on the server hosting the XProtect Event Server (in a typical deployment, this is the Milestone XProtect Management Server), and double-click the file to begin.
- 2. After the opening step, the context sensitive installation wizard offers the option to install the OnGuard XProtect Access MipPlugin. Click **Next** to continue.



3. Optionally, expand the server icon menu to view installation options. The **Reset** button returns the wizard to all default options.

₩ Milestone OnGuard XProtect Access Setup —		Х
Custom Setup Select the way you want features to be installed.	ilesto	ne
Click the icons in the tree below to change the way features will	be insta	
 XProtect Access MipPlugin Install OnGuard XProvide and the installed on local hard drive Entire feature will be installed on local hard drive Entire feature will be unavailable 	otect s on this 6700KB	
Location: C:\Program Files\VideoOS\MipPlugins\Mileston	λ	
Reset Back Next	Cance	el -

4. The ready to install step confirms the wizard can begin installation. Click Install.



5. You have installed the OnGuard XProtect Access MipPlugin. Click Finish.

🖟 Milestone OnGuard XProtect	Access Setup	—		×
milestone	Completed the Milestone XProtect Access Setup W		ard	
	Click the Finish button to exit the	ne Setu	o Wizard.	
	Back Fini	sh	Cano	el

Integration version upgrades

All components are updated with every new OnGuard XProtect Access release. The installation program is designed to automatically remove and replace the required files and folders during an upgrade from older versions of the integration.

The process for upgrading can follow any order. However, the recommended order is as follows:

- 1. Go to the OnGuard server(s) All OnGuard machines where the ACM Server is installed.
- 2. Run the XProtectAccess.OnGuard.msi installation program. It performs the following actions:

- Uninstall the ACM Server OnGuard Plugin
- Uninstall the ACM Server
- Install the OnGuard XProtect Access Service.
- 3. Go to the XProtect server(s) Milestone XProtect Event Server hosts where the Mip Plugin is installed.
- 4. Run the XProtectAccess.OnGuard.msi installation program. It performs the following actions:
- Uninstall the Mip Plugin and the ACM Wizard
- Remove the folder created by the ACM Wizard for OnGuard at the default location (C:\Program Files\Milestone\MipPlugins\OnGuardACMServer)
- Install the OnGuard XProtect Access MipPlugin and create a new folder at the default location (C:\Program Files\Milestone\MipPlugins)

Automatic upgrades of configured and installed instances in the Management Client are supported for all versions of the OnGuard XProtect Access integration. Run the XProtectAccess.OnGuard.msi installer; it upgrades any installed components. The system should be up and running, fully functional, after the upgrade.

Versions 4.1 and higher of the integration add two fields to the **General Settings** menu in the Management Client to define the connection between the OnGuard XProtect Access MipPlugin (on the XProtect server) and the OnGuard XProtect Access Server - Host: and XProtect Access Server - Port:

```
    XProtect Access Service - Host:

    XProtect Access Service - Port:

    8443
```

The upgrade process fills the **Port** field with the default value of 8443, but the **Host** field remains empty. Before saving any changes in the Management Client the host value is required. During the upgrade, the configuration value for the host field is retained from the old version of the integration from the "connection profile" setting. This is why the integration continues to function. However, once it's opened, the UI logic of the Management Client requires this field to be populated and saved accurately.

- 1. Open the XProtect Management Client.
- 2. In the **General Settings** tab of the upgraded OnGuard XProtect Access instance, enter the hostname for the OnGuard server or the Integration Server in the **XProtect Access Service Host:** field.
- 3. Save the changes in the Management Client.

Upgrading to 4.0 or higher from older versions requires reconfiguration of all rules in XProtect triggered by access control events or event categories. Door hardware objects aren't supported as event sources in 4.0 or newer versions, readers are used instead. Read more here: Access control rules stop working after upgrade to 4.0 or newer. on page 102

Upgrading from DataCondulT

Any XProtect Access integration using the DataCondulT connection mode can't upgrade directly to versions 4.0 or newer. DataCondulT is only compatible with XProtect Access versions 3.4 or older. All systems running DataCondulT must enable OpenAccess, upgrade to version 3.6 of the integration, and then upgrade to the most recent version. Perform the following procedure to upgrade.

- 1. Apply the OpenAccess license.
- Contact CARRIER to enable the OpenAccess Integration license (ITM-MLST-001) and the Partner Integration license (IPC-311-MLST01).
- Once you have the OpenAccess license, go to the License Administration app on the OnGuard server. Go to Start > All Programs > OnGuard (X.X), select License Administration and then log in.
- On the left side of the web interface select Install new license.
- Upload the new license file to enable the OpenAccess features.
- 2. Verify that OpenAccess configuration in OnGuard.
- Go to Start > All Programs > OnGuard (X.X), select System Administration.
- In the System Administration client, go to the Administration menu and select System Options.
- Identify the host(s) running the Message Broker Service and OpenAccess services:

General System Options General Asset Options Video Options Rabb	иМQ
Log on authorization warning	FIPS mode
None v Text	Enable FIPS-mode controller encryption
DataCondulT service	Configuration Download Service host
Generate software events	→ Browse
	Message Broker Service host
	MJT-OG82.CUSTOMDEVELOPMENT.MILESTO Browse
Monitoring	OpenAccess host
3 Number of days to save queued events	MJT-OG82.CUSTOMDEVELOPMENT.MILESTO Browse
Specify monitor zone assignments	Generate software events
Linkage Server host	Default Badge Printing Service host
OG82.CUSTOMDEVELOPMENT.MILESTO V Browse	Browse
Reporting and Dashboards Service Host	Port number for IP Client connection
Browse	3001
Cumulus Service URL	
https://identity.cumulus.s2sys.com Link	
Modify	Help Close

• On the host(s), confirm that the following services are all running:

OnGuard Service Name	Known Good Service Locations
LS Message Broker	On the identified host
LS OpenAccess	On the identified host

LS Web Service	By default LS Web Service runs on the same host as the LS OpenAccess service.
LS Event Context Provider	Must run on the same host as the LS OpenAccess service
LS Web Event Bridge	By default LS Web Event Bridge runs on the same host as the LS OpenAccess service.

- 3. Verify prerequisites installed to support the 3.6 version of the OnGuard XProtect Access plug-in.
- Each downloadable .ZIP file available at download.milestonesys.com/lenels2xpa has a prerequisites folder containing any required installation programs.
- 4. Upgrade your OnGuard XProtect Access Plugin to Version 3.6.
- Always upgrade the ACM Server and the OnGuard ACM plugin on the OnGuard machine before upgrading the XProtect Event Server ACM MIP plugin.
- On the OnGuard Server, first install the Milestone ACM Server.
- Second, install the Milestone ACM Server: OnGuard Plugin.
- Lastly, move to the XProtect Event Server and install the XProtect Event Server ACM MIP Plugin.
- Here is the order of installation for all three software components of the plug-in:
- 1 🛃 Milestone.ACMServer.x64.msi
- 2 🛃 Milestone.ACMServer.OnGuard.msi
- 3 B Milestone.ACMServer.MipPlugin.msi
- Refresh the configuration on the OnGuard XProtect Access instance in the Management Client.
- Now, the active OnGuard XProtect Access instance is using OpenAccess connection mode, and running version 3.6.
- An upgrade directly to version 4.3 is supported.
- 5. Verify the prerequisites are in place to support version 4.3.
- 6. On the OnGuard Server first install the OnGuard XProtect Access Service.
- 7. Next move to the XProtect Event Server and install the OnGuard XProtect Access MipPlugin.
- 8. Refresh the configuration on the OnGuard XProtect Access instance in the Management Client and reconfigure the connection properties in the **General Settings** tab as required.
- 9. Reconfigure any rules triggered by access control events or event categories. Read: Access control rules stop working after upgrade to 4.0 or newer. on page 102

Uninstalling the integration

When uninstalling the integration software to revert to an older version, please refer to Integration version downgrades on page 100.

When uninstalling both the OnGuard XProtect Access MipPlugin software and the XProtect Event Server on the same server, it's required to first uninstall the OnGuard XProtect Access MipPlugin components and uninstall the Event Server afterward. If the Event Server is uninstalled first, the integration software fails to uninstall.

Below is the process required to uninstall the current version of the plugin:

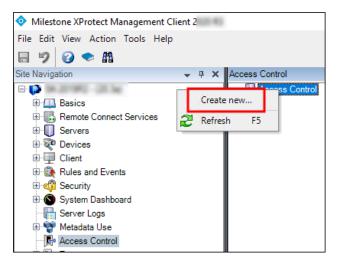
- 1. Go to the **Programs and Features** menu on the Milestone server.
- 2. Uninstall the Milestone OnGuard XProtect Access plug-in.
- 3. Go to the **Programs and Features** menu on the OnGuard server.
- 4. Uninstall the Milestone OnGuard XProtect Access service.

XProtect Management Client Configuration

XProtect Access instance creation wizard

After installing the OnGuard XProtect Access MipPlugin on the XProtect Event Server, create the access control instance in the XProtect Management Client.

1. Right-click the Access Control root node and select Create new... to begin the wizard.



2. Enter a name for the instance and select the Integration plug-in. Select the plug-in named LenelS2 OnGuard.

Create Access Control Sy	rstem Integration		x
Create access	control system integration		
Name the access cor	ntrol system integration, select the integration plug-in and enter the connection det	ails.	
Name:	Your Name Here		
Integration plug-in:			~
	LenelS2 OnGuard		
		Next	Cancel

 After naming and selecting the plug-in there are a set of required credentials, parameters, and options to complete. These fields define the connection to the OnGuard server. All properties for all supported versions of OnGuard are in the Management Client wizard.

Create Access Control System Integration		x
Create access control system integ	ration	
Name the access control system integration, select t	he integration plug-in and enter the connection details.	
Name:	lab	
Integration plug-in:	LenelS2 OnGuard	~
XProtect Access Service - Host:		\wedge
XProtect Access Service – Port:	8443	
XProtect Access Service – SSL Certificate Validation:		
OpenAccess – Host:		
OpenAccess – Port:	8080	
OpenAccess - SSL Certificate Validation:		
OpenAccess – User:		
OpenAccess – Password:		
OpenAccess – Directory:		
Options - OnGuard Web Administration URL:		
Options – Disable Commands:	\checkmark	~
	·	
	Next	Cancel

• Below are the fields required to establish the connection. It's possible to populate any field at this step in the process, the fields listed are the minimum required.

Empty Field Names	Required Values
XProtect Access Service - Host:	Hostname of the OnGuard server or the Integration server.
XProtect Access Service - Port:	Default port is 8443.
OpenAccess - Host:	IP address for the OnGuard server.
OpenAccess - Port:	Default port is 8080.
OpenAccess - User:	SSO user defined in OnGuard
OpenAccess - Password:	Password for the SSO user in OnGuard.
OpenAccess - Directory:	Directory for the SSO user in OnGuard.

4. After connection, the wizard imports data from the OnGuard server. This includes **Doors**, **Units**, **Servers**, **Events**, **Commands**, and **States**. Click **Next**.

ate Access Control System Integration			
Connecting to the access control syste	m		
Collecting configuration data			
Configuration successfully received from access control sy	stem	•	
			1
Added:			
Doors (1025)		•	
Units (7070)		•	
Servers (1)		•	
Events (1938)		•	
Commands (13)		•	
States (48)		•	
			1
		evious Next Car	nce

5. Associate doors with cameras. Select a camera and drag it to a door.

reate Access Control System Integration			x
Associate cameras Drag cameras to the access points for e Client when access control events relate		. The associated cameras are used in the XProtect Smart or's access points are triggered.	
Doors: All doors Name Door for 1000ID2-1320-2-0 Door for 1000ID2-1320-2-1 Access point: 1000ID2-1320-2-1 East Lobby Drop camera here to associate it wit	Enabled Lice	Cameras: IP-0A0004BD Dos Dos Cameras: Ops Cameras: Ops Ops Cameras: Ops Ops Cameras: Cameras:	
Door for 1000-ID1-1320-0-0 Door for 1000-ID1-1320-0-1 Door for 2000 ID0-1320-8-0 Door for 2000 ID0-1320-8-1 Door for 2000 ID0-Series-1-1300-0-0	✔ Per ✔ Per ✔ Per ✔ Per ✔ Per ✔ Per ✔ Per		
		Previous Next Can	el

- 6. Click Next after association of doors and cameras.
- 7. The configuration is saved, and the wizard ends.

XProtect Access instance status & properties

Go to the Access Control menu in the directory tree of the XProtect Management Client. You can view status of all instances by selecting the root of the Access Control directory.

Milestone XProtect Management Client					
File View Action Maintenance Tools Help					
🗟 🦻 🕝 🗢 🏛					
Site Navigation 👻 👎 🗙	Access Control 🗸 🗸	Access C	Control Inform	nation	
🛱 🛄 Basics 🔺	Access Control				
Elicense Information	lab	A	ccess (Control:	
Site Information					
E Remote Connect Services				Connection	Connection
Axis One-click Camera Connection		Enable	Name	Status	Information
			lab	Connected	

Select your OnGuard XProtect Access instance to view or edit the properties of the connection.

General settings	
Enable:	\checkmark
Name:	lab
Description:	
Integration plug-in:	LenelS2 OnGuard (Version: 4
Last configuration refresh:	10/31/2 2:03 PM
	Refresh Configuration
Operator login required:	
XProtect Access Service - Host:	MJT-LNLS2
XProtect Access Service - Port:	8443
XProtect Access Service - SSL Certificate Validation:	\checkmark
OpenAccess - Host:	MJT-LNLS2.custdev.us
OpenAccess - Port:	8080
OpenAccess - SSL Certificate Validation:	✓
OpenAccess - User:	administrator
OpenAccess - Password:	Enter current password
OpenAccess - Directory:	custdev.us
Options - OnGuard Web Administration URL:	
Options - Disable Commands:	\checkmark
Options - States polling interval (seconds):	900
Options - [Legacy] OnGuard SQL Server hostname:	
Options - [Legacy] Connection Profile:	
Options - Enable performance metrics (diagnostics):	

Descriptions for all properties listed below:

Property Name	Description - Purpose
Enable:	Selected by default. Remain selected to keep connection properties active.
Name:	Custom name field.
Description:	Reference information field.
Integration plug- in:	Displays the current version of the OnGuard XProtect Access MipPlugin.
Last configuration refresh:	Displays the date and time of the last system configuration refresh.
Operator login required:	Not selected by default. Select this option to enable the personalized login feature.
XProtect Access Service - Host:	Host name of the OnGuard server or the Integration Server hosting the OnGuard XProtect Access Service.
XProtect Access Service - Port:	8443 is the default port.
XProtect Access Service - SSL Certificate Validation	Not selected by default. Choose this option to secure communication between the OnGuard XProtect Access Service and the XProtect Event Server.
OpenAccess - Host:	IP address of the machine hosting the OnGuard OpenAccess service in non-encrypted scenarios. This field must use fully qualified domain name (FQDN) of the server to support SSL authentication. See the note below for scenarios where the OpenAccess service and the XProtect Access Service are installed on the same server.
OpenAccess - Port:	The port the OnGuard OpenAccess service is listening on. 8080 is the default port.
OpenAccess - SSL Certificate Validation	Not selected by default. Choose this option to secure communication between the OnGuard XProtect Access Service and the OnGuard OpenAccess Service.
OpenAccess - User:	An OnGuard administrative user to log into the OnGuard OpenAccess web service. This user should have access to all hardware, cardholders, etc in the system. Windows user account if using Directory users, OnGuard internal user account if using internal directory.

OpenAccess - Password:	The password of an OnGuard user to log into the OnGuard OpenAccess web service. In XProtect versions 2021 R1 and newer, after entering the password, this field is replaced by the Enter current password button in the General Settings tab. If the SSO user account is changed to update the integrated hardware device set, or the current user's password needs updating - click the button to open a dialog box. Enter current password Selecting Enter will also save the current access control configuration. OpenAccess – Password: Enter Cancel
OpenAccess - Directory:	The name of the OnGuard directory used for logging into the OnGuard OpenAccess web service. If left blank, the OnGuard internal directory is used.
Options - OnGuard Web Administration URL:	A URL for the OnGuard web-based administration portal. This field creates a link to the portal from the Smart Client Access Control workspace. By default the location for this URL is: https://HostName:8080/#/Login - Where "HostName" is the hostname of the OnGuard server.
Options - Disable Commands:	Selected by default. This option controls all command interaction between XProtect and OnGuard access control hardware devices.
Options - States polling interval (seconds):	Default value is 900 seconds. Frequency of status updates retrieved for AC hardware devices. Increase this value for more consistent event processing throughput.
Options - [Legacy] OnGuard SQL Server hostname:	SQL server hostname in systems upgraded from 3.X versions to the current 4.X version which doesn't require a SQL server hostname to establish the connection.
Options - [Legacy] Connection Profile:	This value is automatically filled for systems upgrading to 4.1 or newer versions of the integration from a 4.0 or older version.
Options - Enable performance metrics (diagnostics):	Not selected by default. Select this option to include performance statistic logging on event metadata.

You can verify that the integration module is now connected by looking at the access control tree.

In scenarios where the OpenAccess service and the XProtect Access Service are located on the same server, the **OpenAccess - Host** field must contain the PC name of the server where the OpenAccess service is installed in order to use SSL encryption between the OpenAccess service and the Event Server. In these scenarios the process used to create the certificate specifies the PC name, and any other method of identification for the server - such as the IP address or the fully qualified domain name - will not work. Make sure to match the PC name with the data entered in the **OpenAccess - Host** field.

Personalized login explained

Personalized login is an optional feature of XProtect Access. Personalized login links OnGuard user privileges to the access control hardware, events, and alarms available in the XProtect Access integration.

When a user logs into Smart Client, the personalized login feature presents a second login procedure that authenticates with the integrated OnGuard system. When the user presents valid OnGuard credentials, the Smart Client's XProtect Access features are narrowed to access control hardware, events, and alarms within that user's OnGuard privileges.

Personalized login manages two configurations. First, is the global configuration used by the Management Client. Second, is the personalized configuration used in the Smart Client. Personalized configurations are subsets of the global configuration. This helps control accuracy of event handling, command execution, and device management.

Personalized login has specific requirements:

- OnGuard 7.4 or higher
- XProtect Access 3.5 or higher

Enabling or disabling personalized login

Enable or disable personalized login for a specific access control plug-in in the Management Client. The option is located in the general settings menu and is titled **Operator login required**:

General settings	
Enable:	\checkmark
Name:	lab
Description:	
Integration plug-in:	LenelS2 OnGuard (Version: 4
Last configuration refresh:	10/31/20
	Refresh Configuration
Operator login required:	
XProtect Access Service - Host:	MJT-LNLS2
XProtect Access Service - Port:	8443
XProtect Access Service - SSL Certificate Validation:	\checkmark
OpenAccess - Host:	MJT-LNLS2.custdev.us
OpenAccess - Port:	8080
OpenAccess - SSL Certificate Validation:	\checkmark
OpenAccess - User:	administrator
OpenAccess - Password:	Enter current password
OpenAccess - Directory:	custdev.us
Options - OnGuard Web Administration URL:	
Options - Disable Commands:	✓
Options - States polling interval (seconds):	900
Options - [Legacy] OnGuard SQL Server hostname:	
Options - [Legacy] Connection Profile:	
Options - Enable performance metrics (diagnostics):	

After choosing to enable or disable this feature, make sure to save your changes in the Management Client.

Logging into Smart Client with personalized login

After you launch the Smart Client and login, the personalized login feature presents a second login dialog for OnGuard.

	Log into access con	ntrol
	4.	
	User name	THEFT
	custdev.us\xtian	-
	Password	1235
Ŋ	Remember password	1
	Auto-login	

OnGuard requires three pieces of data during this exchange:

- 1. directory
- 2. user name
- 3. password

The XProtect Smart Client dialog has fields for user name and password. Enter the directory with the user name in this format:

DirectoryName\UserName

If no directory is provided, the OnGuard internal directory is used. OnGuard can use special non-alphanumeric characters, control characters, and spaces in directory names. Use of these characters isn't compatible with XProtect. If these types of characters are included in the OnGuard directory, authentication fails.

After entering the directory/user name and password, the XProtect Smart Client validates the credentials with the OnGuard system. If you click **Skip this step**, the Smart Client opens without using personalized login, and no XProtect Access features are available in the Smart Client. After authentication with OnGuard, Smart Client loads a personalized configuration. The Smart Client displays access control information from the user account that logged in during the personalized configuration login dialog. This includes:

- · Alarms related to hardware the user has privileges to view
- · Events related to hardware the user has privileges to view
- · Devices in the map element selector that the user has privileges to view

Refreshing personalized login

The XProtect Event Server stores personalized configurations for XProtect Smart Client users. Stored personalized configurations vanish when the Event Server restarts. When the global configuration of the XProtect Access instance refreshes, the Event Server updates all stored personalized configurations. Changes to this configuration can cause error messages for users logged into the Smart Client. Below, are two possible error messages, known causes, and how to fix them.

	rotect Smart Client				
Views	Exports	Search	Alarm Ma	nager	Incidents
» < Selec	t view >	~	19 19		
2:49:18 PM	The configuration of the	access control system	'MJT-LNLS2' has bee	n changed. You o	an continue working
-	rror message that t nent configuration fo	-			n a modified
-	nent configuration fo	-			n a modified
OnGuard segm	nent configuration fo	or the current log	iged in operator		n a modified Access Control

Commands explained

Commands in the XProtect Access OnGuard integration interact with access control devices. By default, commands are disabled in the plugin configuration. This can be changed in the XProtect Management Client by clearing the **Options - Disable Commands** checkbox.

If commands are turned off, none of the command features work, however it's still possible to view command buttons in the Smart Client and create rules in XProtect which use commands. These rules validate, and the buttons appear, but nothing happens. In the Smart Client users receive the following error message:

HH:MM:SS AM/PM Failed to perform the access control command '**COMMAND**' on '**DEVICE**'. Error Message: Commands are disabled. Modify the plugin configuration in the XProtect Management Client to enable commands.

Ø Milestone XProtect Smart Client		
Views Exports Search Alarm Manager Incidents	Access Control	System Monitor
		Acce
⊗ 2:57:56 PM Failed to perform the access control command 'Open' on 'Door for MJT	-One'. Error message: Comm	ands are disabled. Modify t

Commands are used to trigger state changes in the access control hardware devices. Commands trigger in four ways with the XProtect Access OnGuard integration:

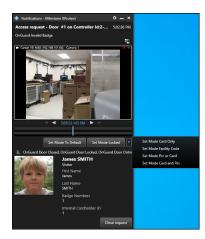
- 1. The XProtect rules system can trigger commands.
- 2. Access request notifications can include commands.
- 3. Any location in the Smart Client where doors are visualized, such as the access monitor or the access control workspace, can contain command buttons.
- 4. The map interface within the XProtect Smart Client can include access control device icons which can be used to trigger commands.

Supported commands reference

The following are the devices and their supported commands.

Readers:

- Set Mode To Default
- · Set Mode Locked
- Set Mode Unlocked
- · Set Mode Card Only
- Set Mode Pin or Card
- Set Mode Card and Pin
- · Set mode Facility Code



Set Mode commands for readers change the authentication mode the reader responds to. For example: a rule can switch readers into unlocked mode during business hours.

Reader Inputs:

- Mask
- Unmask

Reader Outputs:

- Activate
- Deactivate
- Pulse

Manage Rule				-		×
Name:	Flash Exterior Door Lights					
Description:						
Active:						
	S	tep 3: Actions				
Select actions to per	form					
Set Mode Card O						^
Set Mode Pin or						
Set Mode Eacility	Code (Reader)					
Mask disput> Pulse (Output>						
Set Mode Card a	nd Pin (Reader)					
Unmask <input/>						
Activate <output< td=""><td>></td><td></td><td></td><td></td><td></td><td></td></output<>	>					
Deactivate <out< td=""><td></td><td></td><td></td><td></td><td></td><td></td></out<>						
Show <access re<="" td=""><td>equest notification></td><td></td><td></td><td></td><td></td><td>¥</td></access>	equest notification>					¥
Edit the rule descrip	tion (click an underlined item)					
Perform an action on	Pulse Exterior Door Outputs					_
from External						
Pulse Output 1 for rea	ader1					
L'						
Help	Cancel	< Back	Next >		Finish	

Reader inputs have a state of masked or unmasked. A masked input doesn't report or save status in the OnGuard system. The masked input also has a "mask" icon attached to its own icon on the Smart Client map. Unmask enables status of that input to be reported and saved within OnGuard, and removes the mask icon. Reader outputs are activated, de-activated, and pulsed using the respective commands. The **Pulse** command activates the output temporarily, then deactivates it. An activated output has a red circle icon attached to it when viewed on the Smart Client map.

Doors:

Open



Doors are opened via the command. When the door opens, the door icon animation displays this status on the Smart Client map.



Administrative Configuration

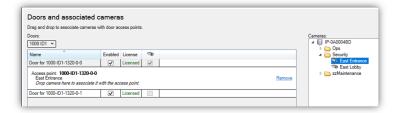
Door & camera association

In the **Doors and Associated Cameras** menu of the XProtect Access Instance it's possible to verify the status of all connected doors, and create, reassign, and remove the association between cameras and doors. Doors require associated cameras to view live and recorded video - and listen to or play audio through any XProtect client that supports visualization of doors.

1. Open the doors list and select a panel to view all doors connected to that panel.

Access Control Information	
Doors and associated cameras	
Drag and drop to associate cameras with door access points.	
Doors:	
1000 ID1 V	
All doors 2220 ID0 2220 ID0 License	
1000 ID2 1000 ID2 3000 Primary IP.2nd 485 ID3 xccess point	Remove
LNL-2000_06-124 LNL-1000_10-204 LNL-1000_10-210	
LNL-1000_10-212 LNL-1000_10-220	
ll.	

- 2. Select a door. A list of all associated cameras appears under the door object.
- 3. Select a camera from the **Cameras** list on the right and drag the selected camera into the list of cameras associated to the chosen door.



4. Click the **Remove** link if you need to end the association between the camera and the door.

Categorize events

Large scale access control systems, such as those managed by OnGuard, need to functionally integrate with XProtect without programming large numbers of individual alarms and rules. Categorizing access control events minimizes the number of individual alarms and rules requiring programming.

The latest update for the OnGuard XProtect Access integration (4.4 CU1), supports OnGuard custom alarm definitions. These customized combinations of devices and events can be created in the Alarm definition tab of the Monitoring > Alarms menu in the OnGuard System Administration client. The **Name** field of the alarm definition is what will appear customized in XProtect. The format of the event message displayed in XProtect is as follows:

OnGuard 'custom name text' (OnGuard event used to trigger the custom alarm)

Once the integration has been upgraded to the 4.4 CU1 version, refreshing the configuration of the XProtect Access instance in the Management Client will import any events created from OnGuard customized alarm definitions. You can find the events listed in alphabetical order in the Access Control Events tab of the XProtect Access menu in the Management Client.

. U	pdate Configuration	×
L L	Jpdate Configuration	
C	ollecting configuration data	
c	onfiguration successfully received from access control system.	
	Added:	
	Events (1) OnGuard You May Enter (Access Granted Entry Made)	
	Apply Cancel	

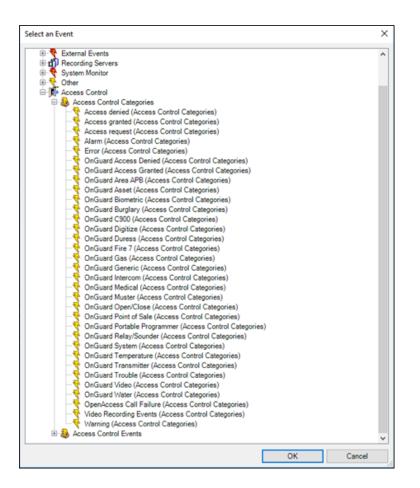
Categorize events to generate XProtect alarms or rule-based actions triggered by any OnGuard event from the chosen category. For example, the integration can start recording video based on any number of unique OnGuard hardware events: "Door Forced," "Denied, Badge Not in Panel," and "Access Denied Unauthorized Entry Level." Categorize the events, then create a rule to start recording based on events from that category.

- 1. Go to the Access Control Events tab of the XProtect Access instance in the Management Client.
- 2. Select an event, and choose a category from the Event Category list.
- 3. Apply the same category to any number of events.
- 4. When creating rules and alarms within XProtect, if you choose an **Access Control Category** as the trigger, any of the events that are in the chosen category cause the rule or alarm to happen.
- 5. Alarms and Rules in XProtect can trigger using any category of event.

Alarm Access Control Event Categories list:

Name: Veloo Recording Event Instructions: Veloo Recording Event Instructions: Togger Togger Toggering event: Rocess Control Event Categories OrGund Terminiter OrGund Access Granted OrGund Field Field OrGund Field Field OrGund Field Field OrGund Field Fiel		
Name: Video Recording Event Instructions: Video Recording Event Instructions: Togor Togor Togor Sources: Access Control Event Categories OrGund Access Control Event Categories Concur Access Control Event Categories Concur Access Control Event Categories Concur Access ArB a Concur Acc	Alam definition	
hetuctions:	Enable:	
Tigger Taggering event: Access Control Event Categories OrGund Transitter OrGund Access Cartel Event Categories OrGund Cartel Event Categories OrGund Cartel Event Categories OrGund Cartel Event Categories Activation pende OrGund Cartel Event Categories OrGund Cartel OrGund OrGund Cartel OrGund OrG	Name:	Video Recording Event
Tageing event: Access Cartool Event Categories Sources: OrGued Travention Sources: OrGued Categories Activation petiod Councy Asset Counc	Instructions:	
Tageing event: Access Cartool Event Categories Sources: OrGued Travention Sources: OrGued Categories Activation petiod Councy Asset Counc	Tricoer	
Sources: OrGued Access Granted OrGued CS00 OrGued CS00 OrGued CS00 OrGued CS00 OrGued Grante OrGued Grante OrGued Grante OrGued Access Granted OrGued Grante OrGued Access Granted OrGued Access Granted OrGued Access Granted OrGued Fre 7 OrGued Access Granted OrGued Grante OrGued Grante OrGued Access Granted OrGued Grante OrGued Access Granted OrGued Access Granted OrGued Grante OrGued Grante OrGued Grante OrGued Access Granted OrGued Transmitter OrGued Grante OrGued Grante OrGued Grante OrGued Transmitter OrGued Transmitter OrGued Transmitter OrGued Ware Orgued Transmitter OrGued Ware Orgued Transmitter OrGued Ware Orgued Ware Orgued Transmitter Orgued Ware		
Sources: OrGund Access Carried OrGund Aces APB OrGund Aces APB OrGund Aces APB OrGund Aces APB OrGund Aces APB OrGund Search OrGund Search OrGund Search OrGund Dates OrGund Dates OrGund Dates OrGund Dates OrGund Dates OrGund Fire 7 OrGund Fire 8 OrGund Gene OrGund Fire 7 OrGund Fire 8 OrGund Gene OrGund Fire 7 OrGund Fire 8 OrGund Gene OrGund Fire 7 OrGund Fir	Triggering event:	Access Control Event Categories
Source: OrGuard Area APB Activation period OrGuard Area APB Activation period OrGuard Area OrGuard Area Activation period OrGuard Source OrGuard Mate OrGuard Mate OrGuard Mate OrGuard Mate OrGuard Source OrGuard Sou		
Activation period OnGund Assist OnGund Sensitive OnGund Sensitive Operation action required OnGund Tennether Events toggered: Warning Other Sensitive Nam ontogory: Sensitive Events toggered by alarm: Sensitive And Colors adam Sensitive	Sources:	
Activation period OnGuid Bonetice OnGuid Bonetice OnGuid Burgery Texp rote: OnGuid Greet OnGuid Gree		
The profile: OnGued Burgley OnGued Burgley OnGued State OnGued State OnGued State OnGued State OnGued State OnGued File 3	Activation period	OnGuard Biometric
Che profile: CrGuard CS00 CrGuard CS00 CrGuard CG00 CrGuard CG00 CrGuard CG00 CrGuard CG00 CrGuard CG00 CrGuard CG0		OnGuard Burglary
CrGuard Digitize CrGuard Digitize CrGuard Digitize CrGuard Digitize CrGuard Dires CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Maca CrGuard Maca CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Maca CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Gires CrGuard Maca	 Time profile; 	OnGuard C900
Child Construction OnGuided File 7 OnGuided File 8 OnGuided File 8 Map OnGuided File 8 OnGuided File 8 OnGuided File 8 An atam only appears on the smatt map if at least OnGuided File 6 OnGuided File 6 Atam manager view: OnGuided File 6 OnGuided File 7 OnGuided File 6 OnGuided File 7 OnGuided File 6 OnGuided File 7 OnGuided File 7 Onguided Temperature OnGuided Temperature OnGuided Vision OnGuided Vision OnGuided Vision OnGuided Vision Onformed OnGuided Vision Onformed Vision OnGuided Vision Onformed Vision OnGuided Vision Onformed Vision OnGuided Vision Onformed Vision OnGuided Vision Onformed Vi	0	OnGuard Digitize
CrGuard Fire 7 CrGuard Greet CrGuard Greet CrGuard Greet CrGuard Greet CrGuard Greet CrGuard Greet CrGuard Madea CrGuard Greet Aba CrGuard Madea CrGuard Greet Aba CrGuard Madea CrGuard Greet Aba CrGuard Greet Aba CrGuard Greet Aba CrGuard Greet Aba CrGuard Madea CrGuard Greet Aba CrGuard Greet Aba CrGuard Greet Aba CrGuard Greet Aba CrGuard Madea CrGuard Greet Aba CrGuard Madea Cr	Event based:	OnGuard Duress
Or-Guad Fire 9 Map Or-Guad Gas Or-Guad Gas Or-Guad Gas Time Int: Or-Guad Gas Or-Guad Gas Or-Guad Gas Or-Guad Gas Or-Guad Gas Intel Islam onner: Intel Islam Intel Islam onner: Intel Islam Nam category: Intel Islam Everta toggead by alam: Intel Islam Ano I	0.00000	OnGuard Fire 7
Map OrGund Gas OrGund Gase OrGund Macha Aam manager view: OrGund Macha Aam manager view: OrGund Orgund Macha OrGund Macha OrGund Macha OrGund Macha OrGund Macha OrGund Gase O		OnGuard Fire 8
Mac OrGund Genetic OrGund Heat Heat Heat Heat Heat Heat Heat Heat		
An alarm only appears on the smatt map if all least Chicard Hote Messages OnGund Hote Messages Message OnGund Hote Messages Messages OnGund Hote Messages Messages OnGund Hote Message Messages Message		
An alam only appears on the smatt map if at least On-Guard Veteriors On-Guard Medical On-Guard Medical On-Guard Medical On-Guard Medical On-Guard Medical On-Guard Medical On-Guard Point State On-Guard State	Мар	OnGuard Generic
Alam manager view: OrGund Mada OrGund Mada OrGund Mada OrGund Mada OrGund Mada OrGund Mada OrGund Mada OrGund Mada OrGund System OrGund Temmitter OrGund Vison OrGund Vison	• • • • • • • • • • • • • • • • • • • •	OnGuard Host Messages
Alam manager view: OrGund Muster OrGund Sport Alex OrGund Sport Alex OrGund Sport Alex OrGund Sport Alex OrGund Sport Alex OrGund Sport OrGund Sport	An alarm only appears on the smart map if at least	
Nam manager view: Orticited Open Close On Guard Port of Sale On Guard Transmiter On Guard Tr		
OnGuard Point of Sale OnGuard Point of Sale OnGuard Points Programmer OnGuard Related map. OrGuard Teaching Points Operator action required OnGuard Trucking OrGuard Trucking Operator action required OnGuard Teaching OrGuard Teaching Operator action required OnGuard Teaching OrGuard Teaching Dentor action required Operator action required Initial alarm porty: I: High Ator cores alarm:		OnGuard Muster
OnGuard Potable Programmer OnGuard Potable Programmer OnGuard System are OrGuard System are OrGuard Travaiter Intel Intel Intel Intel Intel Intel Intel Potable Intel Int	Alam manager view:	OnGuard Open/Close
OnGuid Rely/Sounder OnGuid Rely/Sounder OnGuid System Operator action required Operator action required OnGuid Vision OrGuid Vision OnGuid Vision Operator action required Obser Weining Phila Islam onner: Initial alam onner: Initial alam onner: Events triggered by alam: Events triggered by alam:		OnGuard Point of Sale
Related map: OrGuad System Operator action required OrGuad System Operator action required OrGuad Trachate OrGuad Vision OrGuad Vision Charles of the system OrGuad Vision OrGuad Vision OrGuad Vision OrGuad Vision OrGuad Vision OrGuad Vision OrGuad Vision OrGuad Vision OrGuad Vision Other Orguad Vision Nation actions: Intel action owner: Intal alarm porty: 1: High Alar octore dam: Intel Action of Statement		Unguard Portable Programmer
Operator action required Orduard Transmitter Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Order Waning Other Related cameras: Initial alam conner: Initial alam conner: Initian conner: Initian conner: Initian conner: Initian conn		OnGuard Helay/Sounder
Operator action required Orduard Transmitter Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Orduard Touble Order Waning Other Related cameras: Initial alam conner: Initial alam conner: Initian conner: Initian conner: Initian conner: Initian conn	Related map:	OnGuard System
Operator action required On-Guard Trouble On-Guard Vision On-Guard Vision On-Guard Vision On-Guard Vision On-Guard Vision Order Vision Paulee Vision Recording Events Warring Other Initial alarm owner: Initial alarm owner: Initial alarm protety: Initial alarm protety: Initial alarm owner: Initial alarm	i name a map.	OrGuard Transmitter
Time limit: OnGuind Video OnGuind Video OpenAccess Call Failure OpenAccess Call Failure Video Recording Events Weiming Initial alam owner: I Initial alam	Operator action required	
Interaint. OnGuid Waier Concess Cal Failure Video Recording Events Waring Other Recording Events Waring Events Waring Events Initial alam promy: 1: High Alam category: Events triggered by alam: Acto close alam:		
Everts triggered: OpenAccess Call Faure Weening Other Weening Related cameras:	Time limit:	
Events triggered: Video Recording Events Other Warring Related cameras:		
Other Warring Polated cameras: Initial alam owner: Initial alam pootty: Initial alam pootty: Initial alam category: Alam category: Alam category: Alam category: Alam category: Alam category: Initial alam: Initia	Events triggered:	
Other Constraints		
Initial alam owner: Initial alam pitority: Nam category: Events triggened by alam: Auto close alam:	Other	
Initial alam protty: 1: High Alam category: Events triggered by alam: Auto-close alam:	Related cameras:	
Alam category:	Initial alarm owner:	
Events triggered by alarm:	Initial alarm priority:	1: High
Events triggered by alarm:	Nam extenses:	
Auto-close alam:	nam calegoly:	
	Events triggered by alarm:	
Alarm assignable to Administrators:		
	Auto-close alarm:	

• Rule Access Control Categories event list:



Access control event categories

Below is the list of all access control event categories.

Default XProtect Access events:

- Access Granted
- Access Request
- Access Denied
- Alarm
- Error
- Warning

OnGuard events:

- OnGuard Access Denied
- OnGuard Access Granted
- OnGuard Area ABP
- OnGuard Asset
- OnGuard Biometric
- OnGuard Burglary
- OnGuard C900
- OnGuard Digitize
- OnGuard Duress
- OnGuard Fire 7
- OnGuard Fire 8
- OnGuard Fire 9
- OnGuard Gas
- OnGuard Generic
- OnGuard Host Messages
- OnGuard Intercom
- OnGuard Medical
- OnGuard Muster
- OnGuard Open/Close
- OnGuard Point of Sale
- OnGuard Portable Programmer
- OnGuard Relay/Sounder
- OnGuard System
- OnGuard Temperature
- OnGuard Transmitter
- OnGuard Trouble
- OnGuard Video
- OnGuard Water
- OpenAccess Call Failure

Custom events:

• User Defined Category...

To create a user-defined category, there is a **User-defined Categories** button on the bottom left corner of the **Access control events** menu.

1. Click the User-defined Categories button to create your own custom event category.

ess control events			
ie the events you want to monitor in XProtect Smart Client. Use categories to si	mplify the use of triggering events.		
able all Disable all			
bled Access Control Event	Source Type		Event Category
OnGuard 24 Hour Alarm	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
OnGuard 24 Hour Alarm Restore	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
OnGuard 24 Hour Auto Test	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
5 OnGuard 24 Hour Non-Burglary Alarm	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
OnGuard 24 Hour Non-Burglary Alarm Restore	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
OnGuard 24 Hour Report Closed	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
OnGuard 24 Hour Report Open	Alarm Panel, Door, Input, Output, Pane	el, Reader	Alarm, OnGuard Trouble
OnGuard 24 Hour Zone Bypassed	Alarm Panel, Door, Input, Output, Pane		Alarm, OnGuard Trouble
OnGuard 24 Hour Zone Unbypassed	ies X and	el, Reader	Alarm, OnGuard Trouble
Unduard 30 Minutes Since Paldack Comm	100	el, Reader	OnGuard System
OnGuard 32 Hour Event Log Marker Name		el, Reader	Alarm, OnGuard System
OnGuard Abort	Pare	el, Reader	OnGuard System
OnGuard AC Battery Fail	Remove Pare	el, Reader	OnGuard System
OnGuard AC Restore		el, Reader	OnGuard System
OnGuard AC Trouble		el, Reader	OnGuard System
OnGuard Accepted Biometric Score		el, Reader	OnGuard Biometric
OnGuard Access Closed		el, Reader	OnGuard System
OnGuard Access Code Used		el, Reader	OnGuard System
OnGuard Access Denied		el, Reader	Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied (access_denied 1		el, Reader	Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied : AAM Timeout		el, Reader	Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied : AAM Validation F		el, Reader	Access deried, Access request, OnGuard Access Deried
OnGuard Access Denied Door Secured		el, Reader	Access deried, Access request, OrGuard Access Deried
OnGuard Access Denied Interlock	Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied Passback	Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied to Destination Floor	Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied Unauthorized Arming State	Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied Unauthorized Entry Level	Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied, OnGuard Open/Close
OnGuard Access Denied Unauthorized Time OnGuard Access Denied Linder Duress	Alarm Panel, Door, Input, Output, Pane		Access deried. Access request, OnGuard Access Deried
	Alarm Panel, Door, Input, Output, Pane		OnGuard Duress, Warning
OnGuard Access Denied: Access Control Format Not Found	Alarm Panel, Door, Input, Output, Pane		Access denied. Access request, OnGuard Access Denied
OnGuard Access Danied: Area Empt	Alarm Panel, Door, Input, Output, Pane		Access denied. Access request, OnGuard Access Denied
OnGuard Access Denied: Area Octubied	Alarm Panel, Door, Input, Output, Pane		Access denied. Access request, OnGuard Access Denied
OnGuard Access Denied: Asset Aquired OnGuard Access Denied: Biogentric Reader Office	Alarm Panel, Door, Input, Output, Pane Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied Access denied, Access request, OnGuard Access Denied
OnGuard Access Denied: Ord Expired OnGuard Access Denied, accet Teneout Expired	Alarm Panel, Door, Input, Output, Pane Alarm Panel, Door, Input, Output, Pane		Access denied, Access request, OnGuard Access Denied Access denied, Access request, OnGuard Access Denied
OrGuard Access Deniet Escort I medit Expired OrGuard Access Deniet Invalid Access Control Data	Alarm Panel, Door, Input, Output, Panel Alarm Panel, Door, Input, Output, Panel		Access denied, Access request, Unusing Access Denied Access denied, Access request, OnGuard Access Denied
Unuuard Access Denver: Invand Access Control Data	Asarm Hanel, Door, Input, Output, Pane	R, Pleader	Access bened, Access request, OnGuard Access Denied
ar-defined Categories			

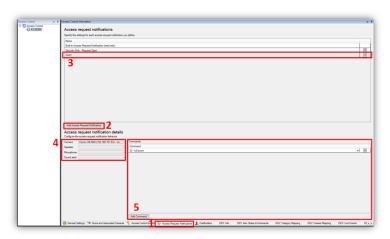
2. Click Add, name the category, and press OK. The user-defined category appears as an option in the Event Category list.

	control events		
te	events you want to monitor in XProtect Smart Client. Use categories to simple	fy the use of triggering events.	
le a	Disable all		
rd	Access Control Event	Source Type	Event Category
Т	OnSuard Access Denied : AAM Validation Failed	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied
1	OnGuard Access Denied Door Secured	Alarm Panel, Door, Input, Output, Panel, Reader	Access deried. Access request, OnGuard Access Deried
1	OnGuard Access Denied Interlock	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied
1	OnGuard Access Denied Passback	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied
1	OnGuard Access Denied to Destination Floor	Alarm Panel, Door, Input, Output, Panel, Reader	Access deried, Access request, OnGuard Access Deried
1	OnGuard Access Denied Unauthorized Arming State	Alarm Panel, Door, Input, Output, Panel, Reader	Access deried, Access request, Or/Guard Access Deried
1	OnGuard Access Denied Unauthorized Entry Level	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied, OnGuard Open/Close
1	OnGuard Access Denied Unauthorized Time	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied
1	OnGuard Access Denied Under Duress	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Duress, Warning
1	OnGuard Access Denied: Access Control Format Not Found	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied
1	OnGuard Access Denied: Area Empty	Alarm Panel, Door, Input, Output, Panel, Reader	Access deried. Access request, OnGuard Access Denied
1	OnGuard Access Denied: Area Occupied	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied, Access request, OnGuard Access Denied
1	OnGuard Access Denied: Asset Required	Alarm Panel, Door, Input, Output, Panel, Reader	Access deried. Access request, OnGuard Access Deried
1	OnGuard Access Denied: Biometric Reader Offline	Alarm Panel, Door, Input, Output, Panel, Reader	Access denied. Access request, OnGuard Access Denied
I	OnGuard Access Denied: Card Expired	Alarm Panel, Door, Input, Output, Panel, Reader	Al categories
	OnGuard Access Denied: Escort Timeout Expired	Alarm Panel, Door, Input, Output, Panel, Reader	
1	OnGuard Access Denied: Invalid Access Control Data	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Relay/Sounder
1	OnGuard Access Denied: Invalid Access Control Data Length	Alarm Panel, Door, Input, Output, Panel, Reader	ConGuard System
1	OnGuard Access Denied: Invalid Access Control Data Parity	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Temperature
1	OnGuard Access Denied: Invalid Access Control Data Type	Alarm Panel, Door, Input, Output, Panel, Reader	
	OnGuard Access Denied: Invalid Smart Card Authentication	Alarm Panel, Door, Input, Output, Panel, Reader	CircGuard Transmitter
1	OnGuard Access Denied: Invalid Smart Card Data	Alarm Panel, Door, Input, Output, Panel, Reader	OpSuard Trouble
1	OnGuard Access Denied: Invalid Smart Card Location	Alarm Panel, Door, Input, Output, Panel, Reader	
	OnGuard Access Denied: Invalid Smart Card Type	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Video
	OnGuard Access Denied: Invalid Timezone	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Inlater
1	OriGuard Access Denied: No Biometric Template	Alarm Panel, Door, Input, Output, Panel, Reader	Open/coess Call Failure
	Or:Guard Access Denied: No Occupant Approval	Alarm Panel, Door, Input, Output, Panel, Reader	
	OnGuard Access Denied: Reader Locked	Alarm Panel, Door, Input, Output, Panel, Reader	Video Recording Events
	OnGuard Access Denied: Secured Mode	Alarm Panel, Door, Input, Output, Panel, Reader	Warring
	OnGuard Access Denied: Smart Card Format Not Found	Alarm Panel, Door, Input, Output, Panel, Reader	
	OnGuard Access Denied: Unknown Code	Alarm Panel, Door, Input, Output, Panel, Reader	
	OnGuard Access Door Propped	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard System, Video Recording Events
	OnGuard Access Door Status Monitor Shunt	Alarm Panel, Door, Input, Output, Panel, Reader	OrGuard System
	OnGuard Access Door Status Monitor Trouble	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard System
	OnGuard Access Exit Request Trouble	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard System
	OnGuard Access Granted	Alarm Panel, Door, Input, Output, Panel, Reader	Access granted, Access request, OnGuard Access Granted
	OnGuard Access Granted - Anti-Passback Not Used	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Area APB
1	OnGuard Access Granted - Anti-Pasaback Used	Alarm Panel, Door, Input, Output, Panel, Reader	OnGuard Area APB
	ned Categories.		

Access request notifications

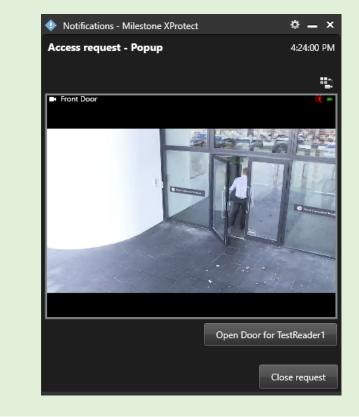
Access request notifications are pop-up notifications which appear in front of all other desktop applications for all users logged into the Smart Client with privileges to view XProtect Access features and devices. The XProtect Access integration includes a built-in access request notification. Use the **Access Request Notifications** menu to customize these notifications.

- 1. Go to the Access Request Notification menu.
- 2. Click the Add Access Request Notification button.
- 3. Name the new notification.
- 4. Associate cameras, speakers, microphones, and sounds.
- 5. Click the Add Command button and open the Command list to select which commands appear on the notification.



When the notification pops up on the desktop, a sound plays if you choose to include an audible notification. The built-in access request notification doesn't include a sound.

Access request notifications can trigger pop up notifications from the XProtect rules system, and these notifications don't need to be related to access control hardware devices.



Searching for cardholders explained

All active cardholders in the OnGuard system are imported to the integration. Active cardholders have one or more badge(s) with a status of "active." Search for cardholders in the **Cardholders** menu of the XProtect Access instance. First Name, Last Name, Badge Numbers, and Cardholder ID are all included in the search. As characters are typed in the box, searching begins:

earch for cardholders to view a pictur	e of the cardholder. The cardholder picture	is used in the XProtect S	emart Client, when an access o	control event has been register
17 🔞	The number of search results exceed the co	urrent limit. Enter more sp	pecific search criteria.	
Name	Туре	F	First Mid test1 6017	73
First Mid test1 60017	Employee	~ E	mployee	
First Mid test1 60117	Employee			
First Mid test1 6017	Employee			
First Mid test1 60170	Employee			
First Mid test1 60171	Employee		2	
First Mid test1 60172	Employee		3	
First Mid test1 60173	Employee	F	irst Name:	First
First Mid test1 60174	Employee		ast Name:	test1 60173
First Mid test1 60175	Employee		Aiddle Name:	Mid
First Mid test1 60176	Employee		ladge Numbers:	60173
First Mid test1 60177	Employee		allowed Visitors:	The
First Mid test1 60178	Employee		nternal Cardholder ID:	60173
First Mid test1 60179	Employee			
First Mid test1 60217	Employee		erson Record Last Changed:	12/11/1996 5:05:00 PM

Visibility of cardholder information, such as name and badge numbers, comes from the OnGuard database.

Edit the **PluginSettings.json** configuration file to change the data available within each cardholder record, and change the order of data display. To learn more read: Cardholder search data fields are missing, or out of order on page 106

Client profiles & Roles explained

Smart Client profiles and user roles in XProtect let administrators manage the features available in the XProtect Smart Client.

Smart Client profiles control visibility of access request notifications. Roles define visibility and control of access control features, visibility of the cardholder list, and access request notifications. For example, if a user can't receive access request notifications, their ability to receive notifications can be controlled in either their Smart Client profile or their role.

Managing client profiles & Roles

- 1. To manage Smart Client profiles:
 - Open the Management Client.
 - Expand Client and select Smart Client profiles.
 - The Access Control menu has the setting for notifications.

Smart Client profile settings - Access Control		
Title	Setting	Locked
Show access request notifications	Yes	× 🗆

- 2. To manage user roles:
 - Open the Management Client.
 - Expand Security and select Roles.
 - · Select the role to manage and click the Access Control menu to adjust the available settings.

Security settings	Milestone XProtect Access
Use access control View cardholders list Receive notifications	

The Receive notifications setting only applies to the XProtect mobile client.

Smart Client Features

Access control workspace explained

The XProtect Access OnGuard integration adds a new workspace, or tab, into the XProtect Smart Client. The **Access Control** workspace should appear in the Smart Client.

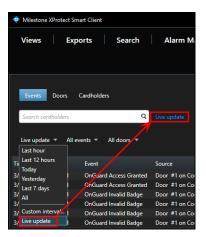
Milestone XProtect Smart Client					
Views Exports	Search	Alarm Manager	Incidents	Access Control	System Monitor

Use this workspace to search and filter the **Events**, **Doors**, and **Cardholders** categories. Select **Events**, **Doors**, or **Cardholders** to work with the list of events related to that category.

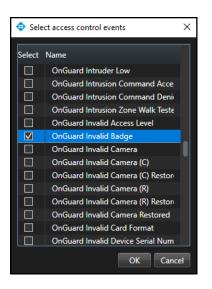
Access control workspace events

To display a list of events, first choose a time range, select a custom time range, or choose to display a live update list of events.

1. Choose the Live update time range to view a real-time display of access control events.



- 2. Filter for specific events including custom events and all integrated OnGuard events.
- Open the All events list and select the Access control event... option to open the Select access control events window.
 - Choose a specific OnGuard event from this list.



- 4. Filter for specific hardware devices.
- 5. Click the Access report button to create a PDF file of the events in the current list.

Milestone XProtect Sm	nart Client					_		×
Views Exp	orts Search	Alarm Manager	Incidents	Access Control	System Monitor	5:27:59 PM	la 🦂	
					ĺ	Access control admini	stration	
Events Doors	Cardholders							
Lifeins Doors	carditolders							
Search cardholders	q							
Last hour 🔻 OnGua	rd Invalid Badge 🔻 All do	ors 🔻		Access report				5
Time 👻	Event	Source	Access control system	Cardholder	StableFPS_T800 (localhost)	Camera 1 - 3/14/2023 5:01:	32.433 PM	0
3/14/2023 5:02:36 PM	OnGuard Invalid Badge	Door #1 on Controller Id:2	MJT-SIM23	James SMITH	10		-	
3/14/2023 5:01:32 PM	OnGuard Invalid Badge	Door #1 on Controller Id:1		James SMITH	part in Te	T. PS.	TRA.	1
3/14/2023 5:01:28 PM	OnGuard Invalid Badge	Door #1 on Controller Id:2	MJT-SIM23	James SMITH				18
3/14/2023 5:01:24 PM	OnGuard Invalid Badge	Door #1 on Controller Id:2	MJT-SIM23	James SMITH			and a	1
3/14/2023 5:01:15 PM	OnGuard Invalid Badge	Door #1 on Controller Id:2	MJT-SIM23	James SMITH	ST MAGE DAN	1 31 - CT	1"M' 2	
3/14/2023 4:41:36 PM	OnGuard Invalid Badge	Door #1 on Controller Id:1	MJT-SIM23	James SMITH	S B B B	1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	Sec. "	
							A 1	
					• •	5:01:32.454 PM	•	5:02 PM
					OnGuard Inv	alid Badge		(
					Time 3/14/2023 5:01:32 PM			

• In the Access report window: name the report, choose a destination to save the report, include comments, and select the option to include snapshots.

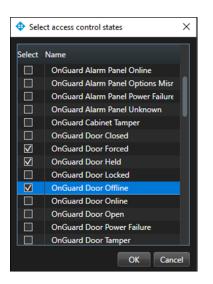


Access control workspace doors

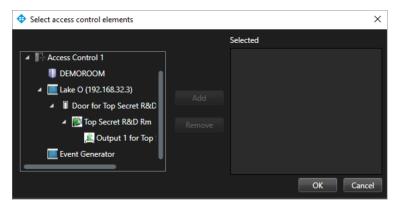
- 1. Open the **Door** list and select the access control hardware to display.
- 2. Choose the Access control type..., option to open the Select access control types window.
 - **Door** is the default option for this list. Use this menu to select servers, panels, and any access control hardware in the system.

Selection	ct access control types X
Select	Name
	ACServer
	AlarmPanel
	Door
	Input
	Output
	Panel
	Reader
	OK Cancel

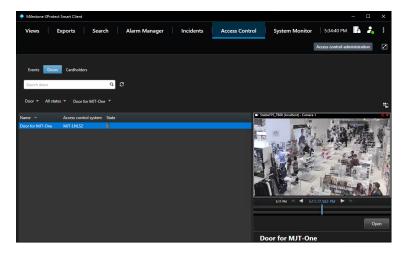
- 3. Open the All states list to filter hardware by status.
- 4. Choose the Access control state..., option to open the Select access control states window and select from all available OnGuard hardware states.



- 5. Open the All doors list and select the Other..., option to open the Select access control elements window.
 - This window provides a directory of all the OnGuard hardware in the system.
- 6. Expand the directory, find the hardware device(s), and add them to the selected list.



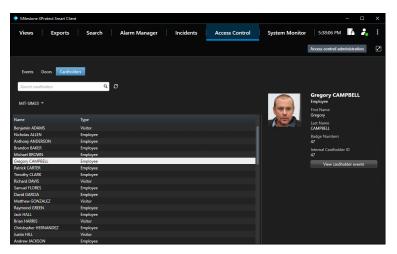
7. Select a Door in the list to see video from associated cameras, view door status information, and command buttons available for that door.



Access control workspace cardholders

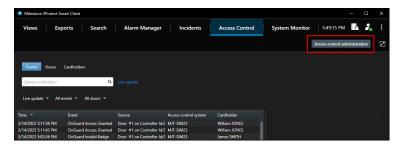
By default, this list displays all cardholders in the system.

- 1. Filter for specific cardholders by typing into the search field.
- 2. Select a cardholder to view their data.
- 3. Click the **View cardholder events** button to switch to the **Events** list filtered to display events from the chosen cardholder.



OnGuard web admin link

If a web portal link was added to the **General Settings** of the XProtect Access OnGuard integration within the XProtect Management Client, then the **Access control administration** link in the **Access Control** workspace of the XProtect Smart Client is active.



1. Click the Access control administration link to view the OnGuard Admin button.



2. Select the OnGuard Admin button to launch the OnGuard web administration portal.

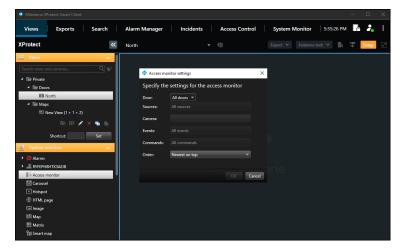
🗲 🛞 🔶 https://nky-onguard80.custder.us:8000/ 🔎 - C 🖗 Lenel® - Login 🛛 x	- □ × 命命题。
◆ OnGuard [®]	^
Directory <internal></internal>	
Lisemame * This field is required	
Password *	
Language English 💌	~

If multiple XProtect Access systems integrate with the same XProtect VMS it's possible to have more than one button in the Smart Client after selecting the **Access control administration** link.

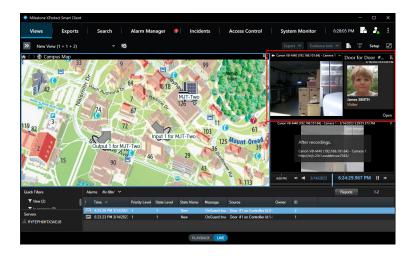
Access Monitor

The Access Monitor view item displays live status from doors and video from associated cameras in a single view pane in the Smart Client.

- 1. Click Setup in the Smart Client and expand the System Overview panel menu.
- 2. Select the Access Monitor view item and drag it into any available view pane:



3. In the Access Monitor Settings window open the lists to select the door, sources, cameras, events, commands, and the order in which new events appear in the access monitor.



After choosing a door the access monitor options change, based upon the available cameras, events, and commands. The access monitor view item can go into any available view pane and works in a view alongside all available view items.

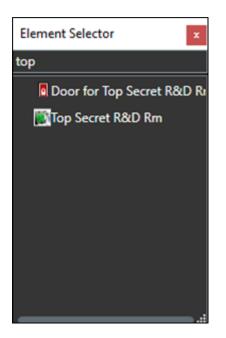
Maps

It's possible to place doors, readers, inputs, outputs, panels, and OnGuard server(s) on an existing Smart Client map. The map icons can display hardware status and execute commands.

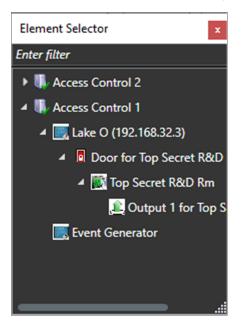
- 1. With the Smart Client in setup mode, a **Tools** window appears in the view pane.
- 2. From this window, select the Add Access Control icon:



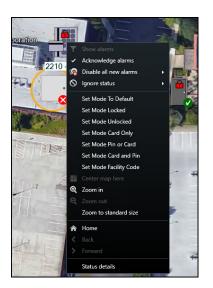
3. The Element Selector window appears.



4. Type the name of a hardware device into the filter to find a device or expand the servers and panels to find all available hardware icons in the system.



- 5. Drag the chosen icon onto the map.
- 6. During normal operations, it's possible to right-click any of these icons to execute the commands from the shortcut menu.



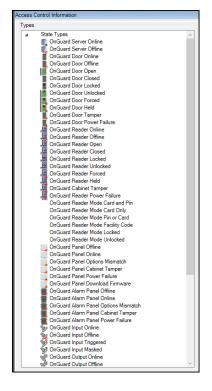
7. Right click the device icon and select **Status Details** from the shortcut menu to view more information. The popup window displays the device status information in the **Value** field.



In versions 4.2 and newer of the integration, the map icons include more status options and hardware items. If you want to know the possible hardware items and status options refer to the Map icon hardware and status details on page 79 topic.

Map icon hardware and status details

There are several different access control map icons available on the standard Smart Client map. Each different type of icon represents a specific hardware device. Visual indicators appear on these hardware icons to display the current status of the devices they represent. Many different types of hardware and status options are listed below.



The map feature of the XProtect Smart Client has many capabilities, please refer to the maps section of the Smart Client user guide.

Controllers send status information to XProtect Access to support display of tamper alarms on those device icons. For supported controllers, a red alarm status ring appears on the icon when it's in a tampered state. When the controller physically returns to a safe state, the alarm status disappears from the icon.

If you want to verify the list of available device icons and statuses in your XProtect Access system follow this process:

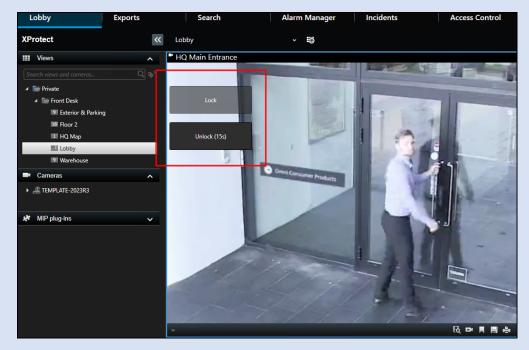
- 1. Go to the Tools menu in the XProtect Management Client and select Options.
- 2. On the Access Control Settings tab of the Options window choose to Show development property panel.
- 3. Close and re-open the Management Client.
- 4. Go to the DEV:Category Mapping tab of the XProtect Access instance.

Overlay buttons & commands

Overlay buttons are used to add manual buttons to video panes. Anything that can be triggered by a command can be added with an overlay button in the Smart Client. Read more about how overlay buttons work in XProtect here.

Overlay buttons appear as a layer on top of the live video when you move your mouse over the individual view pane. Use overlay buttons to activate device functionality, trigger system events, trigger low-voltage outputs, start recording,...etc. This functionality is extended into the XProtect Access integrations. There are a large number of possible uses for these buttons.

The most common use case for overlay buttons and XProtect Access integrations is to allow experienced video operators the ability to add door lock and unlock functionality to the familiar Smart Client views they use everyday. The ability to add door control (lock/unlock functionality) to live views is a great way to increase the overall functionality of the entire system, and makes the integration between access control and video feel much more seamless from an operational perspective.



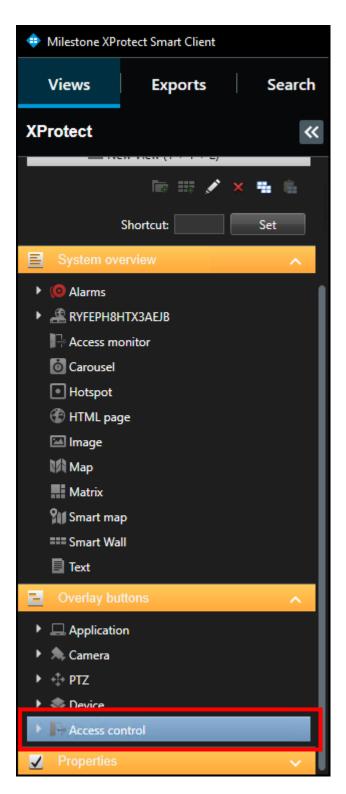
In particular, if customers want to visually verify access requests on highly secure doors, overlay buttons allow anyone who can view live video, to also have the ability to open the doors.

Other use cases can include any functionality connected to the door panel via programmable input and output connections, which can include the following:

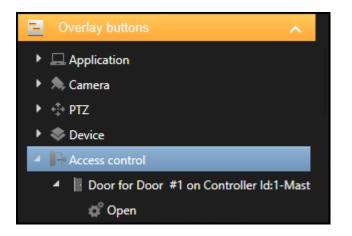
- Control lights or heating/cooling systems.
- · Arm/Disarm connected intrusion alarms and other sensors.

Follow this process to add an overlay button to a view:

- 1. When the Smart Client is in setup mode, there is an Overlay Buttons panel on the left side of the client.
- 2. Select the Access Control icon.



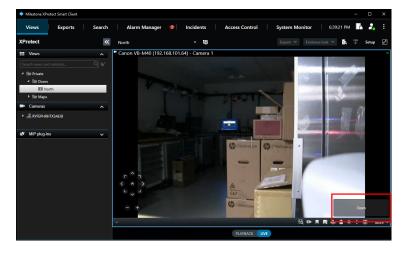
3. Expand the Access Control icon to find all the doors and readers, panels, and the connected inputs and outputs in the system.



4. Select a command from the list and drag it onto the view pane.



5. The output commands include activate and deactivate. Once the button is visible on a camera view pane, and the Smart Client is in setup mode, it is possible to re-size, move, and rename the overlay button.



Alarm acknowledgment explained

Alarm status between XProtect and OnGuard is shared. When alarms change state in XProtect that state is shared with OnGuard. Alarm status is shared in the opposite direction as well - from OnGuard to XProtect.

Alarm states in XProtect and OnGuard are not the same. In XProtect alarms can be new, in progress, on hold, or closed. In OnGuard alarms are new, in progress, or acknowledged.

OnGuard Alarm Status	XProtect Alarm Status
• NEW	• NEW
IN PROGRESS	IN PROGRESS
	ON HOLD
ACKNOWLEDGED	CLOSED

There are improvements to how alarms change state in the integration.

• Acknowledging an alarm in XProtect changes the alarm state to in progress both in XProtect and in OnGuard.

Alarms New (filter applie	ed) ❤ Clear filter	
! Time 👻	Priority Level State Level State	Name Message
5:16:19 PM 10/10/2	Acknowledge Set on hold Close	OnGuard /
	Edit Disable all new alarms Print	

• In XProtect alarms can change from closed to other states by manually editing the alarm. This isn't allowed in OnGuard. Acknowledged alarms are no longer available to change in OnGuard. If users continue to change the state of a closed/acknowledged alarm in XProtect these changes are not communicated to OnGuard.

Frames per second: 6.3.2 Video rode:::/PEG Video resolution: 640x480	40x480 40x480 fter recordings. non VB-M40 (192.	Camera 1 - 10/10/2022 501/29.31 O 168:101.64) - Camera 1 hrh.custdev.us:7563/
Frames per second : 5 22 Video order: JIPE Video resolution: 640x480	40x480 40x480 fter recordings. non VB-M40 (192.	168.101.64) - Camera 1
Ca	non VB-M40 (192.	168.101.64) - Camera 1
	10/10/2022	5:16:19.003 PM 🕨
Carnera: Canon VB-M40 (192.168.101.64) - Carnera 1 🔹 💌		Go to Alarm Time
Instructions	Assigned to:	Administrator (custdev\admir 🔻
	State:	4: In progress 🛛 👻
	Priority:	1: New
	Category:	4: In progress
	ID:	9: On hold 11: Closed
	Source:	testdoor
	Alarm:	Access Denied
		OnGuard Access Denied (acces
	Message: Type:	Access Control System Event
Activities	Rule:	Alarm Definition
Time Activity Owner 5:16 PM Initial priority: 1: High	Location:	Padimedenniadh
5:19 PM State changed to: 4: In progress Administrator (custo		
Vadministrator)	Tag:	
5:19 PM Assigned to: Administrator (custdev/administrator) Administrator (custde \administrator)	Vendor:	
5:19 PM State changed to: 4: In progress	Object	
Add		
Help Print		ОК

- Alarms in XProtect can return to the new state from any other state, if the alarm is manually edited. This isn't allowed in OnGuard. If a user manually edits an alarm state to new in XProtect from any other state, that change is not made in OnGuard.
- Although it's possible in XProtect to move a new alarm directly to on hold, this change does not take place in OnGuard, the activity is not even logged in OnGuard. If an alarm is accidentally moved to on hold in XProtect and instead it needs to move to in progress in both OnGuard and XProtect, it can be moved back to in progress, only by manually editing the status in XProtect.
- Once an alarm is in progress in OnGuard it can be "updated" with notes, however its status in XProtect will remain in progress, until it is acknowledged/closed. Status changes made in XProtect from in progress to on hold do not impact the status in OnGuard.

It's possible to change the alarm acknowledgment behavior of the integration to match previous versions (older than 4.2). How to make this change, and what this behavior means is documented here: Changing alarm acknowledgment behavior on page 87.

Acknowledge alarms in XProtect

In XProtect operators perform alarm acknowledgment and other alarm status change operations from the XProtect Smart Client.

- 1. In the Alarm Manager workspace, or any alarm list view item in the Smart Client, right-click an alarm.
- 2. Select a new status for the alarm from the shortcut menu.



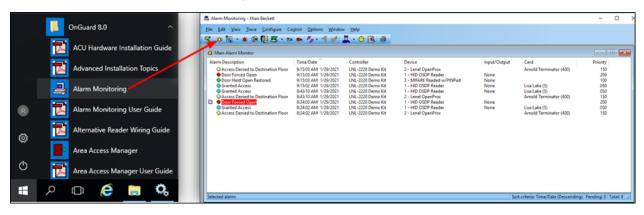
3. Alarm status synchronizes as much as possible between XProtect and OnGuard.

Learn more about how the integration handles alarm acknowledgment here: Alarm acknowledgment explained on page 83.

Checking alarm acknowledgment status in OnGuard

When alarms are acknowledged in OnGuard, the alarm is closed, and the associated alarm is also closed in XProtect. If the alarm is acknowledged within XProtect it changes state to in progress both in XProtect and in OnGuard. The status of the alarm in OnGuard changes to reflect the status in XProtect as much as possible. Learn more about how the integration handles alarm acknowledgment here: Alarm acknowledgment explained on page 83.

- 1. Verify state changes of alarms in the OnGuard system in real time by opening the **Alarm Monitoring** app from the **Start** menu.
- 2. If it isn't automatically opened, click the View Alarms icon to open the Main Alarm Monitor window.
- 3. Status of OnGuard alarms are displayed in this window in real time.



4. Right click an alarm in this window to acknowledge the alarm.

- 1. To view a report of all closed alarms, open the View menu.
- 2. Select the Reports option.
- In the Alarm Acknowledgement Reports tab choose a time range and export a report of all acknowledged alarms in the OnGuard system.

Acc System Status Gra Dending Alarms Gra Video Verification Gra Video Verification Gra Video Monitoring Prism Application Map Defeutit Map Map Defeutit Map Map Selection Schgduler Sigt by	ion Repot Repot Rem Acknowledgments. by Definition / Rem Acknowledgments. by Definition / Rem Acknowledgments. by Parel Receiver Account Rem Activity Content of the Receiver Account Rem Activity Date./Time Filter Today	Panel 500	Report Al Segment Default Segment Default Segment Default Segment Segment1 Segment1 Segment1 Segment2	pots Receiver Acc.
Selected al. Status Bar	Stat: Monday , February 8, 202 End: Monday , February 8, 202 Apply stat and end time to each d	21 V 11.59.59 PW		

Changing alarm acknowledgment behavior

Edit the PluginSettings.json file to change the behavior of the alarm acknowledgment between OnGuard and XProtect.

The section of the .json file to edit looks like this:

```
"AlarmAcknowledgmentSettings": {
    /*Set this property to 'true' if you want to use the pre-4.2 sync behavior where only
    the acknowledged/closed alarm states are synchronized.*/
    "OnlySynchronizeAlarmClosed": false
}
```

Change the false to true, save the file and restart the services.

In older versions of the integration alarm status between XProtect and OnGuard was shared in a limited way. When alarms were closed in XProtect that state was shared with OnGuard. In the OnGuard system the same alarm would be acknowledged. Alarm status was shared in the opposite direction as well - from OnGuard to XProtect.

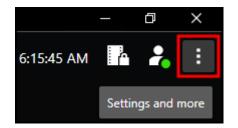
Possible alarm states in XProtect and OnGuard weren't the same. In XProtect alarms could be new, acknowledged, set on hold, or closed. In OnGuard alarms were either active or acknowledged. For the XProtect Access OnGuard integration, acknowledged alarms in OnGuard were the same as closed alarms in XProtect. All other alarm states in XProtect were active alarms in OnGuard.

OnGuard Alarm Status	XProtect Alarm Status
• ACTIVE	 NEW ACKNOWLEDGED > IN PROGRESS ON HOLD
ACKNOWLEDGED	CLOSED

When alarms were acknowledged in OnGuard, the alarm was closed, and the associated alarm was also closed in XProtect. If the alarm was acknowledged within XProtect it would not change status in OnGuard. The status of the alarm in OnGuard would change when the alarm was closed in XProtect.

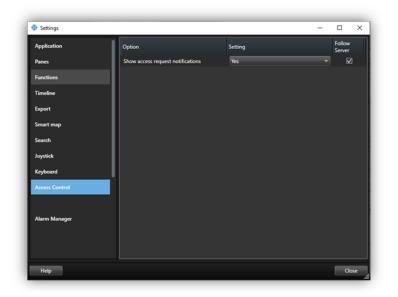
Smart Client access control options

1. In the upper right corner of the Smart Client is the Settings and more menu.



Click this icon and choose the **Settings** option to enter the Smart Client **Settings** window.

2. Select the Access Control menu in the Settings window.



3. Choose to show or block access request notifications in the Smart Client.

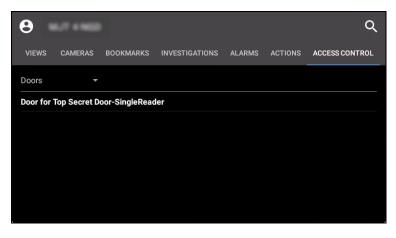
Mobile Client

XProtect Mobile application

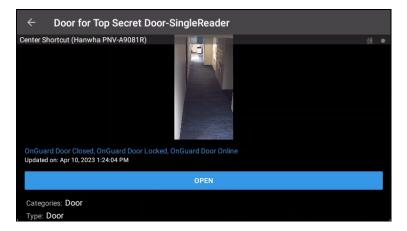
XProtect Mobile is a mobile device app that connects to your VMS system. The XProtect Access OnGuard integration adds capability to XProtect Mobile. Using XProtect Mobile it's possible to receive a push notification from the access control system, view live video related to the notification, and open the door - all remotely from the app.

Using the access control tab in XProtect Mobile

- 1. Log into the VMS with XProtect Mobile. By default the Views tab appears.
- 2. Select the Access Control tab. The Access Control tab shows the list of doors available.



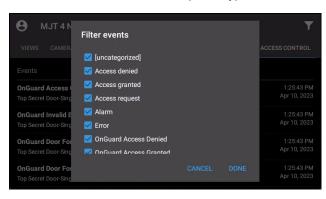
3. Filter for specific doors or select a door to view cameras associated to that door or interact with commands available for the selected door.



- 4. Swipe to switch between cameras when more than one camera is associated to the door.
- 5. Switch between Doors, Events, and Access Requests.
- 6. Select an event from the event list to view still images associated to the event and playback video related to the event.

₿ №	/JT 4 NGD)				T
VIEWS	CAMERAS	BOOKMARKS	INVESTIGATIONS	ALARMS	ACTIONS	ACCESS CONTROL
Events						
OnGuard	Access Gran	nted				1:25:43 PM
	Door-SingleRe					Apr 10, 2023
OnGuard	Invalid Bado	e				1:25:43 PM
Top Secret	Door-SingleRe	ader				Apr 10, 2023
OnGuard	Door Forced	Open				1:25:43 PM
Top Secret	Door-SingleRe	ader				Apr 10, 2023
OnGuard	Door Forced	Open				1:25:43 PM
Top Secret	Door-SingleRe	ader				Apr 10, 2023

7. Filter the event list to find specific types of events.



Access requests are visible if the Smart Client profile assigned to the role of the current user can view access requests.

Service Tray Icon

Service tray icon (explained)

The OnGuard XProtect Access Service, that runs on the OnGuard server has a service tray icon with a shortcut menu used for viewing status of the service, managing certificates, launching the log viewer, and starting and stopping the service. Right-click the OnGuard XProtect Access Service service tray icon to view the shortcut menu.

(OnGuard XProtect Access
	Version: 4.
:	Status: Running
	Select Certificate
	Start service
:	Stop service
	Restart service
1	View logs
	Exit

Using the Select Certificate menu

- 1. From the server hosting the OnGuard XProtect Access Service right-click the service tray icon for the OnGuard XProtect Access Service and choose the **Select Certificate...** option.
- 2. This opens the Select Certificate dialog. Initially, the Use default self signed certificate option is selected.

Select Certificate	×
Encryption Options	
A certificate is needed for communication encryption (HTTP/SSL). Please choose one of the options below.	
 Use default self signed certificate (less secure) 	
Our Sectificate from the list below:	
VMS SSL Certificate	>
Certificate properties	
Ok	Cancel

3. The option is also available to choose any other certificate. Choose the **Use certificate from the list below** option to select any certificate from the local machine's personal certificate store.

If there are no certificates available in the list, please refer to Secure communications explained on page 24 and read about creating compatible certificates.

4. The Certificate properties... button launches a properties menu for the chosen certificate.

Using the log viewer application

When upgrading the integration, all log levels configured in a non-default level of detail (not Info) are reset to "Info" after the upgrade. Please confirm and reconfigure the log level to the desired setting after the upgrade is complete.

1. Choose the View logs option from the shortcut menu of the service tray icon to launch the log viewer.

OnGuard XProtect Access Logs		- 0	×
OnGuard XProtect Access Logs			
XPA Translator - Event Manager Events Logs	Info 🔻	Open	
XPA Translator - Event Manager Logs	Info 🔻	Open	
	Info 🔻	0	ר
XPA Translator - State Manager Logs	1110 +	Open	
XPA Translator - State Manager Logs XPA Translator - Backward Compatibility Manager Logs	Info 🔻	Open	
XPA Translator - Backward Compatibility Manager Logs	Info 🔻	Open	

2. All available log files are in the **Logs List**. Adjust the detail level of the log using the list to the left of the **Open** button. Once you have chosen the level of detail click the **Apply** button to change the log level. The success dialog window pops up when the change is applied.

The available log levels are **Trace**, **Debug**, **Info** (default), **Warn**, **Error**, and **Fatal**. Trace shows the highest level of detail, Fatal shows the least amount of detail.

3. Click the Open button to launch a new window used to search through the individual log file.

VideoOS.OnGuar	rd.XPA.Service-MJT-LNLS2.json — 🗆 🗙
Clear Screen	🔍 First Prev Next Last
Reload Filter Options	10/21/2022 9:48:16 AM Info Removing HTTP Url ACL registration for <u>https://+8443/XPA/OnGuard/</u> 10/21/2022 9:48:16 AM Info Adding HTTP Url ACL registration for https://+8443/XPA/OnGuard/
🗹 Info	10/21/2022 9:48:16 AM Info Loaded SSL certificate from Local Machine store HASH 0xF78A4DD2866CA4BA6CEF4A949733E08DE5 10/21/2022 9:48:17 AM Info
	10/21/2022 9:48:17 AM Info VideoOS Common XPA Service Module v1.0 (c) 2013-2022
Trace	10/21/2022 9:48:17 AM Info 10/21/2022 9:48:19 AM Info Server module address : <u>https://localhost:8443/XPA/OnGuard/ACMServer</u>
🗹 Warn	10/21/2022 9:48:19 AM Info 10/21/2022 9:48:19 AM Info 1 XPA Translator(s) found.
Error	10/21/2022 9:48:19 AM Info XPA Translator: 'LenelS2 OnGuard-4.2.19.28078' was successfully initialized.
Fatal	10/21/2022 9:48:22 AM Error GetSystemConnectionState: There is no existing resource with id:82cd4bff-2ef8-c1ef-ef3e-afa70d8a
Word Wrap	
Auto scroll	
Load Progress	
	< > >

- Type in the text field at the top of the menu and hit enter or click the magnifying glass icon to start a text search. Use the **First**, **Prev**, **Next**, and **Last** buttons in the top right to navigate the search results.
- The **Clear Screen** button empties the main text display window, and the **Reload** button resets the current log file after a search. If the log file is large and takes time to load, the **Load Progress** graph at the bottom left displays the status of the load operation.
- Use the Filter Options menu to choose which types of log messages to display.
- The Word Wrap and Auto scroll options control the appearance and real-time behavior of the main text display window.
- 4. Click the Open Log File... button to launch a file explorer menu set to the local log file location.

The default location of the log files is C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\logs

- 5. Click the About button for version information and online access to Milestone support resources.
- 6. Click the **Color Configuration** button to open the **Color Configuration** menu to create a custom color scheme for the log reader. Custom color schemes are saved, exported, and imported with this menu. The Default button removes any customized configurations and applies the default settings.

◆ VideoOS.OnGua	rd.XPA.Service-N	/JT-LNLS2.json				- 🗆 ×
Clear Screen	DISK			•	First	Prev Next Last
Reload						
Filter Options						
🗹 Info						
🗹 Debug						\VideoOS.OnGuard.XPA.Service\Vid
Trace			elf-signed SSL certificate from D ITTP Url ACL registration for http			deoOS.OnGuard.XPA.Service\VideoO
Warn	0/26/2022 8:0	Color Configurati	on	-	ПX	102C0BE62849190A522C2C
Error	0/26/2022 8:0					
🗹 Fatal	0/26/2022 8:0 0/26/2022 8:0	Info	This is a sample text	Fore Color	Back Color	rver
Word Wrap	0/26/2022 8:0 0/26/2022 8:0	Debug	This is a sample text	Fore Color	Back Color	
Auto scroll	0/26/2022 8:0	Trace	This is a sample text	Fore Color	Back Color	red.
Load Progress		Warn	This is a sample text	Fore Color	Back Color	
	<	Error	This is a sample text	Fore Color	Back Color	>
		Fatal	This is a sample text	Fore Color	Back Color	
		Selected Line	This is a sample text	Fore Color	Back Color	
		Search	This is a sample text	Fore Color	Back Color	
		Selected Search	This is a sample text	Fore Color	Back Color	
		Backgound			Back Color	
		Default	Export Import	Save	Cancel	

Plugin Settings File

Working with the PluginSettings.json configuration file

The OnGuard XProtect Access Integration uses a .json file to control the configuration options for cardholder and visitor search, and alarm acknowledgment. This **PluginSettings.json** file is on the OnGuard server or the host of the OnGuard XProtect Access Service. The file location should be:

C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\Translators\OnGuard\PluginSettings.json

Edit this file to change the data displayed for cardholders in the Smart Client, and change the display order for cardholder names. For example, the first name, middle name, and last name can appear in any order. It's also possible to change the data displayed for visitors. Lastly, the **PluginSettings.json** file can enable or disable the default alarm acknowledgment behavior.

After editing and saving the .json file, changes take effect after the next restart of the OnGuard XProtect Access Service and the XProtect Event Server. Follow this process to edit the file:

- 1. Complete the first cardholder search or receive the first access control event
- 2. .json file is created with the default configuration.
- 3. Edit the .json file to meet the new requirements.
- 4. Restart the OnGuard XProtect Access Service.
- 5. Restart the XProtect Event Server

Upgrades from older versions of the OnGuard XProtect Access integration to versions 4.2 or newer may not automatically receive a fully detailed **PluginSettings.json** file. Delete the file, restart the OnGuard XProtect Access Service, send an event or perform a cardholder search.

Known Issues

Limitations

- OnGuard doesn't model doors; instead it models readers. But XProtect Access requires doors. The OnGuard
 plugin creates virtual doors based on reader properties (i.e. panel id, panel address, reader number, etc). The
 virtual door names are taken from the first reader that has a non-empty display name. If that reader is named
 "reader 1", that's what the door is named. This may not be intuitive when viewed in the XProtect Management
 Client or Smart Client applications' hardware hierarchy
- The XProtect Access instance in the Management Client can fail to load after the Event Server starts or is restarted if the OnGuard XProtect Access Service on the OnGuard server isn't started and running. Symptoms of this issue include:
 - Existing XProtect Access instance disappears from Management Client
 - Creation of new XProtect Access instance is not allowed
 - NullReferenceException log entries appear in the Event Server log file

Troubleshooting Guide

Basic support checklist

For issues not covered in this guide, please contact Milestone Support at support@milestone.us, or by phone at 503-350-1100.

Simple items can lead to support calls if overlooked. Below is a short list of those items. First are the items to check on the XProtect Access system, followed by a list of things to verify on the OnGuard system. For both, make sure the versions of the OnGuard system and the XProtect system are supported.

XProtect Access

This set of items are helpful for resolving all troubleshooting issues.

- Check that the doors in XProtect Access are licensed.
- Check that the doors in XProtect Access are enabled.
- Verify the XProtect Access Service is running.
 - · Check the service tray icon on the server where the XPA service is installed to verify.

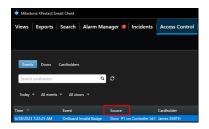
2

- Make sure the Event Server connection to the XPA service is connected.
- Double check that the credentials used for the OpenAccess user and password fields are correct.

The next set of issues are helpful for issues related to events, alarms, and status changes not being received between the two systems.

- Verify all required doors and other devices from the OnGuard system are added to the XProtect Access system.
 - As devices change over time, it's suggested to refresh the configuration from the General Settings tab.
- · Check that events are displayed in the Smart Client access control workspace Events List.
 - · Make sure there are no filters applied which might be changing the results.
- Check that events are being displayed in the Management Client when the Live Events dev tab is displayed.
- Match the Source of events appearing in the Smart Client access control workspace to any Alarms defined in the Alarm Definition menu of the Management Client.
 - Smart Client event source location:

Manual | XProtect Access for OnGuard



• Management Client Alarm Definition source location:

Milestone XProtect Management Client 2023 R2			- 0	×
File View Action Maintenance Tools Help				
E 9 😧 🗢 🛍				
Site Navigation - A X Alarm Definitions	 Q Alarm Definition Information 			*
- 💎 User-defined Events 🛛 🗚 🖃 🧏 Alarm Definitions	Aam definition			
- 🕈 Analytics Events - 🧏 Front Door Acces	s Denied Enable:			
- 🍖 Generic Events				
- 🖧 Webhooks	Name:	Front Door Access Denied		
E 🕼 Security	Instructions:		<u>^</u>	
- Roles				
- 🤮 Basic Users 🕀 🛇 System Dashboard			~	
Current Tasks	Trigger			
System Monitor				
System Monitor Thresholds	Triggering event:	Access Control Event Categories	~	
- R Evidence Lock		Access depied	~	
Configuration Reports				- 1
Server Logs	Sources:	Door for Door #1 on Controller Id:1-SingleReader	~	
🕀 🐨 Metadata Use	Activation period			
- 🍕 Metadata Search				
- R Access Control	Time profile:	Aways	~	
C Incidents	 Event based: 	Start: S		
3 Incident properties				
e 🔍 Transact		Stop: St	lect	
Transaction sources	Map			
Instaction definitions	A de alem ante annum an the ar	nart map if at least one source of the alarm is a carnera, an input device.		
- Alarm Definitions	An alarm only appears on the sh	hart map it at least one source of the alarm is a camera, an input device.	or a micropho	.00.
Alarm Data Settings				
Sound Settings	Alarm manager view:	 Smart map 		
< >		Map		
Site Navigation Federated Site Hierarchy			~	
	Related map:		~	

- Open the log viewer application and check the following logs to verify your events are received by the XProtect Access Service:
 - XPA Translator Event Manager Logs
 - Change the log level to Debug and Apply the change. Send some events into the system and then Open the log file.

♦ OnGuard XProtect Access Logs – □ ×	VideoOS.OnGuard.XPA.Service-MIT-SIMS-OnGuard-Events.json	- 🗆 ×
OnGuard XProtect Access Logs	Close Store Image: 101/0000 Inford Queue CP/2022 6/03.1 /PA (doing Activities if a constraint of constraint of a	R Tint Prev Next Last
Select the log you want to open.	Error ACMSProperty Key : Panelld Value :1	
Logs List XDA Translator - Event Manager - Management Events Logs Info Qpen	Word Wrep ACMSProperty Key : DeviceId Ø Auto scroll ACMSProperty Key : DeviceId Josef Torress Value : 2 : 2	
XPA Translator - Event Manager Logs Debug Open	Load Progress Value :1 6/28/2023 7:22:25 AM Debug ACMSEvent Id :2[1]2[0]1[4 EventTypeId :0neuror_imedid_bedge_1_4 SrcOperationabletistanceid: Oneuror_instance.inReader:12	
XPA Translator - State Manager Logs Info Appen XPA Translator - Backward Compatibility Manager Logs Info XPA Translator - Main Logs Info Open	Timedamp (27/2/03/37223374/ Message (OnGurd Nobused Involutional Beage Reason : Related/orientalbiloiderids (OnGurd-Instance-Lrit_Cardholder:1 Related/orientalbiloiderids)	
Open Access - Client Logs Info 💌 Open	ADMSProperty Key : Panelld Value : 1	
Main Logs Info - Open	ADMSProperty Key : DeviceId Value : 2	
About Color Configuration Apply Open Log File	ACMSProperty Key : Dventid Value :2 6/28/2023 7:32:34 AM Debug Alarm '2(1)2(0)1(4' state was changed to: Close	d

- Open the MIP Plugin logs at this location to verify that the events are received by the Event Server:
 - C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.MipPlugin\VideoOS.Event.Server\logs

In order to have all of the log information that might be required to help troubleshoot event issues, it is recommended to use the Milestone Diagnostics Tool. Read about how to use this tool, and how to gather log data, here.

OnGuard

- · Check that the required OnGuard services are running.
- Check SQL server configuration for the OnGuard system. This process is detailed in a knowledge base article here.
 - This step requires running a SQL query using SQL Server Management Studio and potentially modifying the configuration.

If all of these attempts to fix event communication fail contact Milestone technical support. There are additional tools, such as the OnGuard Event Subscriber tool, which can be used to gather all event communication on an OnGuard system and output it to a text file for further troubleshooting. This tool is only available through support.

OnGuard loses communication with access control hardware

Communication can fail for the following reasons:

- 1. Firewall blocking traffic.
- 2. The OnGuard LS Communication Server service isn't running or needs a restart.
- 3. The OnGuard LS Web Service service isn't running or needs a restart.

Integration version downgrades

Here is the process required to uninstall the 4.3 version of the plugin.

1. Go to the **Programs and Features** menu on the Milestone server. Uninstall the Milestone OnGuard XProtect Access program.

← → × ↑ 🖸 > Control P	anel > All Control Panel Items > Programs and Features			~	Search Progra
Control Panel Home	Uninstall or change a program				
View installed updates	To uninstall a program, select it from the list and then	click Uninstall, Change, or Repa	ir.		
Turn Windows features on or					
off	Organize 🕶 Uninstall Change Repair				
Install a program from the network	Name	Publisher	Installed On	Size	Version
	Microsoft Visual C++ 2010 x64 Redistributable - 1	Microsoft Corporation	7/22/2019	26.1 MB	10.0.40219
	Microsoft Visual C++ 2010 x86 Redistributable - 1	Microsoft Corporation	7/22/2019	17.3 MB	10.0.40219
	Hicrosoft Visual C++ 2013 Redistributable (x64)	Microsoft Corporation	8/14/2020	20.5 MB	12.0.21005.1
	Microsoft Visual C++ 2013 Redistributable (x86)	Microsoft Corporation	8/14/2020	17.1 MB	12.0.21005.1
	Microsoft Visual C++ 2015 Redistributable (x64)	Microsoft Corporation	8/14/2020	22.4 MB	14.0.23026.0
	Microsoft Visual C++ 2015 Redistributable (x86)	Microsoft Corporation	8/14/2020	18.6 MB	14.0.23026.0
	Microsoft Visual Studio 2015 Shell (Isolated)	Microsoft Corporation	10/26/2020	134 MB	14.0.23107.10
	Microsoft Visual Studio Tools for Applications 2015	Microsoft Corporation	8/14/2020	16.7 MB	14.0.23829
	Microsoft Visual Studio Tools for Applications 201	Microsoft Corporation	8/14/2020	88.0 KB	14.0.23107.20
	Microsoft VSS Writer for SQL Server 2016	Microsoft Corporation	7/22/2019	6.26 MB	13.1.4001.0
	Milestone OnGuard XProtect Access	Milestone Systems Inc.	11/29/2021	40.8 MB	4.1.27.39633
	Milestone Open Network Bridge	Milestone Systems A/S	11/9/2020	26.4 MB	20.3.1
	Milestone XProtect VMS 2020 R3	Milestone Systems A/S	12/17/2020	129 MB	20.3.1
	Milestone XProtect VMS Device Pack 11.1c	Milestone Systems A/S	11/12/2020	1.20 GB	11.1.3.34
	Notepad++ (32-bit x86)	Notepad++ Team	5/15/2020	8.16 MB	7.7
	🐍 SnakeTail 64-bit v1.9.4.0	SnakeNest.com	9/19/2018	1.55 MB	1.9.4.0
	ኛ XProtectToolkit	XProtectToolkit	11/18/2021		1.0.0.77

- 2. Go to the **Program and Features** menu on the OnGuard server. Uninstall the Milestone OnGuard XProtect Access component
- 3. Download the old version of the integration.
- 4. On the OnGuard server: re-install the OnGuard XProtect Access Service.
- 5. On the Milestone server: re-install the OnGuard XProtect Access MipPlugin.
- Open the XProtect Management Client. Reconfigure any connection properties in the General Settings tab of the XProtect Access instance as needed. Save the settings. Refresh the configuration of the XProtect Access instance.

XProtect 2021 R1 and R2 shows no error if OpenAccess - password is incorrect.

When running XProtect VMS 2021 R1 or 2021 R2, if a change to the configuration on any XProtect Access integration in the **General Settings** tab is saved, the system prompts for a password. This is the password for the account that authenticates between XProtect and the integrated access control system. If the wrong password is provided, there is no error or warning displayed and the integration is broken, without any warning, until the password is changed again to the correct one.

This issue can occur during every XProtect Management Client session when the XProtect Access system configuration changes. When any information or setting controlled within the XProtect Access integration section of the Management Client is changed and saved, the system asks for a password.

ccess Control	→ ‡	Access Control Information
Access Control		
		Enter current password X Selecting Enter will also save the current access control configuration. OpenAccess – Password:
		Enter Cancel

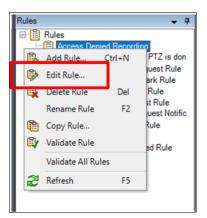
To verify the correct settings are in place for the password and all other parameters controlling the connection between integrated access control systems and the XProtect Event Server, use the **Refresh Configuration** feature each time after entering the password, and each time the settings on the **General Settings** page change. If the connection breaks because the password is wrong, then the refresh configuration process produces an error.

Access Control 🚽 🕂	Access Control Information	
E Access Control	General settings Enable: Name: Description:	
	Integration plug- Last configuration Last configuration Update Configuration Operator login re XProtect Access XProtect Access CopenAccess - P OpenAccess - P OpenAccess - P OpenAccess - D Options - OnGur Options - OnGur Options - States U Unable to receive configuration from the access control CopenAccess - P OpenAccess - P OpenAccess - P Options - OnGur Options - States U Unable to receive configuration from the access control Coperation of the access - P Options - OnGur Options - States U Unable to receive configuration from the access control Coperation of the access - P Options - OnGur Options - States U	
	Options - [Legac Options - [Legac Options - Enable	Apply Cancel

Access control rules stop working after upgrade to 4.0 or newer.

In versions 4.0 and newer of the XProtect Access LenelS2 OnGuard integration doors can't be a source for access control events or event categories in the XProtect VMS rule system. For existing rules to continue to function, and for new rules, readers must be the source for all events. To fix broken rules after a system upgrade, the source door objects must be replaced by the associated reader objects. Edit the existing rules, remove the doors as the source and replace them with readers. Below is the process to perform this change.

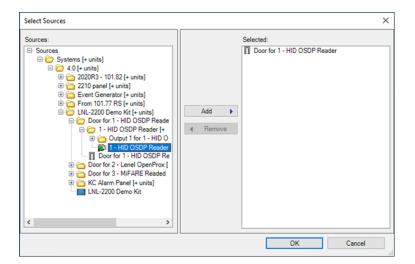
1. Find all access control related rules in the XProtect **Rules** menu. Right-click each individual rule, and select **Edit Rule...** from the shortcut menu.



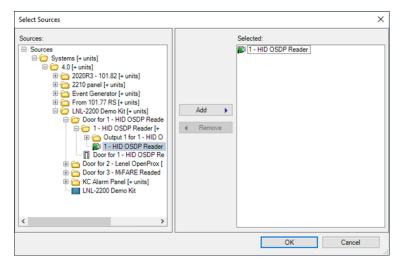
2. Click the door hardware object used as the source of the event.

Manage Rule				- 0	×
Name:	Access Denied Recording				
Description:					
Active:	\square				
		Step 3: Actions			
Select actions to pe	rform				
Start recording of					^
Start feed on <de< td=""><td></td><td></td><td></td><td></td><td></td></de<>					
Set <smart td="" wall<=""><td>> to <preset> > <monitor> to show <came< td=""><td></td><td></td><td></td><td></td></came<></monitor></preset></td></smart>	> to <preset> > <monitor> to show <came< td=""><td></td><td></td><td></td><td></td></came<></monitor></preset>				
	> <monitor> to show <called > <monitor> to show text '<r< p=""></r<></monitor></called </monitor>				
	ras> from <smart wall=""> mor</smart>				
	te on <devices></devices>				
	ame rate on <devices></devices>				
	ame rate to all frames for Mf on <device>using <profile></profile></device>		evices>		
	in coevices using cpromes	with PT2 sphoney>			
	otion (click an underlined ite	m)			
Perform an action of	Access denied (Access Cor HID OSDP Reader	ntrol Categories)			
	hid OSDP Reader	work Camera (192.168.10	1.65) - Camera 1, Canon	VB-M40 (19	2.168.1
Perform action <u>30 se</u> stop recording imme					
<					>
Help	Cancel	< Back	Next >	Fin	ish

- The Select Sources window opens. Expand the source directory to identify the door hardware object(s) matching the Selected hardware objects. Associated to that door hardware object are one or more reader hardware objects.
- 4. Choose the correct reader associated to the door for this rule.

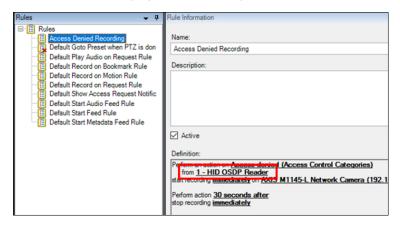


5. Select the reader hardware object from the directory and click the Add button.



6. Select the door hardware object from the Selected list, and click the Remove button.

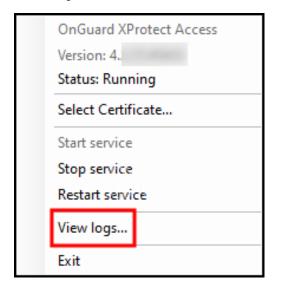
- 7. Finish editing the rule.
- Perform this same process for all access control related rules in the XProtect VMS. Check the rules by selecting
 a rule and verifying the hardware object used as the source.



OnGuard XProtect Access Service: MipPlugin post-install verification

Verify the MipPlugin (located on the XProtect Event Server host machine) was installed by checking the logs, following these steps:

1. Right-click the OnGuard XProtect Access Service tray icon, and select **View logs** from the shortcut menu.



2. Choose to open the Main Logs from the log viewer application.

OnGuard XProtect Access Logs	-	- 🗆 🗙
OnGuard XProtect Access Logs		•
Logs List		
XPA Translator - Event Manager Events Logs	Info 🔻	Open
XPA Translator - Event Manager Logs	Info 🔻	Open
XPA Translator - State Manager Logs	Info 🔻	Open
XPA Translator - Backward Compatibility Manager Logs	Info 🔻	Open
XPA Translator - Main Logs	Info 🔻	Open
Open Access - Client Logs	Info 🔻	Open
Main Logs	Info 🔻	Open
About Color Configuration App	oly Ope	n Log File

3. Verify that the following entries are in the log file:

Info 1 XPA Translator(s) found.

Info XPA Translator: 'LenelS2 OnGuard-4.x.xx.xxxxx' was successfully initialized.

	· · · · · · · · · · · · · · · · · · ·	
Clear Screen	Sirst Prev Next Last	
Reload	12/27/2022 6:42:59 AM Info Removing HTTP Url ACL registration for https://+.8443/XPA/OnGuard/	
Filter Options	12/27/2022 6:42:59 AM Info Adding HTTP Url ACL registration for https://+8443/XPA/OnGuard/12/27/2022 6:42:59 AM Info Loaded SSL certificate from Local Machine store HASH 0xEEC0C071E16702FB598896C7E0AFB705DF5BDDDA	
🗹 Info	12/27/2022 6:42:59 AM Info	
🗸 Debug	12/27/2022 6:42:59 AM Info VideoOS Common XPA Service Module v1.0 (c) 2013-2022 12/27/2022 6:42:59 AM Info	
Trace	12/27/2022 6:43:01 AM Info Server module address : https://localhost:8443/XPA/OnGuard/ACMServer 12/27/2022 6:43:01 AM Info	
✓ Warn	12/27/2022 6:43:01 AM Info 1 XPA Translator(s) found.	
Error	12/27/2022 6:43:01 AM Info XPA Translator: 'LenelS2 OnGuard-4. was successfully initialized.	
🗹 Fatal		
Word Wrap		
Auto scroll		
Load Progress		

Cardholder search data fields are missing, or out of order

The OnGuard XProtect Access Integration uses a default list of cardholder data fields when searching for cardholders. Edit the **PluginSettings.json** file to change which data is available, and the order of the cardholder name fields.

The default list of cardholder data fields:

.JSON file data field text	Description
LASTNAME	Cardholders last name
FIRSTNAME	Cardholders first name
MIDNAME	Cardholders middle name
ADDR1	Street address on file for cardholder
CITY	City on file for cardholder
ZIP	Zip code or postal code on file for cardholder
PHONE	Phone number on file for cardholder
OPHONE	Additional phone number on file for cardholder

Edit the list in this .json file to add new data fields, remove existing data fields and change the order of the data fields. **"CardholderSearchFields"** defines the data types available, and **"CardholderDisplayName"** sets the order of data display. If the list in the .json file is empty, then the complete range of search-able fields is used. The file location should be:

The section of the .json file to edit in order to change the cardholder settings looks like this:

```
"CredentialHolderSettings": {
    /*The Onguard Cardholder fields used when searching for Credential Holders in
XProtect. Leave empty to use all available searchable string fields in OnGuard.*/
    "CardholderSearchFields": {
      "LASTNAME",
      "FIRSTNAME",
      "MIDNAME",
      "ADDR1",
      "CITY",
      "ZIP",
      "PHONE",
      "OPHONE"
    }
    /*The Onguard Cardholder display name field is for changing the cardholder display
name. Available fields are FIRSTNAME, MIDNAME, LASTNAME, and any additional Card
Holder properties.*/,
    "CardholderDisplayName": {
      "FIRSTNAME",
      "MIDNAME",
      "LASTNAME",
```

}

}

After editing and saving the .json file, changes take effect after the next restart of the OnGuard XProtect Access Service and the XProtect Event Server.

Upgrades from previous versions of the OnGuard XProtect Access integration may not automatically receive a fully detailed **PluginSettings.json** file. If the .json file is not available, it can be recreated with the default search fields and display names the next time the OnGuard XProtect Access Service is restarted and a new search is performed. After the default file is created, it's recommended to edit the file to obtain the correct combination of search fields and name order for your installation.

Not receiving cardholder or badge changes

If cardholder or badge changes aren't reflected in either the XProtect Management Client or Smart Client, verify that software events are enabled in OnGuard.

XProtect Access integration flooding OnGuard user transaction report

Milestone's XProtect system frequently requests status of OnGuard hardware. To get the current state of a hardware device, the integration must update the hardware status on the parent panel, then query for the device state. A transaction for each hardware status update/query is entered into OnGuard for the single sign-on (SSO) user.

Customers making use of OnGuard's built-in User Transaction report from OnGuard's Sys Admin + Reports will see these transactions from the OnGuard XProtect Access integration under the SSO user in the report. It's not possible to filter the User Transaction report to omit the SSO user.

Possible workarounds include:

- Install a compatible version of Crystal Reports and customize the report. However, OnGuard Technical Support, OAAP, etc., don't support custom reports.
- Contact the OnGuard Custom Solutions group and have them create/customize the reports.

OnGuard XProtect Access instance not displayed in the XProtect Management Client

If XProtect is unable to communicate with the OnGuard XProtect Access instance, the instance won't appear in the **Access Control** section of the Management Client. This process should restore visibility:

On the Milestone server:

- 1. Close the Management Client and Smart Client.
- 2. Stop the XProtect Event Server.

On the OnGuard server:

- 3. Stop the OnGuard XProtect Access Service.
- 4. Verify the required OnGuard services are running.
- LS Event Context Provider.
- LS Message Broker.
- · LS OpenAccess.
- LS Web Event Bridge.
- · LS Web Service.
- 5. Start the OnGuard XProtect Access Service

On the Milestone server:

- 6. Start the XProtect Event Server and wait for it to begin running.
- 7. Start the Management Client.

If the instance still isn't in the Management Client, investigate the logs and contact Milestone Technical Support.

LS OpenAccess service automatically stops seconds after starting

There is a known issue with OnGuard caused by an Active Directory account logging into the OpenAccess service after it starts, which can cause OpenAccess to crash. The OnGuard XProtect Access Service tries to log into OpenAccess when both services are running. This can trigger the crash. The recommended workaround is to switch the Single Sign-On user to a local Windows account and adjust the services to use this same local Windows account.

For questions and information about this issue, please contact support at oaaptechnical@carrier.com. Reference LenelS2 Bug DE40122.

I/Os connected to OSDP readers are no longer detected

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) where I/Os connected to OSDP readers are not detected in the OnGuard XProtect Access integration.

For questions and information about this issue, please contact support at oaaptechnical@carrier.com. Reference LenelS2 Bug DE40122.

LS OpenAccess events fail in OnGuard Enterprise systems

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) running in an Enterprise configuration. Devices don't send events through OpenAccess to the OnGuard XProtect Access integration.

For questions and information about this issue, please contact support at oaaptechnical@carrier.com. Reference LenelS2 Bug DE40122.

XProtect Access developer tabs (explained)

Hidden tabs are built into the XProtect Access instance in the Management Client. These tabs contain helpful information when troubleshooting.

ess Control 🚽					
Access Control	Icon Eventid	EventName	Timestamp	Message	EventCategories
C CICHER	★ 13c493d3-4d87-450e-8683-e8b1899ebba9	Door #1 on Controller Id:5-SingleReader.OnGuard Door Held Open	6/28/2023 2:56:43 PM	OnGuard Door Held Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
		Door #1 on Controller Id:5-SingleReader.OnGuard Access Granted	6/28/2023 2:56:42 PM	OnGuard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6ccM, 7H4e6d4-9078-5716-a83c-3#
		Door #1 on Controller Id:3-MasterReader OnGuard Door Held Open		On/Guard Door Held Open	ef7a3cbe-663d-541e-80o4-ceb1185809c3
	✓ 1edecd1d-3651-458a-acc1-3ea185ebd010	Door #1 on Controller Id 5-SingleReader OnGuard Door Held Open	6/28/2023 2:56:42 PM	On/Guard Door Held Open	ef7a3cbe-663d-541e-80o4-ceb1185809c3
	✔ 102212b0-3a10-4a60-b440-2fab9a93231	Door #1 on Controller Id:4-MasterReader.OnGuard Door Forced Open	6/28/2023 2:56:41 PM	OnGuard Door Forced Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
	✓ 6360bd7d-0925-4e53-b7c3-d8bd23cdaeb5	Door #1 on Controller Id:4-MasterReader.OnGuard Invalid Badge	6/28/2023 2:56:41 PM	OnGuard Invalid Badge	87e8ae65-7671-592b-a896-b1c9f36b8116, 7ff4e6d4-9078-5716-a83c-3
	★ aad73ace-e47a-4e71-8e85-67838e35e140	Door #1 on Controller Id:3-MasterReader.OnGuard Access Granted	6/28/2023 2:56:41 PM	OnGuard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6ccM, 7#4e6d4-9078-5716-a83c-3#
		Door #1 on Controller Id:4-MasterReader OnGuard Invalid Badge		OnGuard Invalid Badge	87e3ae85-7671-592b-a896-b1c9936b8116, 7H4e6d4-5078-5716-a83c-3
	✓ 593b93c0-a553-4a50-be45-2ab3b7ad5c39	Door #1 on Controller Id:6-MasterReader.On/Guard Door Forced Open	6/28/2023 2:56:41 PM	On/Guard Door Forced Open	ef7a3cbe-663d-541e-80o4-ceb1185809c3
		Door #1 on Controller Id 5 SingleReader.OnGuard Access Granted	6/28/2023 2:56:40 PM	Or/Guard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6ccl4, 7/l4e6d4-9078-5716-a83c-3/l
	✓ 54be26bc-158c-47df-bb22-a7d8b8eb04ed	Door #1 on Controller Id:5-SingleReader.OnGuard Door Forced Open	6/28/2023 2:56:40 PM	OnGuard Door Forced Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
	✔ 962882b9-d9ae-4bbe-a407-4ebec394e935	Door #1 on Controller Id 9-SingleReader.OnGuard Invalid Badge	6/28/2023 2:56:40 PM	OnGuard Invalid Badge	87e8ae85-7671-592b-a896-b1c9t36b8116. 7#4e6d4-9078-5716-a83c-3
	✔ 16e4/e7b-14ce-4663-bc13-5cebdf577823	Door #1 on Controller Id:2-SingleReader.OnGuard Access Granted	6/28/2023 2:56:40 PM	OnGuard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6cc44, 7#4e6d4-9078-5716-a83c-3#
	¥ 26c5a190-b30a-4dea-b540-25/33cbcde04	Door #1 on Controller Id 4-SlaveReader.OnGuard Access Granted	6/28/2023 2:56:40 PM	Or/Guard Access Granted	144/923c-51bd-5251-8/a7-7d876fb6cc44, 7H4e6d4-9078-5716-a83c-3H
	✔ 16ab561a-3029-43aa-9693-2d02023a7e1	Door #1 on Controller Id 1-SingleReader OnGuard Access Granted	6/28/2023 2:56:40 PM	Or/Guard Access Granted	144/923c-51bd-5251-8/a7-7d876fb6ccl4, 7//4e6d4-9078-5716-a83c-3//
	e Biblined Joseph Carteria Hibline	Pedag Access Control Imms	Procenties		Refer Somberg term
	< Related Access Canad Credental Holders	Related Access Cantol Innos	Properties:		Tolast Scrollarse Inne
	- Reland Access Control Contential Holdern	Public Access Control Terror	Properties:		Related Scirolines Inno Activate Windows Social Extension in activate Windows

Enabling developer tabs

Take these steps to enable the hidden developer tabs built into the XProtect Access instance.

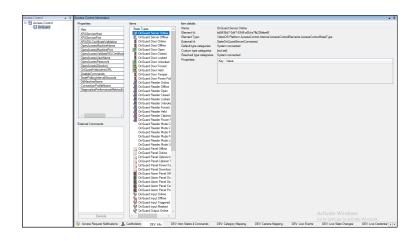
- 1. Select **Options** from the **Tools** menu of the Management Client.
- 2. Go to the Access Control Settings tab of the Options dialog and select the Show development property panel option.

Options						×
External IDP	Evidence Lock	Audio Messages	Privacy settings	Access Control Settings	Analytics Events	Custe < ->
Access Cont	rol Settings evelopment proper	ty panel				
Help	p			OK	Canc	el

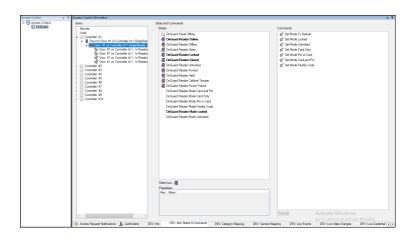
Developer tabs (reference)

Below is a description of how to use each of the hidden developer tabs available within the XProtect Access instance.

Tab Name	Description
DEV: Info	This tab has the entire hierarchy of servers, devices, statuses, commands, and events in the system. Selecting an individual object allows for identification of any properties associated to it.



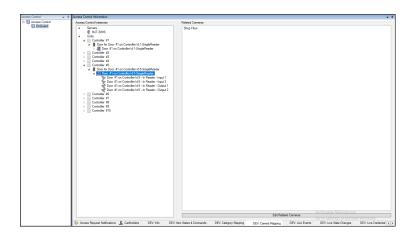
	This tab shows all devices and servers in the system. Select a device or	
DEV: Item States & Commands	server to view all associated commands and possible statuses. The	
	current state of the device or server is displayed in bold.	



	The Category Mapping tab is primarily used for debugging during development
DEV: Category Mapping	making sure that the Events, Commands, States, Servers, and Devices are
	mapped correctly between OnGuard and XProtect.

Access Control	Access Control Information					
OnGuard	Types	Category				
CI UNDERIG	ConGuard Granted-Eacort	Default categories:	Access denied			
	✓ OnGuard Granted-Exit-Escort		Access request			
	OnGuard Granted-Master		Or/Guard Access Denied			
	✓ OnGuard Granted-Exit-Master					
	ConGuard Granted-Dual Custody					
	✓ OnGuard Granted-Exit-Dual Custody					
	OnGuard Granted-Pending Entry	Override default:	1			
	OnGuard Access Granted Entry Made					
	OnGuard Access Granted to Destination Floor		Ignore	^		
	OnGuard Granted Double Card		Error	_		
	OnGuard Access Granted: Pin		Warring			
	OnGuard Access Granted: Lift		Alarm			
	OnGuard Access Granted: Soft Passback		Access granted			
	OnGuard Access Granted: Time and Attendance In		Access denied			
	OnGuard Access Granted: Time and Attendance Out					
	OnGuard Invalid Card Format					
	OnGuard Denied Count Exceeded					
	OnGuard Denied, PIN Only Request					
	OnGuard Invalid Facility Code					
	CorGuard Invelot Badge					
	OnGuard Invalid Issue Code					
	OnGuard Invalid PIN Number					
	OnGuard Invalid Access Level					
	OnGuard Inactive Badge					
	OnGuard Denied, Reader Excluded					
	OnGuard Denied, No Command Authority					
	OnGuard Denied UnMask - Active Zones in Group					
	OnGuard Use Limit Exceeded					
	OnGuard Access Denied: Invalid Timezone					
	OnGuard Denied Low Battery					
	OnGuard Biometric Mismatch					
	OnGuard Access Denied: Reader Locked					
	OnGuard Access Denied Door Secured					
	OnGuard Access Denied Interlock					
	OnGuard Access Denied Passback					
	OnGuard Access Denied Unauthorized Arming State					
	OnGuard Access Denied Unauthorized Entry Level					
	OnGuard Access Denied Unauthorized Time					
	OnGuard Access Denied					
	OnGuard Denied - No Host Approval					
	OnGuard Denied - Unauthorized Assets					
	OnGuard Access Denied: No Biometric Template					
	OnGuard Access Denied: Biometric Reader Office					
	OnGuard Egress Denied					
	of Oxformed Descured to Enter Destart					
	C					

DEV: Camera Mapping	This tab displays the current camera to device mapping used in the XProtect Access instance.
---------------------	--



DEV: Live Events	This tab will display live events as they're received by the XProtect Access system when selected. If the client is closed, or the user switches to another view, the Live Events tab won't retain any memory of the events displayed. This memory-less behavior is something all three Live tabs have in common.
------------------	---

	Access Control Information				• 5
Access Control	loon Eventid Event?	latie	Timestamp	Message	EventCategories
C) UNIVERD	✔ 13o493d3-4d87-450e-8648-e8b1898ebba9 Door #	1 on Controller Id:5-SingleReader.OnGuard Door Held Open	6/28/2023 2:56:43 PM	OnGuard Door Held Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
	✓ 70408783-3748-46se-b1e9-dbf0b48cfc35 Door #	1 on Controller Id 5-SingleReader.OnGuard Access Granted	6/28/2023 2:56:42 PM	OnGuard Access Granted	144/523c-51bd-5251-8/a7-7d876/b6cc44, 7#4e6d4-9078-5716-a83c-3#5a2t
	₩ #3b22096-2732-4s88-b428-60ebf9ca69b Door #	1 on Controller Id 3-MasterReader. OnGuard Door Held Open	6/28/2023 2:56:42 PM	On/Guard Door Held Open	ef7a3cbe-663d-541e-80o4-ceb1185809c3
	₩ 1edecd1d-8151-45fa-acc1-3ea185ebd010 Door #	1 on Controller Id 5-SingleReader.OnGuard Door Held Open	6/28/2023 2:56:42 PM	Or/Guard Door Held Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
	₩ 102212b0-3a10-4a60-b440-2fab/9a93231 Door #	1 on Controller Id:4-MasterReader.OnGuard Door Forced Open	6/28/2023 2:56:41 PM	OnGuard Door Forced Open	ef7a3cbe-663dr541e-80c4-ceb1185809c3
	★ 6360bd76-0925-4e53-b7c3-d8bd23cdaeb5 Door #	1 on Controller Id:4-MasterReader.OnGuard Invalid Badge	6/28/2023 2:56:41 PM	OnGuard Invalid Badge	87e8ae85-7671-592b-a896-b1c9936b8116, 7#4e6d4-9078-5716-a83c-3#5a
	✓ aad73ace-e47a-4e71-8e85-67838e35e140 Door #	1 on Controller Id:3-MasterReader.OnGuard Access Granted	6/28/2023 2:56:41 PM	OnGuard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6ccl4, 7#4e6d4-9078-5716-a83c-3#5a2t
	₩ bf022ab0-8b74-4f1a-9945-04146f19e6bc Door #	1 on Controller Id 4-MasterReader OnGuard Invalid Badge	6/28/2023 2:56:41 PM	On/Guard Invalid Badge	87e3ae85-7671-592b-a896-b1c5936b8116, 7H4e6d4-5078-5716-a83c-3H5a
	✓ 593b93c0-a553-4a50-be45-2ab3b7ad5c39 Door #	1 on Controller Id 6-MasterReader. OnGuard Door Forced Open	6/28/2023 2:56:41 PM	On/Guard Door Forced Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
	₩ 909244e7-e535-4c1d-8529-8383e03534ad Door #	1 on Controller Id 5 SingleReader OnGuard Access Granted	6/28/2023 2:56:40 PM	Or/Guard Access Granted	144/923c-51bd-5251-81a7-7d876fb6ccf4, 7lf4e6d4-9078-5716-a83c-3lf5a2
	★ 54be26bc-158c-47df-bb22-a7d8b8eb04ed Door =	1 on Controller Id 5-SingleReader.OnGuard Door Forced Open	6/28/2023 2:56:40 PM	OnGuard Door Forced Open	ef7a3cbe-663d-541e-80c4-ceb1185809c3
	★ 962832b9-d?ae-4bba-a407-4ebec394e935 Door #	1 on Controller Id 9-SingleReader.OnGuard Invalid Badge	6/28/2023 2:56:40 PM	OnGuard Invalid Badge	87e8ae85-7671-592b-s896-b1c936b8116, 7H4e6d4-9078-5716-a83c-3H5e
	✔ 16e4/e7b-14ce-4663-bc13-5cebdf577823 Door #	1 on Controller Id:2-SingleReader.OnGuard Access Granted	6/28/2023 2:56:40 PM	OnGuard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6cc44, 7#4e6d4-9078-5716-a83c-3#5a2
	¥ 26c5a190-b30a-4dea-b540-25/33cbcde04 Door #	1 on Controller Id 4-SlaveReader.On/Guard Access Granted	6/28/2023 2:56:40 PM	On/Guard Access Granted	144/923c-51bd-5251-8/a7-7d876/b6cc44, 7#4e6d4-9078-5716-a83c-3#5a2
	¥ 16ab561a-3129-43aa-9693-2d021023a7e1 Door #	1 on Controller Id:1-SingleReader.OnGuard Access Granted	6/28/2023 2:56:40 PM	Or/Guard Access Granted	144/923c-51bd-5251-81a7-7d87686cc44, 7#4e6d4-9078-5716-a83c-3#5a2
	Related Access Control Credential Holders:	Related Access Control Items	Properties:		Related Surveillance Items:
	neiaseo Access Coreos Credential Holders.	Neutros Access Control Herris.	riopenses:		heased ourvemance raths:
					Activate Windows
	Control Access Request Notifications	DEV. Info DEV: Item States & Commands DEV: Catego	Massing DEV	Cenera Macoino DIFV-	Go to Settings to activate Windows. Ave Events DEV: Live State Changes DEV: Live Credential (

C	DEV: Live State Changes	This tab displays the live status changes of devices and servers. This tab has no memory.

	Access Control Information	
Access Control	Icon Trmestemp AccessControlSystemName SourceIter/Name NewStates New	Categories
OnGuard		r closed. Door locke
	G28/2023 3.05 53 PM OnGuard OnGuard Door #1 on Controller Id:2-Single/Reader OnGuard Reader Closed, OnGuard Reader Mode Locked, O	
	6/28/2023 3 05 52 PM On/Guard Door for Door #1 on Controller 1d 2-Single/Reader On/Guard Door Online, On/Guard Door Unlocked Doo	r open, Door unlocke
	628/2023 3 05 52 PM OrGuard Door #1 on Controller Id 2-SingleReader OrGuard Reader Mode Locked, OrGuard Reader Online, OrGuard Reader Unlocked	
	NewState Properties:	
	Activate Windows	
	Go to Settings to activate V	

DEV: Live Credential Holder Changes	This tab shows all credentials added to the XProtect Access system. This tab has no memory.	
-------------------------------------	---	--

	Roles	PropertiesCount	PictureImageSource	Name	Roles	PropertiesCount	AccessControlCredentialHolder
Diana ROSS	Visitor	5	System Windows Media Imaging WriteableBitmap	Diana ROSS	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCon
Danielle LONG	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Danielle LONG	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCon
Marilyn MYERS	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Marilyn MYERS	Visitor	5	VideoOS.Platform.AccessControl.Internal.Data.AccessCon
Amber PATEL	Employee	5	System Windows Media Imaging WriteableBitmap	Amber PATEL	Employee	5	VideoOS Platform AccessControl Internal Data AccessCon
Denise SANDERS	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Denise SANDERS	Visitor	5	VideoOS.Platform.AccessControl.Internal.Data.AccessCon
Jane CASTILLO	Employee	5	System Windows Media Imaging WriteableBitmap	Jane CASTILLO	Employee	5	VideoOS Platform AccessControl Internal Data AccessCon
Sophia ALVAREZ	Employee	5	System.Windows.Media.Imaging.WriteableBitmap	Sophia ALVAREZ	Employee	5	VideoOS Platform AccessControl Internal Data AccessCon
Beverly PRICE	Employee	5	System.Windows.Media.Imaging.WriteableBitmap	Beverly PRICE	Employee	5	VideoOS Platform AccessControl Internal Data AccessCon
Judy HUGHES	Visitor	5	System Windows Media Imaging WriteableBitmap	Judy HUGHES	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCon
Abigail RUIZ	Employee	5	System.Windows.Media.Imaging.WriteableBitmap	Abigail RUIZ	Employee	5	VideoOS Platform AccessControl Internal Data AccessCon
Charlotte MENDOZA	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Charlotte MENDOZA	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Madison GRAY	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Madison GRAY	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Theresa BENNETT	Employee	5	System.Windows.Media.Imaging.WriteableBitmap	Theresa BENNETT	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Janice JAMES	Visitor	5	System Windows Media Imaging WriteableBitmap	Janice JAMES	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Gloria WOOD	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Gloria WOOD	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Teresa CHAVEZ	Employee	5	System.Windows.Media.Imaging.WriteableBitmap	Teresa CHAVEZ	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Jacqueline BROOKS	Visitor	5	System Windows Media Imaging WriteableBitmap	Jacqueline BROOKS	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCon
Sara WATSON	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Sara WATSON	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Andrea RICHARDSON	Employee	5	System Windows Media Imaging WriteableBitmap	Andrea RICHARDSON	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Megan WARD	Employee	5	System Windows Media Imaging WriteableBitmap	Megan WARD	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Cheryl COX	Employee	5	System.Windows.Media.Imaging.WriteableBitmap	Cheryl COX	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Hannah KIM	Employee	5	System Windows Media Imaging WriteableBitmap	Hannah KIM	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Mildred RAMOS	Visitor	5	System Windows Media Imaging WriteableBitmap	Mildred RAMOS	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Judith HOWARD	Visitor	5	System Windows Media Imaging WriteableBitmap	Judith HOWARD	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Kathryn KELLY	Visitor	5	System Windows Media Imaging WriteableBitmap	Kathryn KELLY	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Lillian REED	Visitor	5	System.Windows.Media.Imaging.WriteableBitmap	Lillian REED	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Jean BAILEY	Visitor	5	System Windows Media Imaging WriteableBitmap	Jean BAILEY	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Doris PETERSON	Employee	5	System Windows Media Imaging WriteableBitmap	Doris PETERSON	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Julia COOPER	Employee	5	System Windows Media Imaging WriteableBitmap	Julia COOPER	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Ann MORGAN	Employee	5	System Windows Media Imaging WriteableBitmap	Ann MORGAN	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Lauren ORTIZ	Visitor	5	System Windows Media Imaging WriteableBitmap	Lauren ORTIZ	Visitor	5	VideoOS Platform AccessControl Internal Data AccessCont
Kelly GUTIERREZ	Employee	5	System Windows Media Imaging WriteableBitmap	Kelly GUTIERREZ	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont
Christina ROGERS	Employee	5	System Windows Media Imaging WriteableRitman	Christina ROGERS	Employee	5	VideoOS Platform AccessControl Internal Data AccessCont

All other support issues

For issues not covered in this guide, please contact Milestone Support at support@milestone.us, or by phone at 503-350-1100.

Version Notes

Current document version

Version	Notes
4.4	Current documentation refers to integration versions 4.4 and newer.

For more information on earlier versions, check version specific documents. For version specific change details, check release notes available with each version's documentation.

Run this script once, to create a certificate that can sign multiple server SSL certificates

Thumbprint of private certificate used for signing other certificates
Set-Content -Path "\$PSScriptRoot\ca_thumbprint.txt" -Value \$ca_certificate.Thumbprint

Public CA certificate to trust (Third-Party Root Certification Authorities)
Export-Certificate -Cert "Cert:\CurrentUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\root-authority-public.cer"

Appendix B | Create Server SSL Certificate script

```
# Run this script once for each server for which an SSL certificate is needed.
# Certificate should be executed on the single computer where the CA certificate is located.
# The created server SSL certificate should then be moved to the server and imported in the
# certificate store there.
# After importing the certificate, allow access to the private key of the certificate for
# the service user(s) of the services that must use the certificate.
# Load CA certificate from store (thumbprint must be in ca_thumbprint.txt)
$ca_thumbprint = Get-Content -Path "$PSScriptRoot\ca_thumbprint.txt"
$ca certificate = (Get-ChildItem -Path cert:\CurrentUser\My\$ca thumbprint)
# Prompt user for DNS names to include in certificate
$dnsNames = Read-Host 'DNS names for server SSL certificate (delimited by space - 1st entry is also subject of certificate)'
$dnsNamesArray = @($dnsNames -Split ' | foreach { $_.Trim() } | where { $_})
if ($dnsNamesArray.Length -eq 0) {
    Write-Host -ForegroundColor Red 'At least one dns name should be specified'
    exit
}
$subjectName = $dnsNamesArray[0]
$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Join '&'
# Optionally allow the user to type in a list of IP addresses to put in the certificate
$ipAddresses = Read-Host 'IP addresses for server SSL certificate (delemited by space)'
$ipAddressesArray = @($ipAddresses -Split ' | foreach { $ .Trim() } | where { $ })
if ($ipAddressesArray.Length -gt 0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$ " }) -Join '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}
# Build final dns entries string (e.g. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={text}$dnsEntries"
# The only required purpose of the sertificate is "Server Authentication"
$serverAuthentication = '2.5.29.37={critical}{text}1.3.6.1.5.5.7.3.1'
# Now - create the server SSL certificate
$certificate = New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject $subjectName -Signer $ca certificate `
                                         -FriendlyName 'VMS SSL Certificate' -TextExtension @($dnsEntries, $serverAuthentication)
```

```
# Export certificate to disk - protect with a password
$password = Read-Host -AsSecureString "Server SSL certificate password"
Export-PfxCertificate -Cert "Cert:\CurrentUser\My\$($certificate.Thumbprint)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password
```

```
# Delete the server SSL certificate from the local certificate store
$certificate | Remove-Item
```



helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.

