MAKE THE
WORLD SEE

Milestone Systems

XProtect Access for OnGuard

Manual

milestone

Contents

Copyright, trademarks, and disclaimer

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 4.2?

The most prominent changes to version 4.2 of the OnGuard XProtect Access integration are listed below.

Requirements:

- OnGuard and XProtect version support statement: OnGuard & XProtect Compatibility.

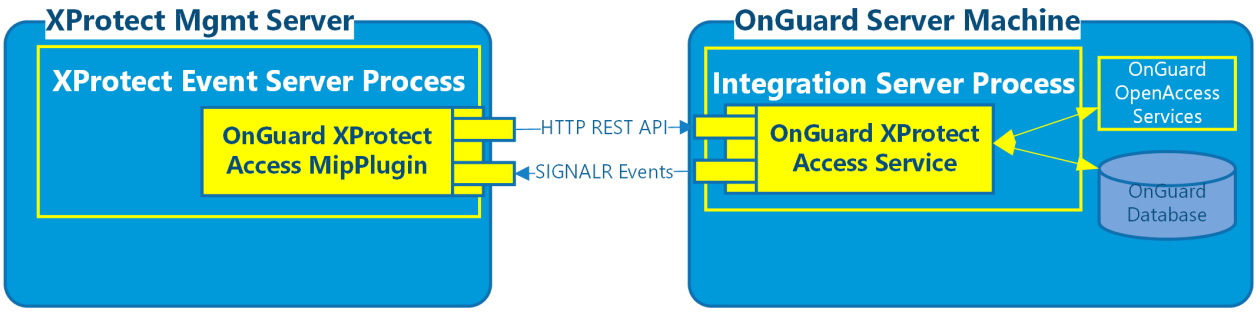
Features & User Experience:

- Improved map icons. Map icon hardware and status details on page 75
- End to end encryption. Secure communications explained on page 22
- Expanded alarm acknowledgment options. Alarm acknowledgment explained on page 78
- Increased customization for cardholder data display. Working with the PluginSettings.json configuration file on page 92
- Enhanced log viewer. Using the log viewer application on page 89

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

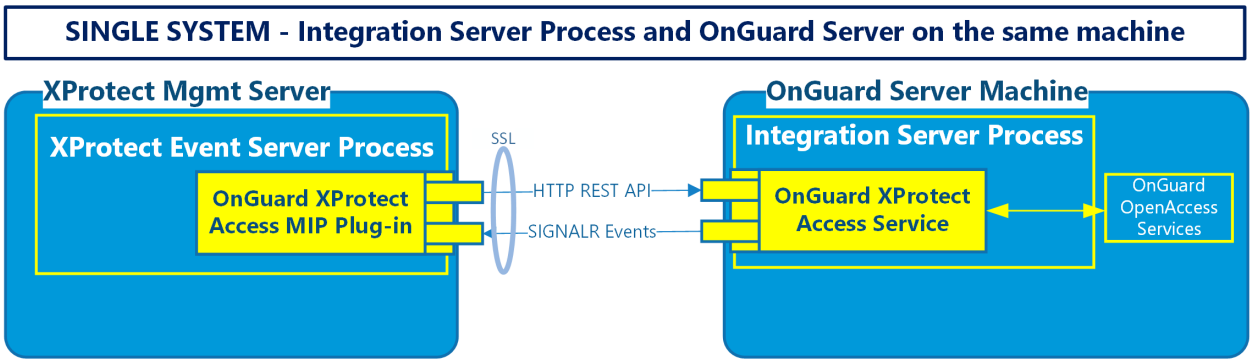
Different installation scenarios (explained)

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.
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

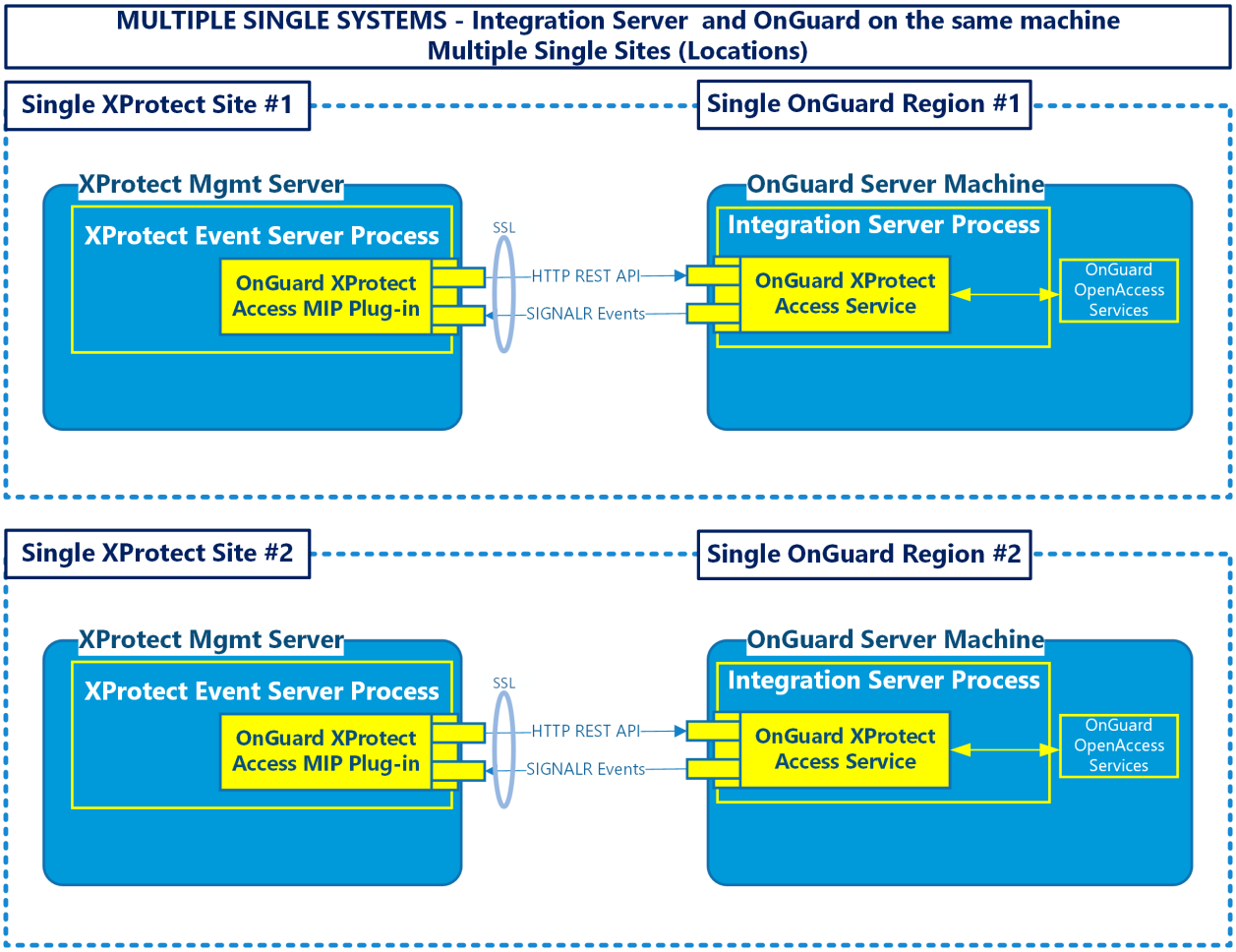


For most systems, this is the recommended installation scenario.

- 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

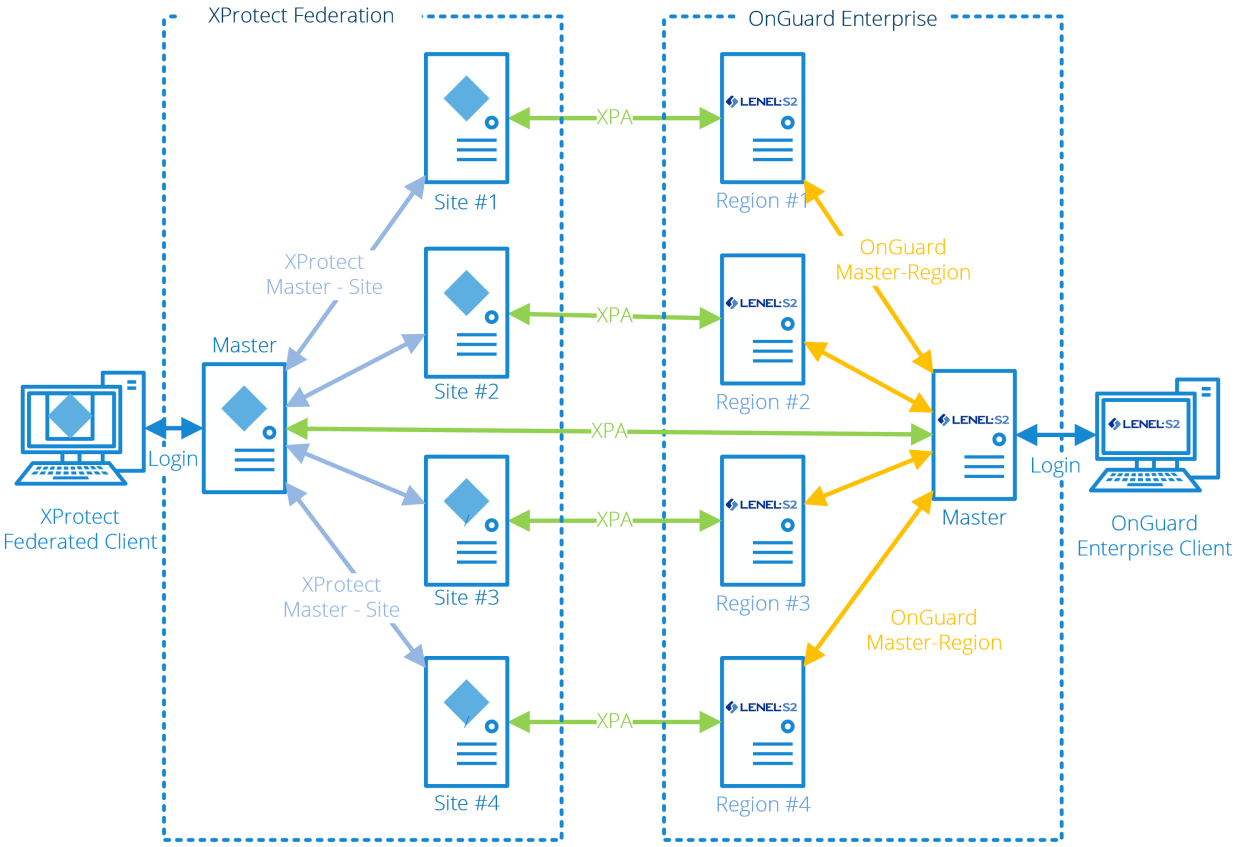
Scaling the default scenario means adding more OnGuard systems and XProtect systems in a 1:1 ratio. The OnGuard and XProtect systems are independent of each other, keeping the OnGuard XProtect Access Service process on the OnGuard machine. The customer is NOT interested in centralized configuration or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



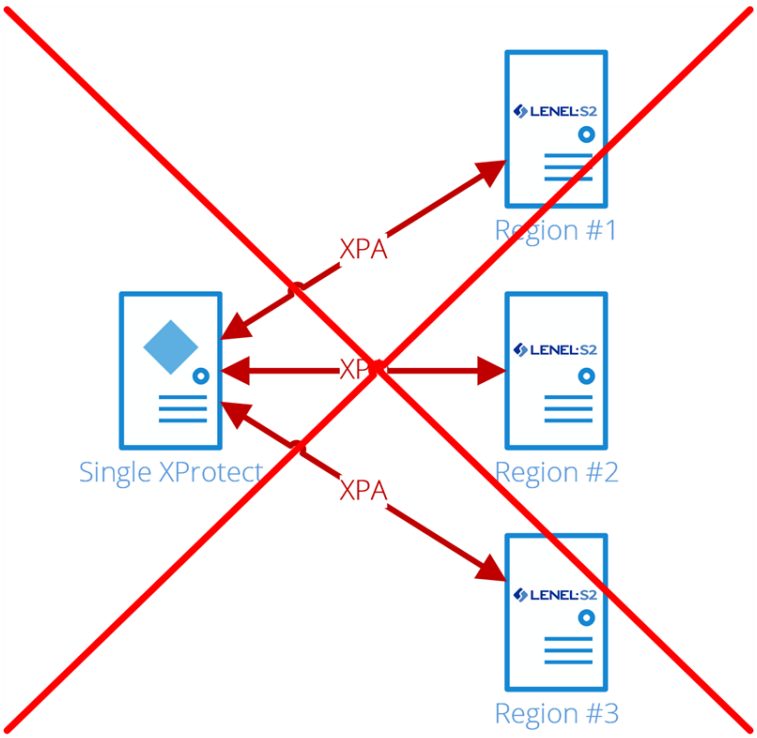
Site #1 and site #2 are independent of each other and not communicating with each other, or commonly managed. The same is true for both the XProtect and the OnGuard systems in this scenario.

Milestone XProtect Federated Architecture with OnGuard Enterprise

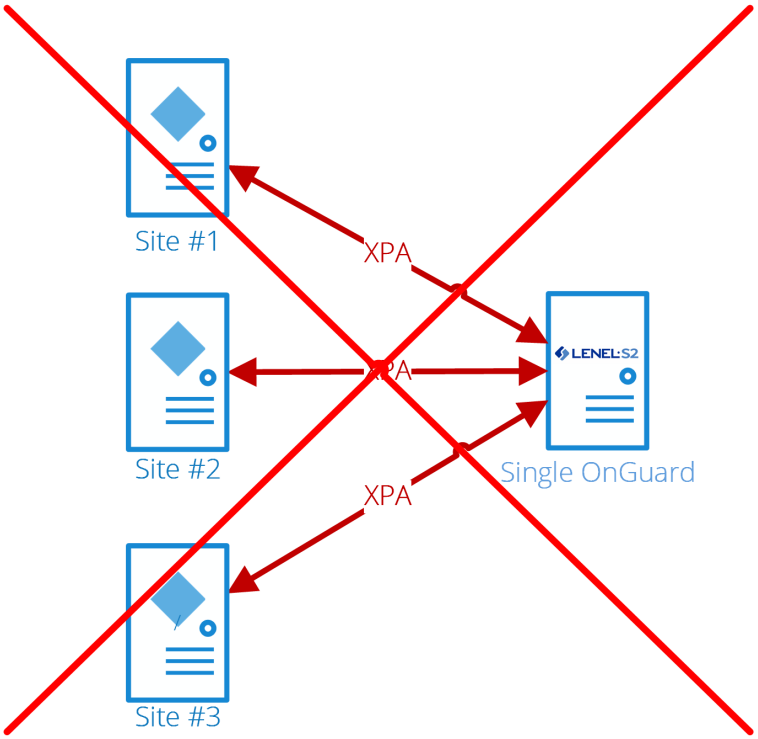
This scenario has many uses. It is recommended for large scale deployments. This is the default scenario when the customer has an Enterprise deployment of OnGuard and wants to integrate with XProtect. Also, it is recommended when the customer wants centralized alarm and configuration management for both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



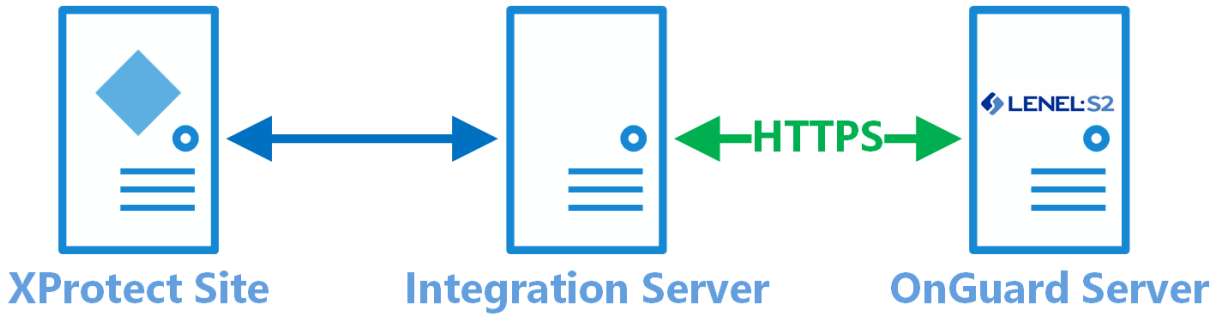
Milestone DOES NOT support connecting more than one XProtect site to a single OnGuard region.



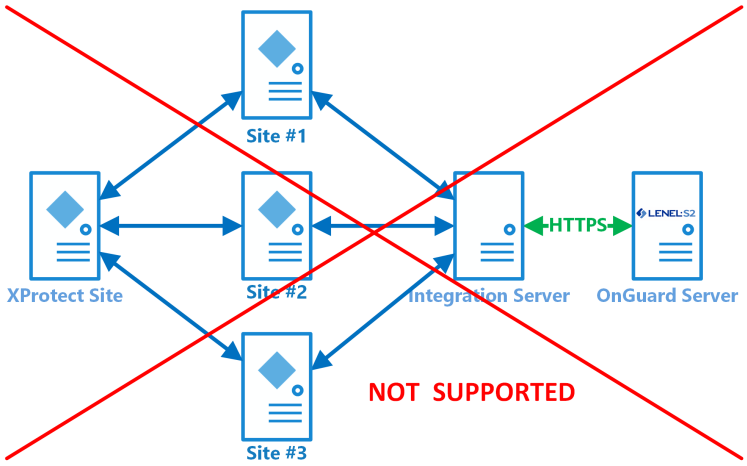
Each XPA line in these diagrams represents the HTTP/SignalR connection between the Event Server in XProtect and the OnGuard XProtect Access Service on the OnGuard server. There are some scenarios where the OnGuard XProtect Access Service may not live on the same OnGuard server, see Distributed deployment options on page 13 for details.

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.

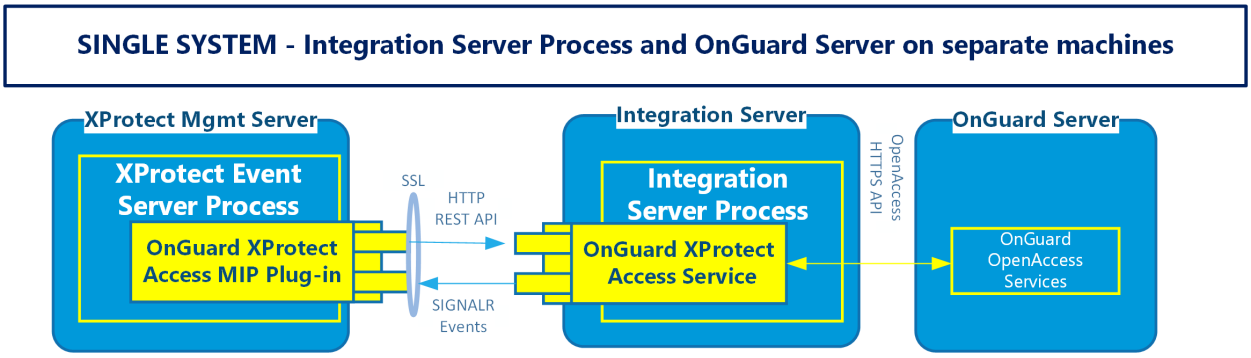


> For design, scaling, and performance reasons, Milestone doesn't support connecting multiple XProtect sites to the same Integration Server instance.



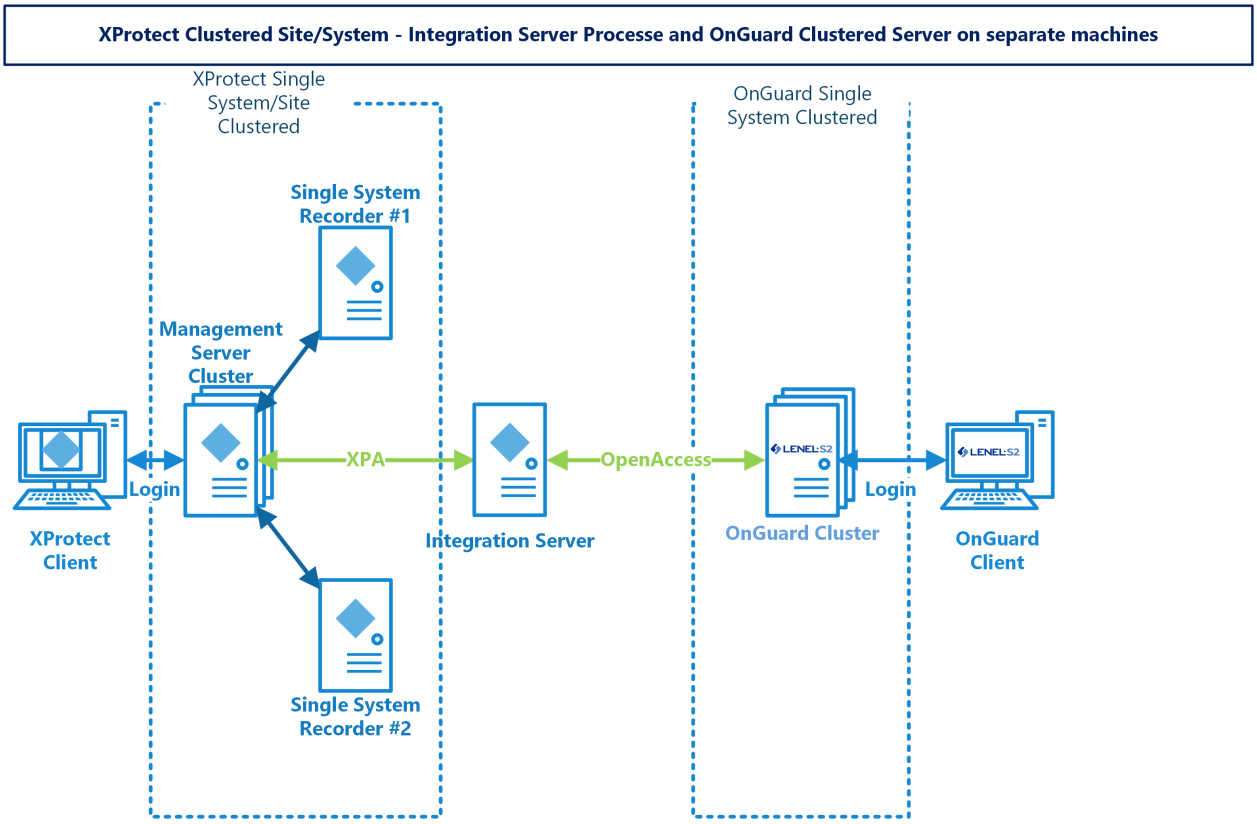
Single system with integration server

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 OnGuardXProtect Access integration.

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

Both XProtectManagement 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 reestablish 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 forh all XProtect VMS products that support MIP integrations.

Read the most recent compatibility information.

> 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.

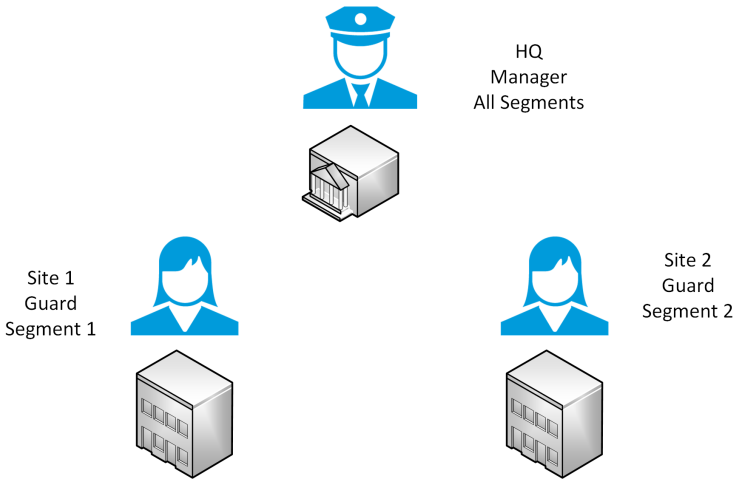
OnGuard segments explained

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.

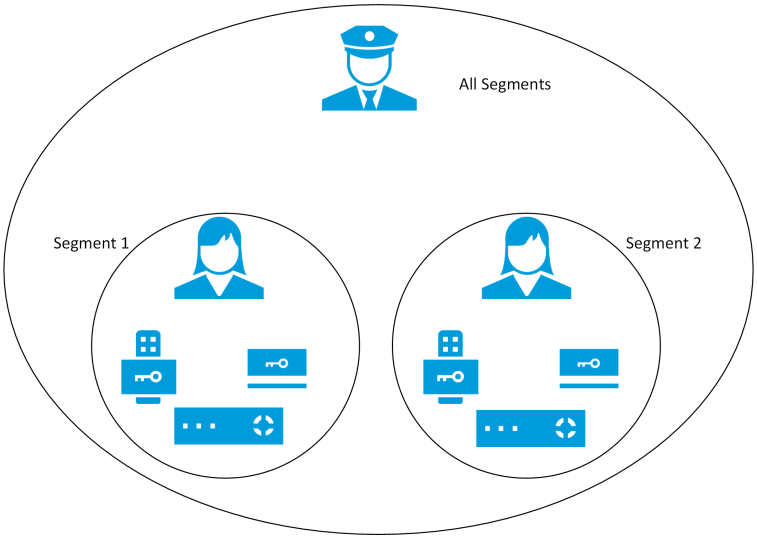
> Creating a segmented system within OnGuard shouldn't be a part of installing the XProtect Access OnGuard integration. It's recommended to consult with an authorized OnGuard representative before configuring segments.

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.



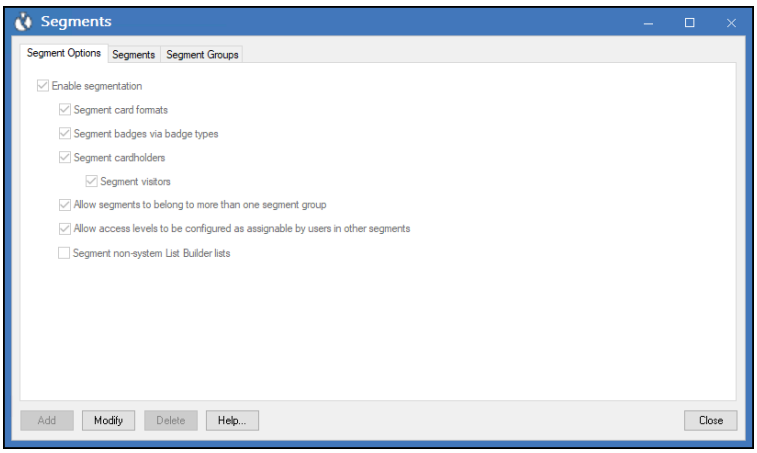
Using segments, the guard user at site 1 can see readers, panels, and cardholders from segment 1, and the guard user from site 2 can see the devices and information from segment 2. The manager can see all devices and information, since they're in the default "All Segments" segment.



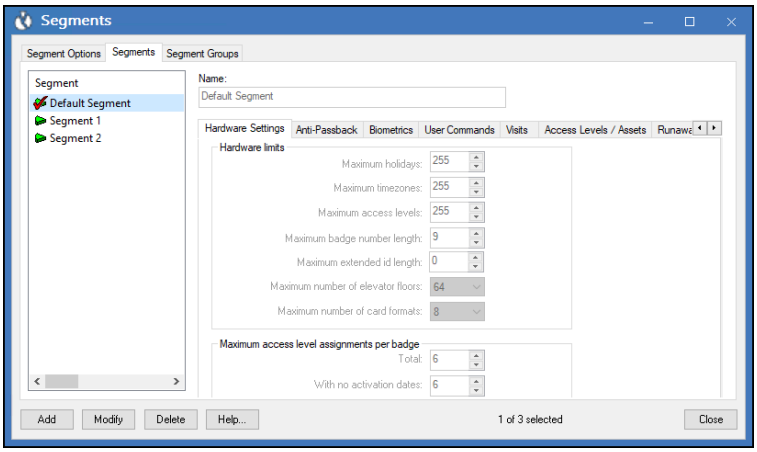
Configuring segments within OnGuard

> 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.



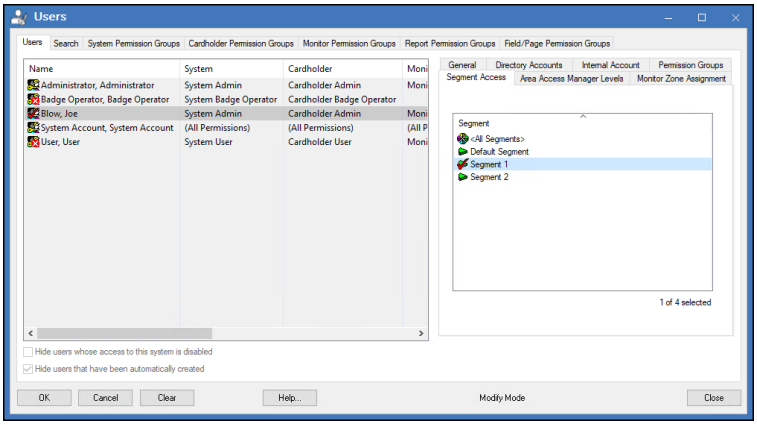
3. The **Segments** tab contains the segments configured within OnGuard.



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.

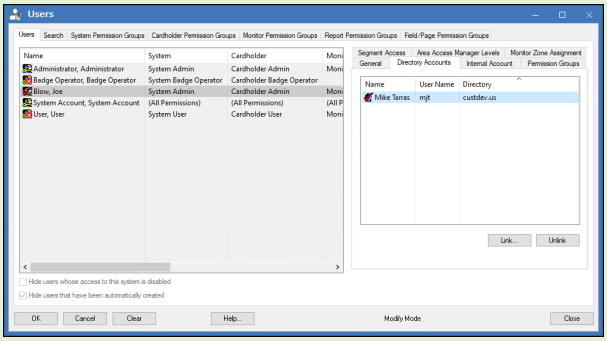
4. In the **Segment** listing window, select the segment(s) the user has access to.



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** sub-tab of the **Users** sub-menu of the **Administration** menu in the OnGuard System Administration application.

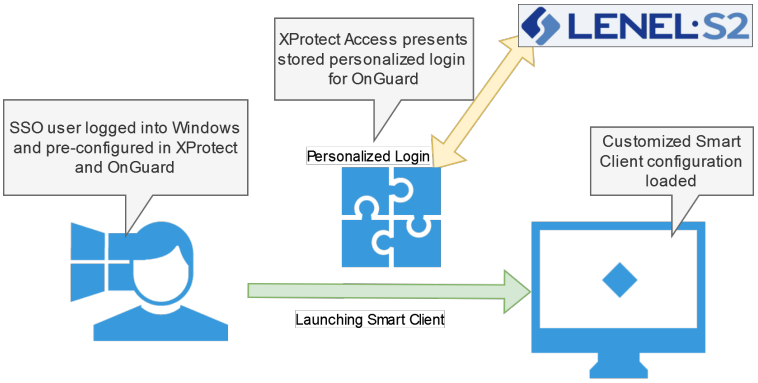


XProtect Access and SSO authentication (explained)

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.



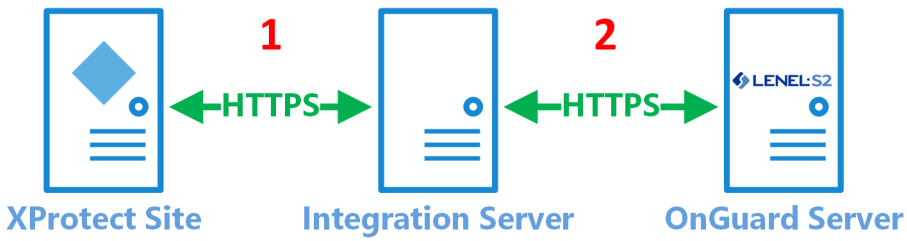
This is the closest to a true SSO user experience that the XProtect Access integration offers. It requires using the personalized login feature. If this feature isn't used, all authentication to OnGuard from XProtect Access uses the same user credentials that the OnGuard XProtect Access Service uses 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.



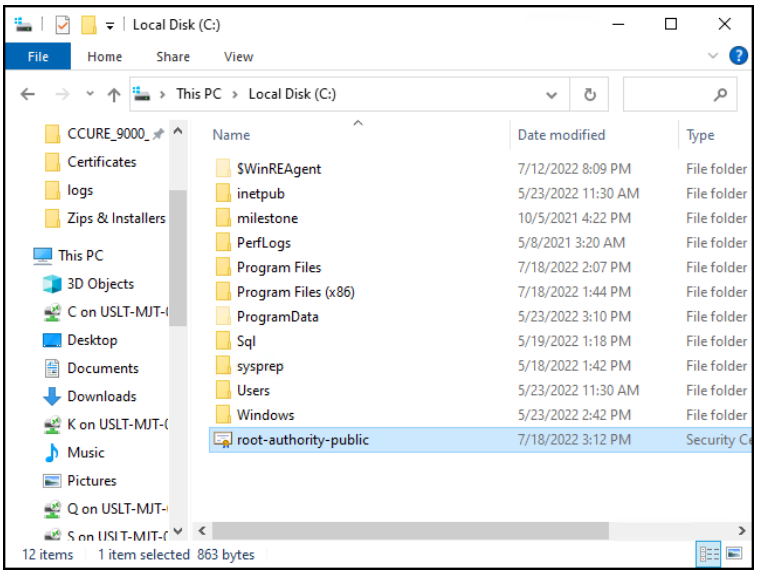
1. Certificate generation, distribution, and configuration supporting secure communications between XProtect and the OnGuard XProtect Access Service.
2. Certificate extraction, distribution, and configuration supporting secure communications between OpenAccess and the OnGuard XProtect Access Service. 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.

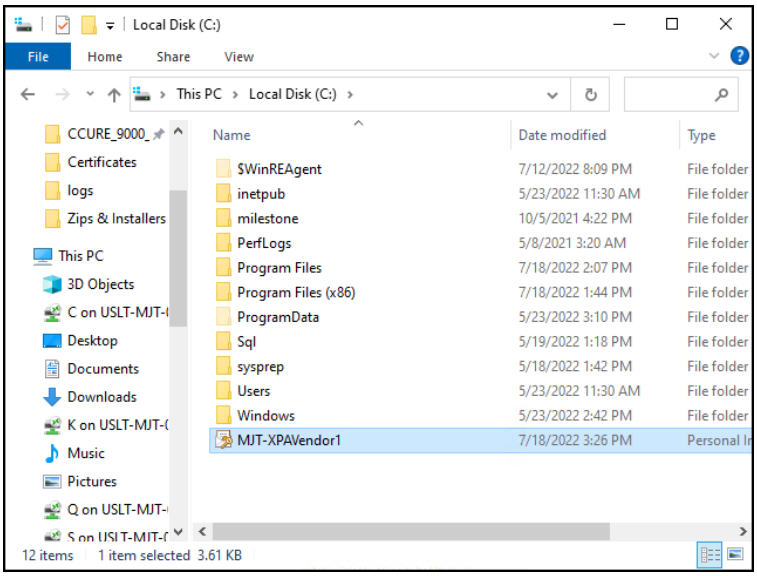
> The process included below is for self-signed certificates. If you are using a third party certificate, from a commercial certificate provider, please skip ahead to step number ten below. Refer to the XProtect Certificate Guide for any questions on dealing with certificates.

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

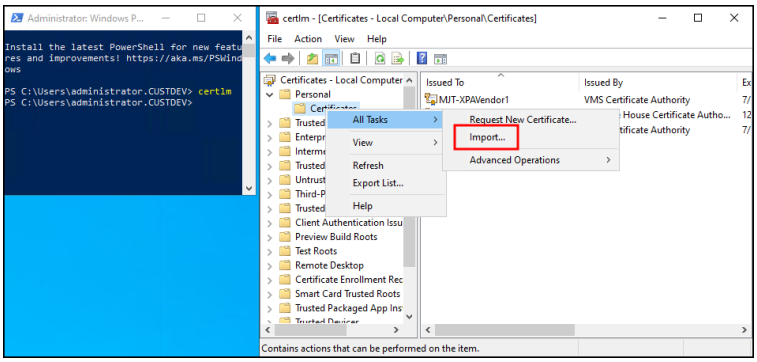


2. By default the script places the new root certificate in the **C:** file location. Move the certificate to the XProtect server.
3. On the XProtect server right-click the certificate and select **Install Certificate** to begin the certificate installation wizard.
4. Choose to place the certificate 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.
7. 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.
8. 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.

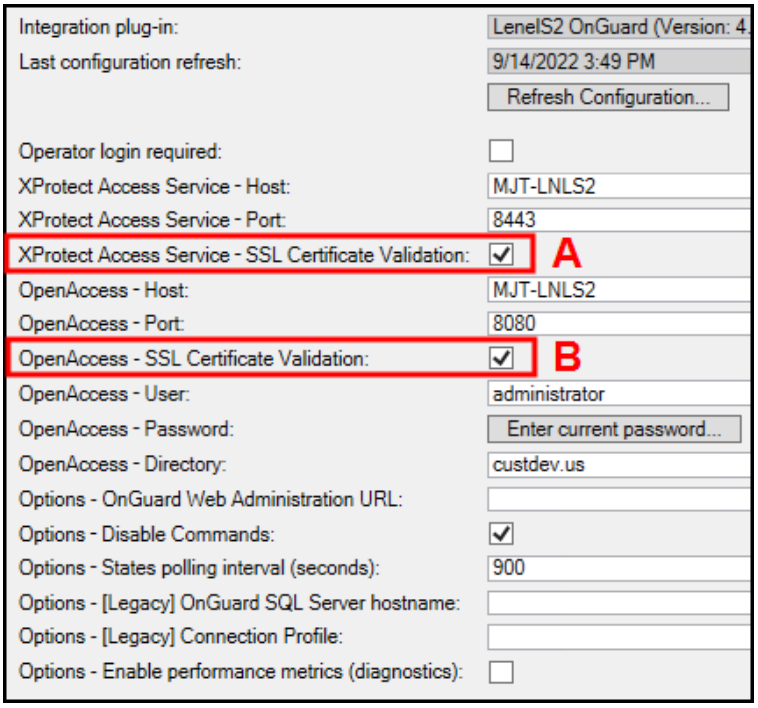


10. Go to the server hosting the OnGuard XProtect Access Service and run the certificates snap-in for the local machine. Right-click the **Certificate** store within the **Personal** folder and choose to **Import** a new certificate.



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.
13. Now apply encryption for the OnGuardXProtect 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.



Applying secure communications between the OnGuard XProtect Access Service and OpenAccess

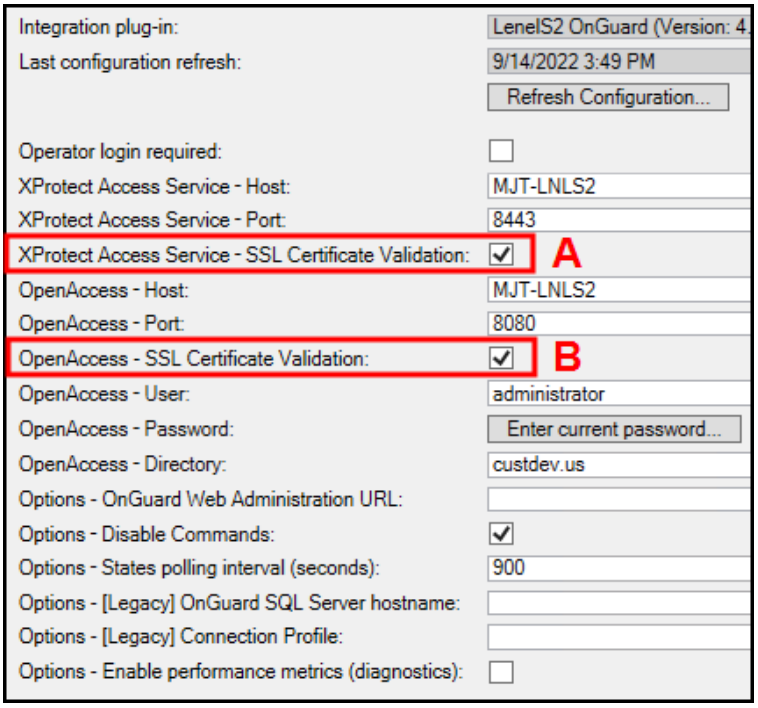
In versions 4.2 and higher of the XProtect Access OnGuard integration, encrypted communication is fully supported. This process shows the steps required to extract and distribute the required certificates and configure the solution to enable secure communications between the OnGuard XProtect Access Service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

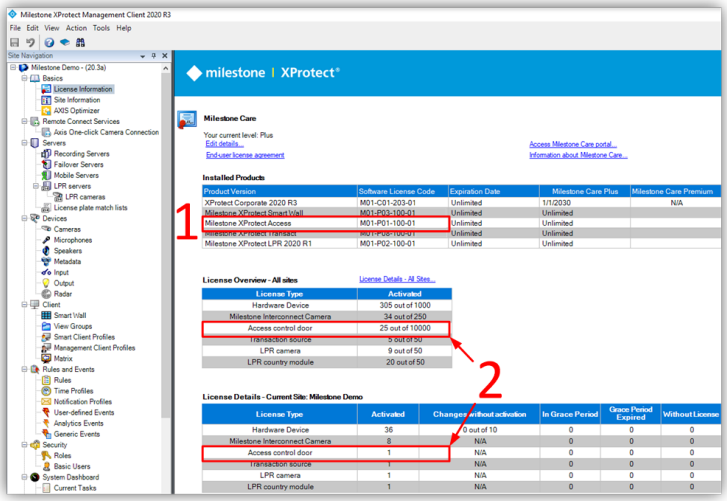
All OnGuard and XProtectservers must be time-synchronized to within a couple of minutes.

.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	OpenAccess Integration (ITM-MLST-001) enabled with an expiration date 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 DataConduIT license, please refer to Milestone Knowledge Base article 33277.

Required OnGuard services

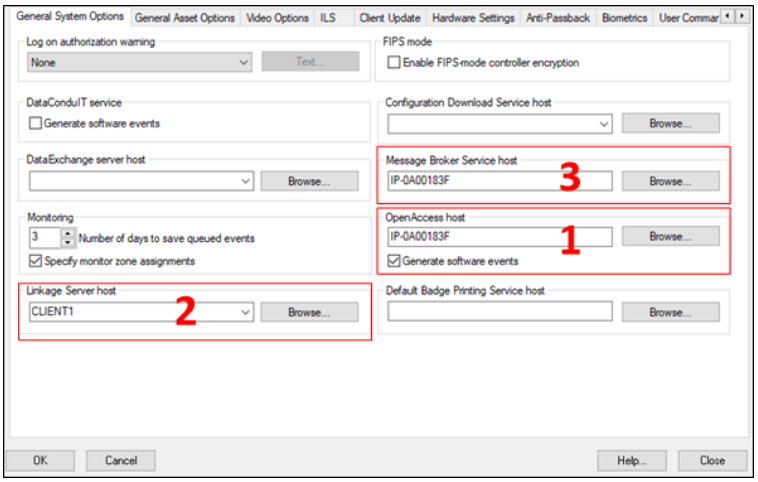
The following Windows services must run on the OnGuard machine:

OnGuard Windows Service Name	Description
LS Event Context Provider	Required to send events from the OnGuard system
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**:

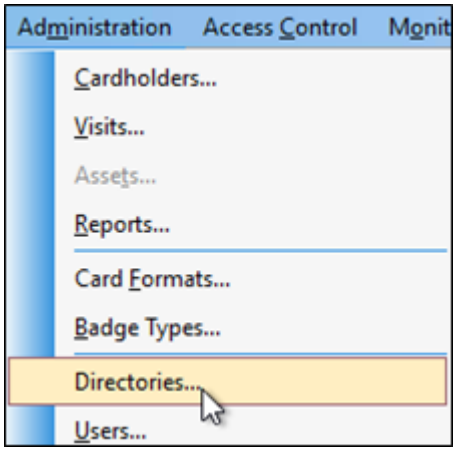
1. For OnGuard versions greater than or equal to 7.4 using OpenAccess, check the **OpenAccess host** and **Generate software events** checkbox.
2. Set the **Linkage Server host** to the OnGuard server's machine name.
3. Set the **Message Broker Service host** to the OnGuard server's machine name.



Create directory in OnGuard

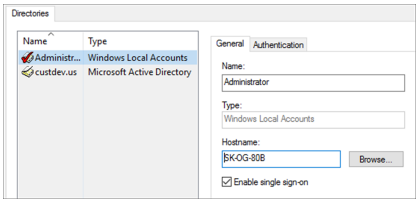
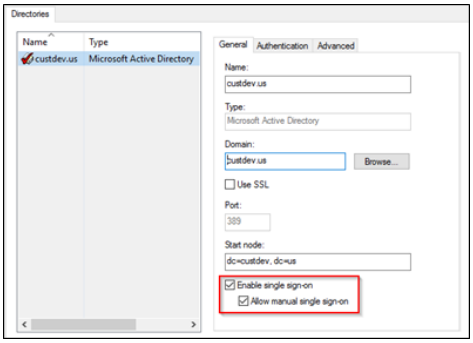
> These instructions are not meant to replace the knowledge of a trained LenelS2 system administrator. They are here to enable the basic setup of an authentication directory and user, so the integration can connect to the OnGuard system.

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.

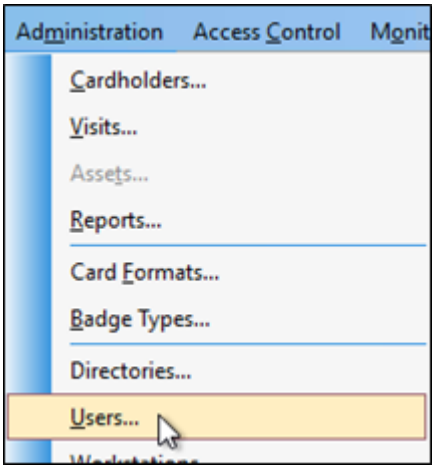
For **Windows Local Account** support, the single sign-on account MUST be a **Windows Local Account**.	For Domain User Account support, the single sign-on account MUST **Allow manual single sign-on** as shown below.
	

> 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.

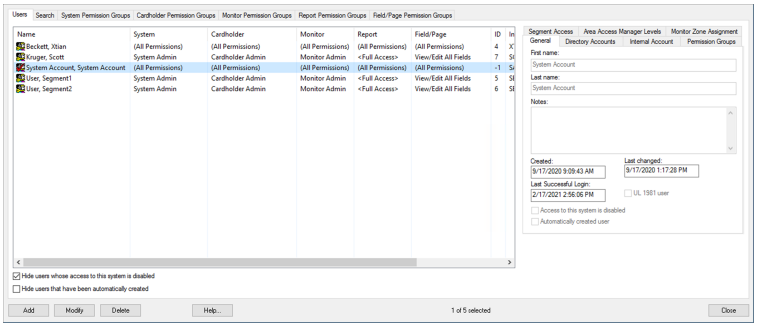
Create user in OnGuard

> 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.

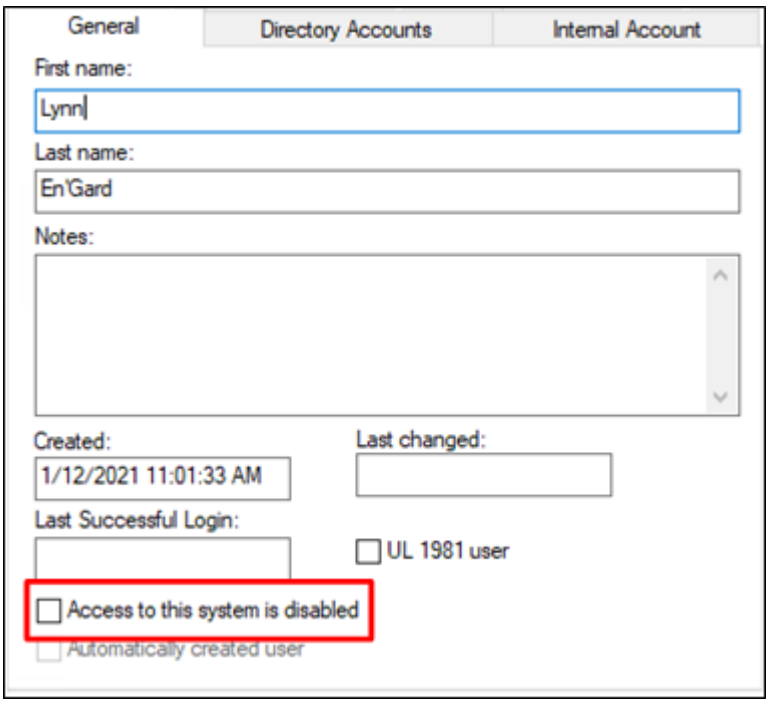
1. Go to the **Administration** menu and select **Users...**



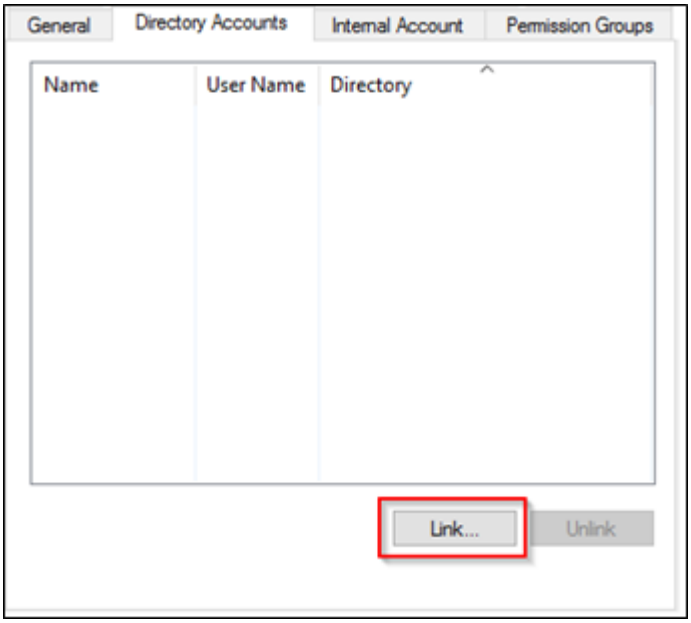
2. Add a new user, or modify a user from the list of internal system users.



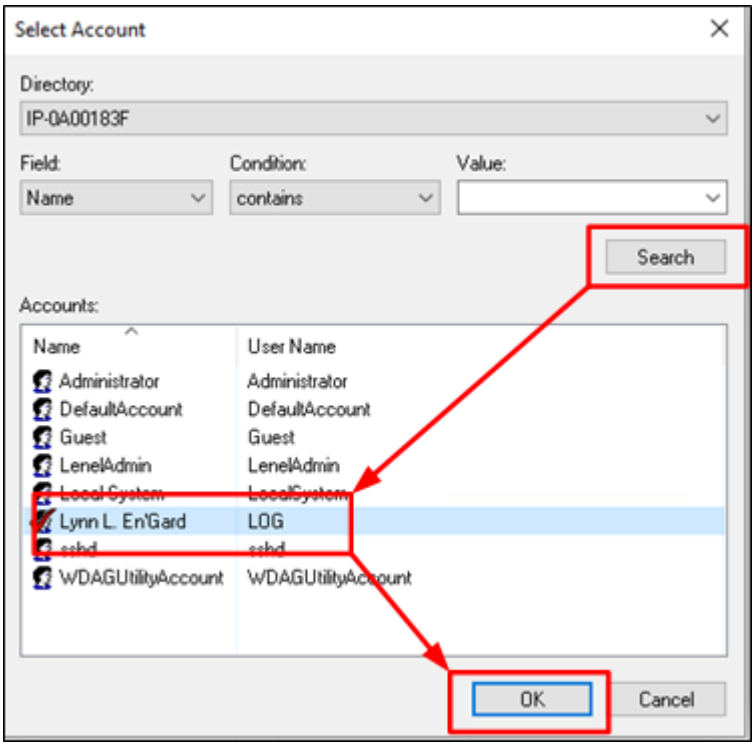
3. On the **General** tab **Access to this system is disabled** should NOT be selected.



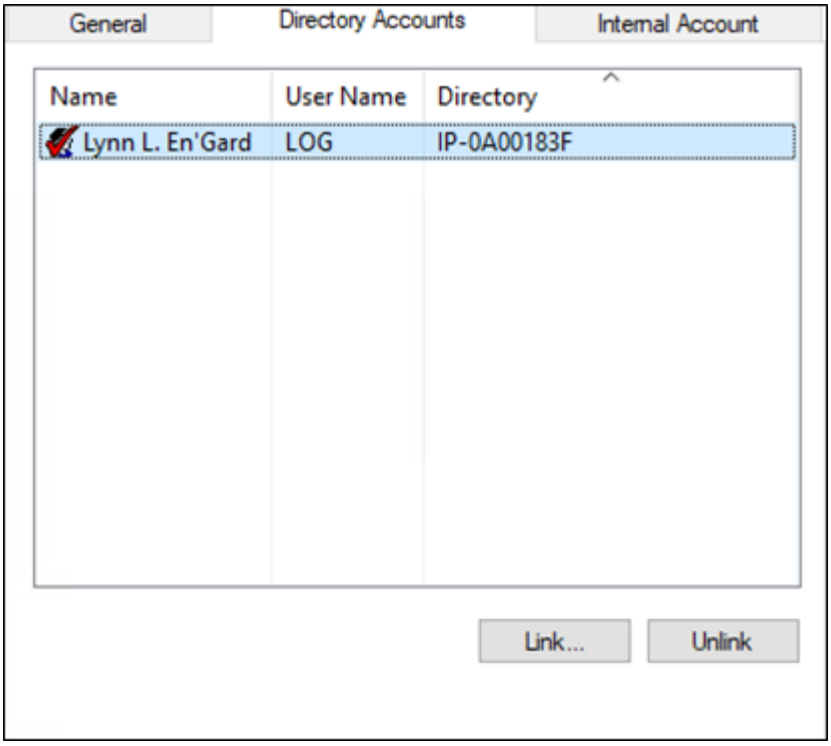
4. On the **Directory Accounts** tab click **Link** to associate the user to the directory user (or local account user) from the directory created in this topic: Create directory in OnGuard on page 30.



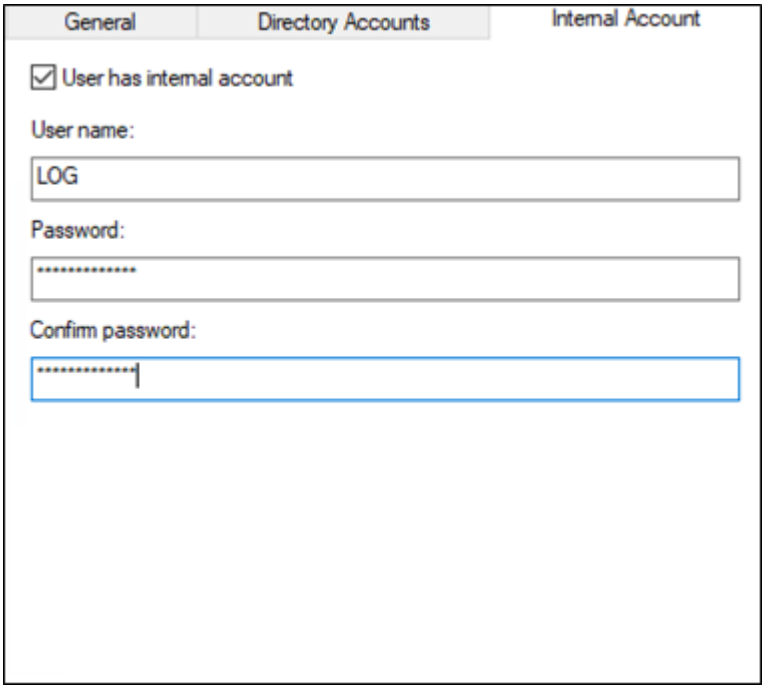
5. In the **Select Account** dialog select the directory from the Directory list. Click **Search** and select a user in **Accounts** then click **OK**.



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

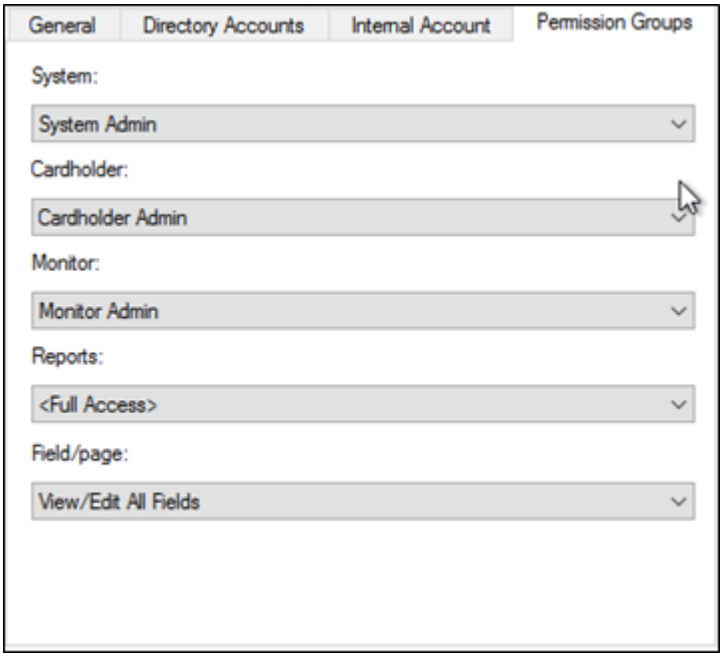


7. On the **Internal Account** tab, make sure that the **User has internal account** option is selected. Next, enter the account credentials.



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**



Installation

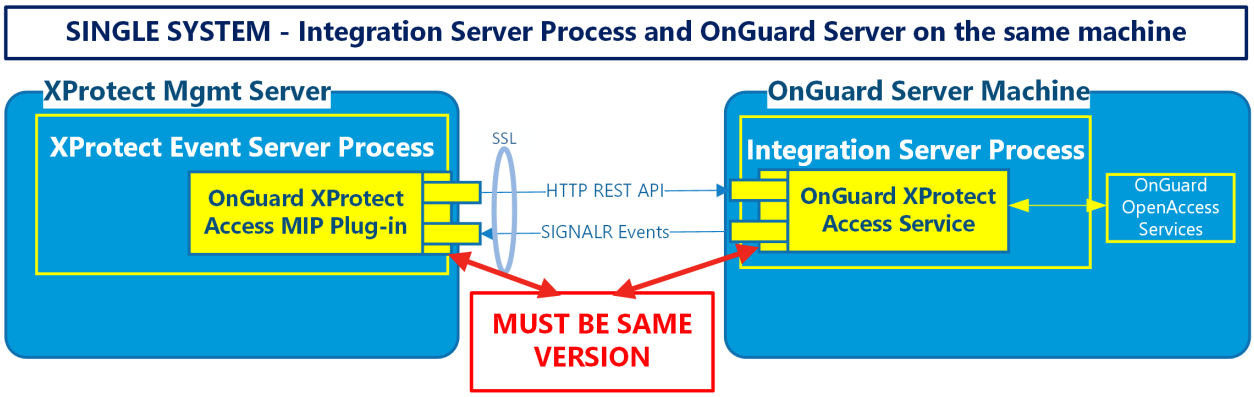
Installation program (explained)

The installation package consists of one context sensitive installer program:

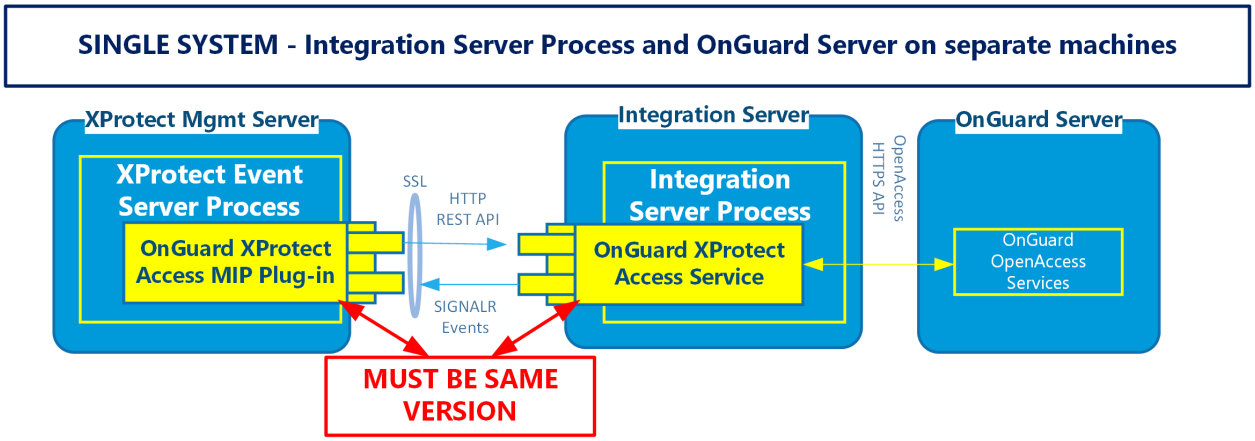
- XProtectAccess.OnGuard.msi

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.



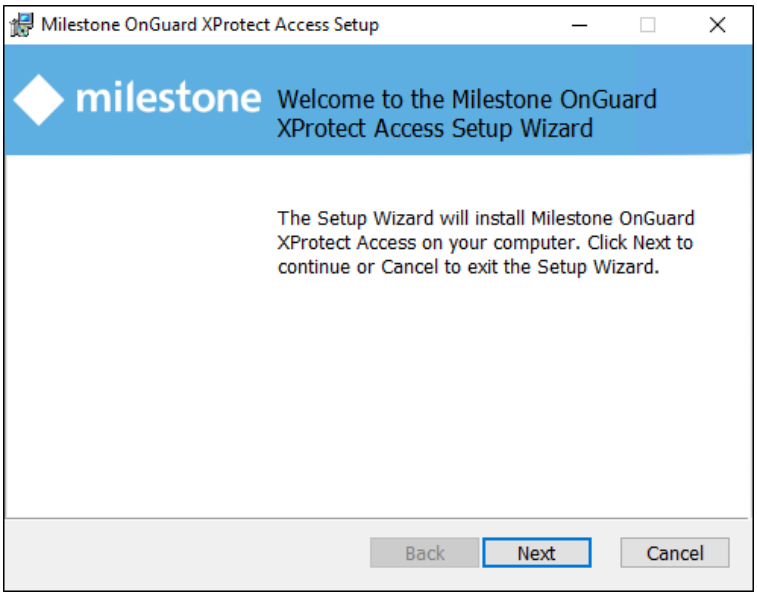
OR



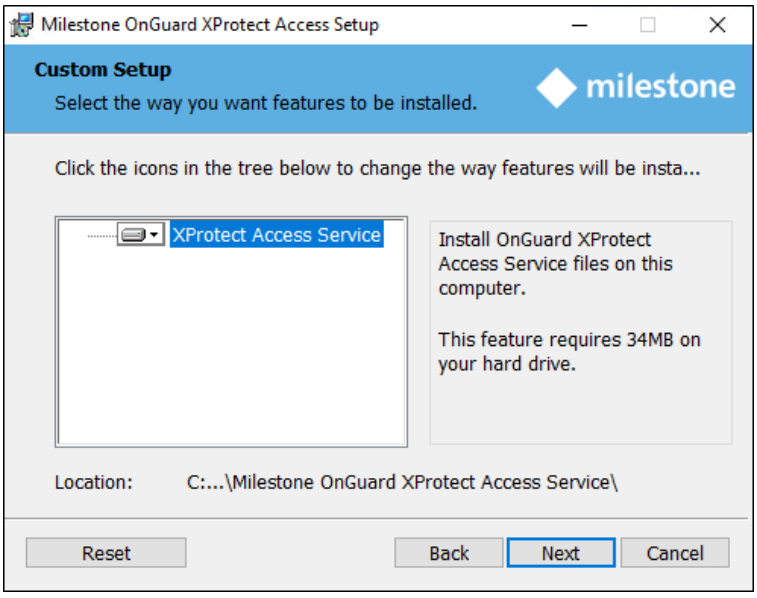
> It's required that the exact same versions of the OnGuard XProtect Access integration software components are installed on both the XProtect and OnGuard machines.

Step 1: Installing OnGuard XProtect Access Service

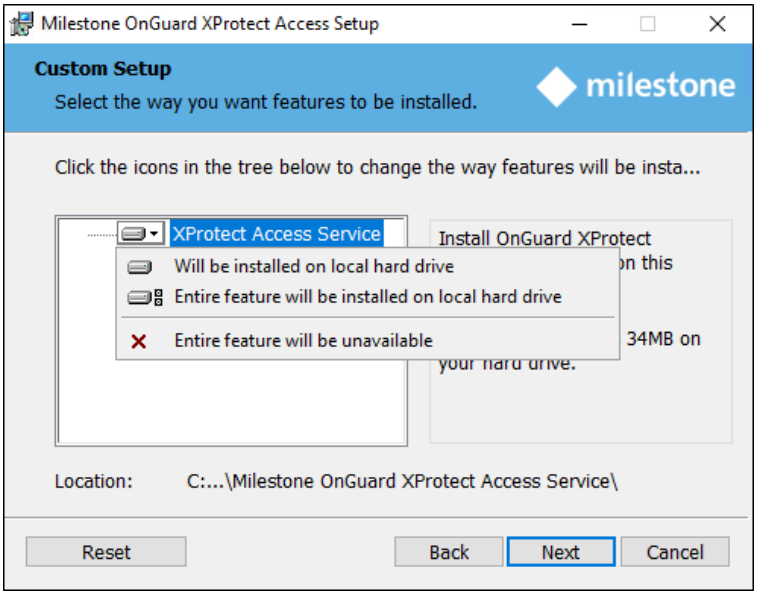
1. Double-click the XProtectAccess.OnGuard.msi file to begin.
2. The installation wizard launches. Click **Next** to continue.



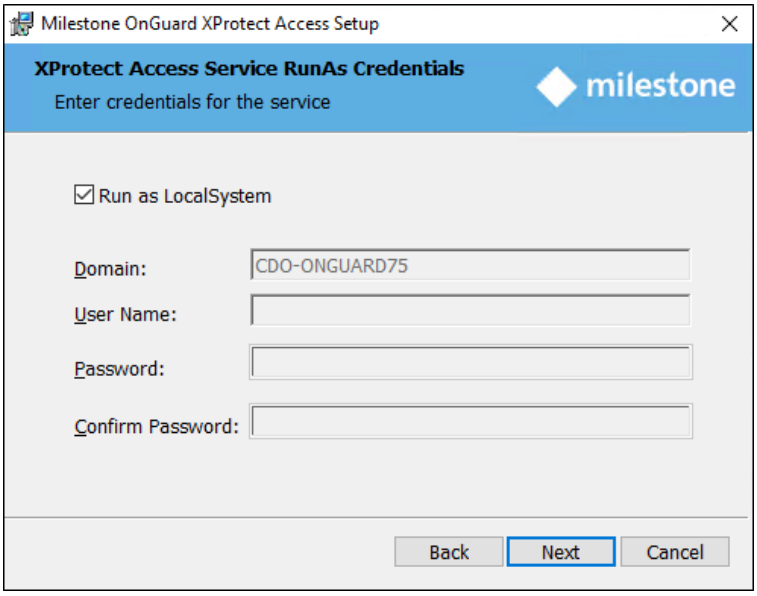
3. The context sensitive wizard offers to install the required components for the OnGuard XProtect Access Service. Click **Next** to continue.



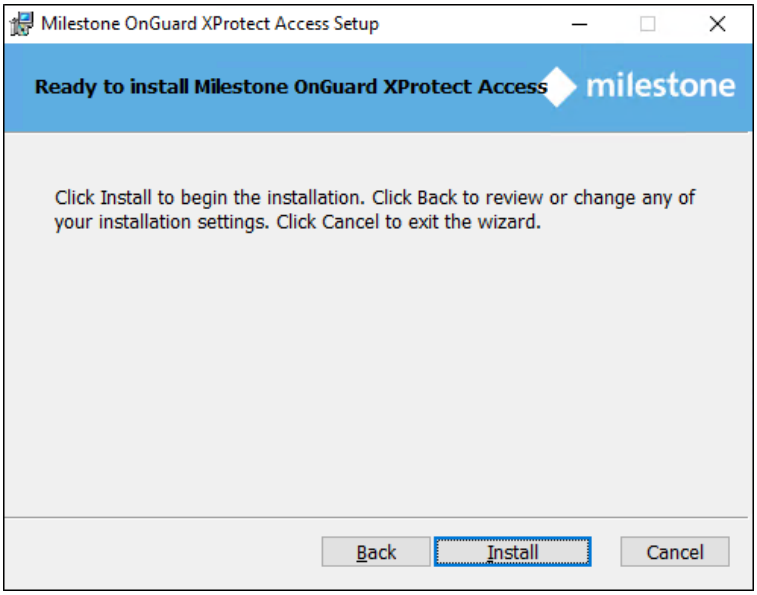
4. Optionally, expand the server icon menu to view installation options. The **Reset** button returns the wizard to all default options.



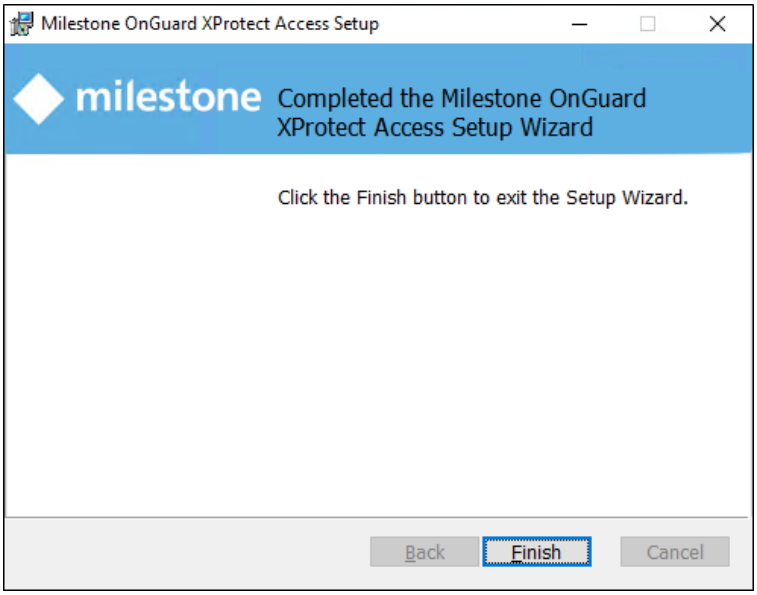
5. Choose the account used to run the OnGuard XProtect Access Service. The wizard selects the **LocalSystem** account by default. Click **Next**.



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

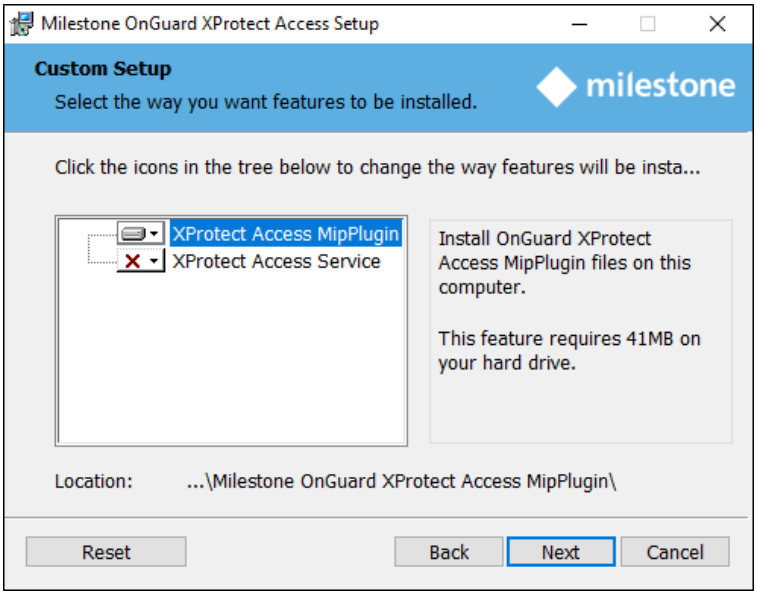


7. Installation is complete. Click **Finish**.

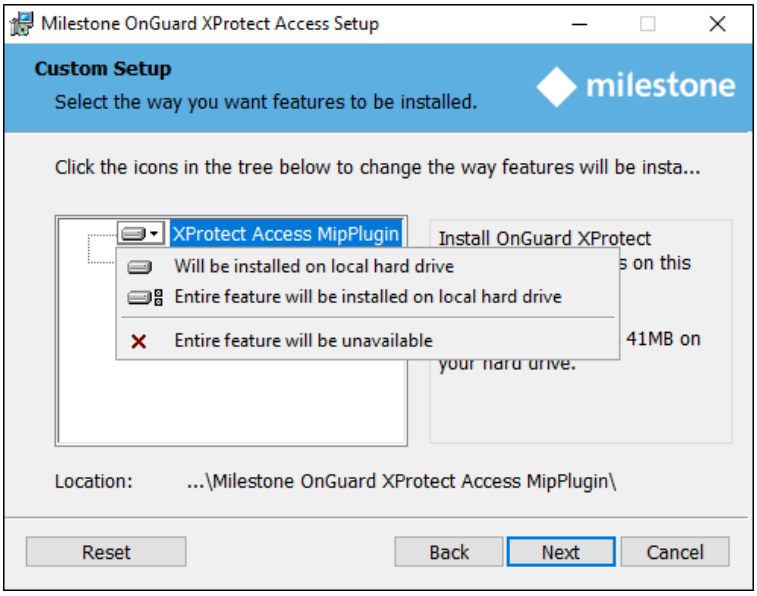


Step 2: Installing OnGuard XProtect Access MipPlugin

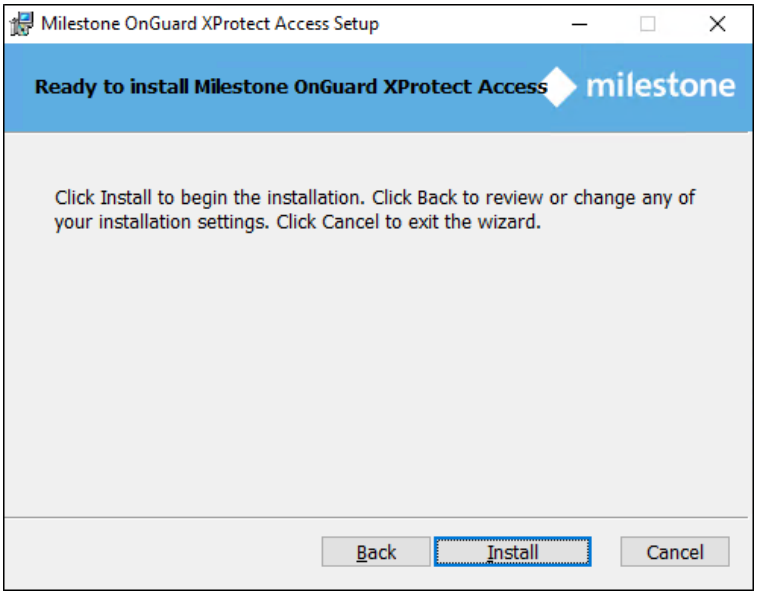
1. Place the XProtectAccess.OnGuard.msi file on the server hosting the XProtect Event Server (in a typical deployment, this is the Milestone XProtect Management Server), and double-click the file to begin.
2. After the opening step, the context sensitive installation wizard offers the option to install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



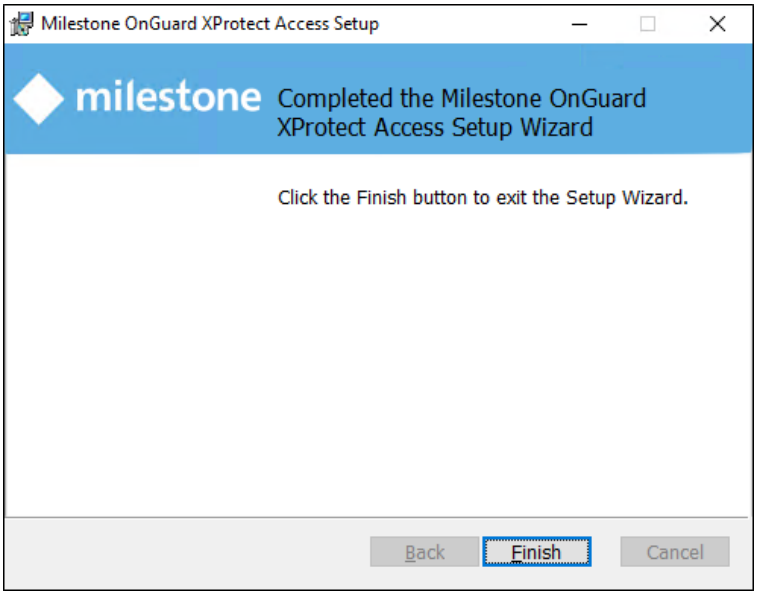
3. Optionally, expand the server icon menu to view installation options. The **Reset** button returns the wizard to all default options.



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**.



MIP Plugin 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:

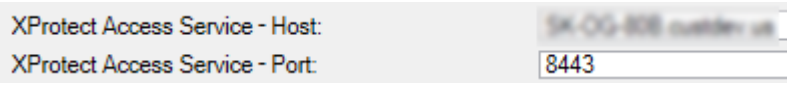
- Uninstall the ACM Server OnGuard Plugin
- Uninstall the ACM Server
- Install the OnGuard XProtect Access Service.

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 Service. These are **XProtect Access Server - Host:** and **XProtect Access Server - Port:**



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 96

Upgrading from DataConduIT

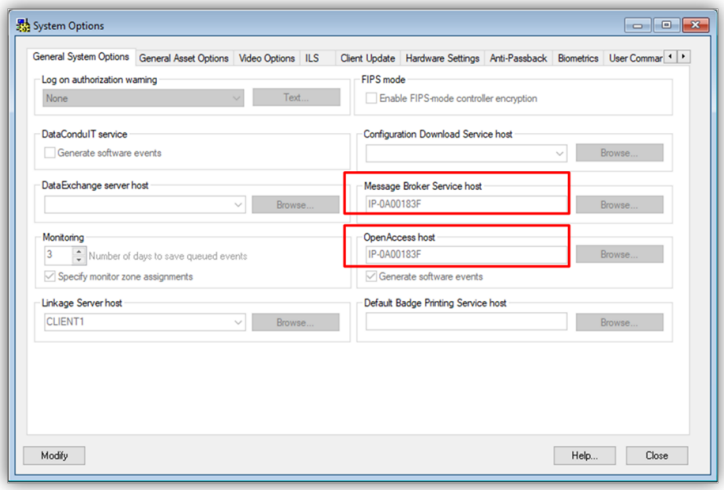
XProtect Access integrations using versions 3.5, 3.6, 4.0, or 4.1 with OpenAccess connection mode, may upgrade directly to version 4.2. Any XProtect Access integration using the DataConduIT connection mode can't upgrade directly to versions 4.0 or newer. DataConduIT is compatible with XProtect Access version 3.4 or older. All systems running XProtect Access versions 3.4 or older, and DataConduIT, need to 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:

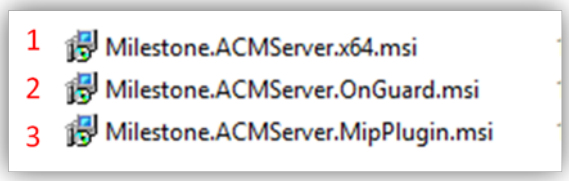


- On the host(s), confirm that the following services are all running:

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: OnGuardPlugin.
   - 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:



   - Refresh the configuration on the OnGuard XProtect Access instance in the Management Client.
   - Now, the active OnGuard XProtect Access instance is usingOpenAccess connection mode, and running version 3.6.
   - An upgrade directly to version 4.2 is supported.
5. Verify the prerequisites are in place to support version 4.2.
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 96

Uninstalling the integration

When uninstalling the integration software to revert to an older version, please refer to Integration version downgrades on page 94.

> 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 4.2 version of the plugin:

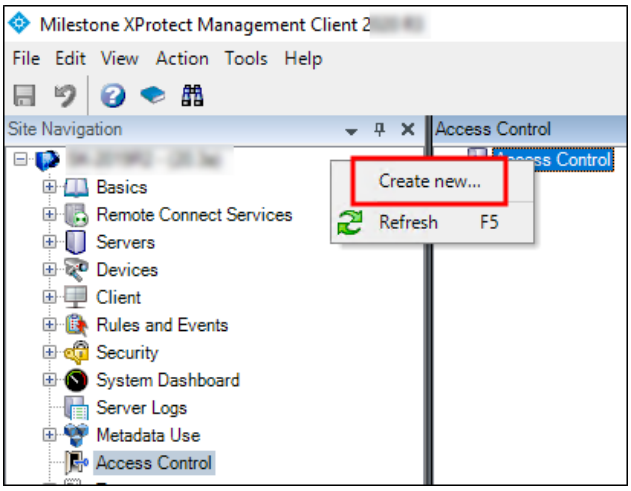
1. Go to the **Programs and Features** menu on the Milestone server.
2. Uninstall the **Milestone OnGuard XProtect Access** plug-in.
3. Go to the **Programs and Features** menu on the OnGuard server.
4. Uninstall the **Milestone OnGuard XProtect Access** service.

XProtect Management Client Configuration

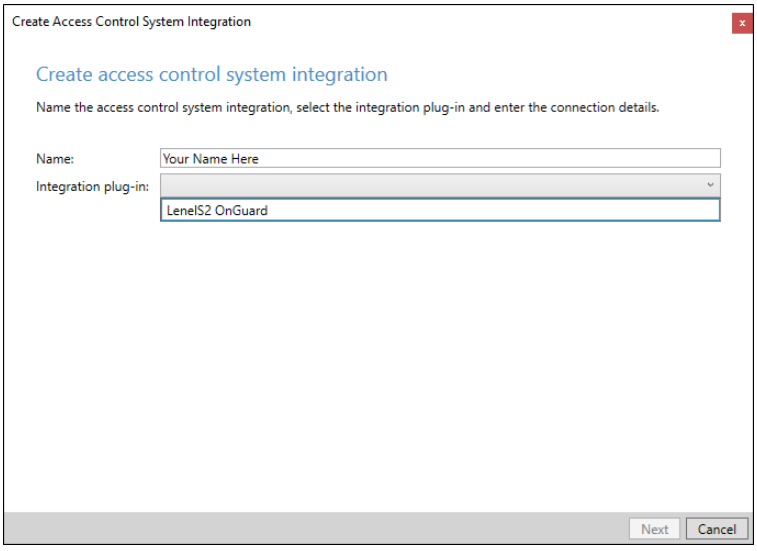
XProtect Access instance creation wizard

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

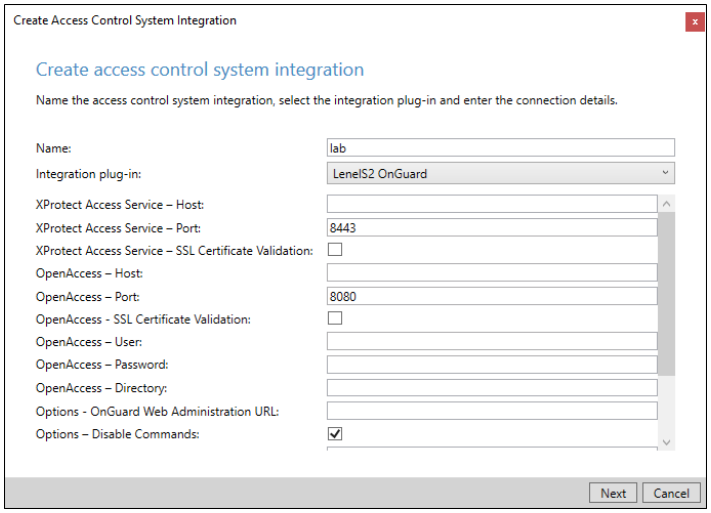
1. Right-click the **Access Control** root node and select **Create new...** to begin the wizard.



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



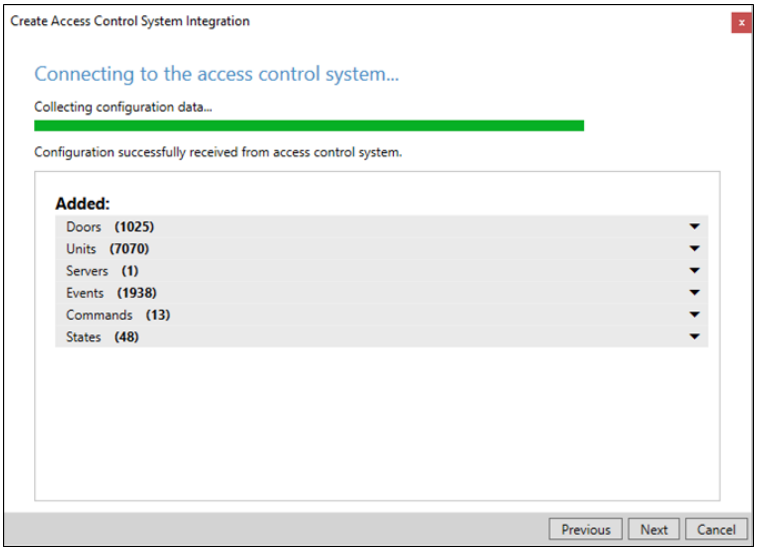
3. After naming and selecting the plug-in there are a set of required credentials, parameters, and options to complete. These fields define the connection to the OnGuard server. All properties for all supported versions of OnGuard are in the Management Client wizard.



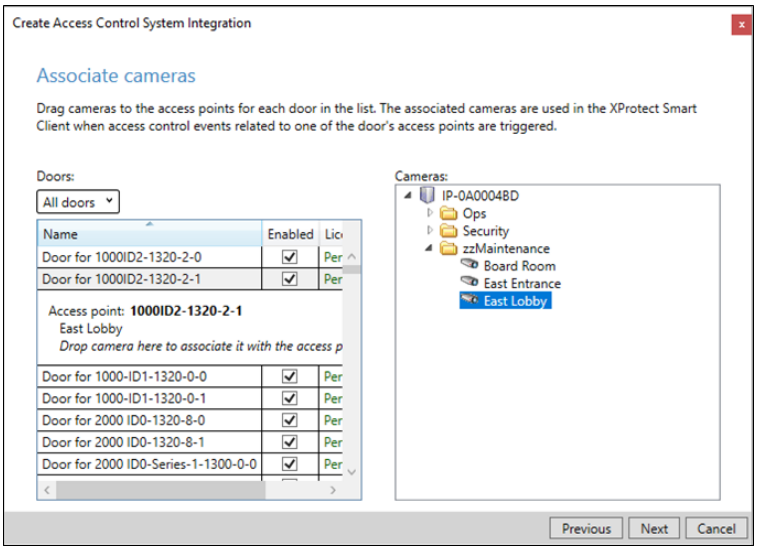
   - Below are the fields required to establish the connection. It's possible to populate any field at this step in the process, the fields listed are the minimum required.

Empty Field Names	Required Values
XProtect AccessService - Host:	Hostname of the OnGuard server or the Integration server.
XProtect AccessService - 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**.



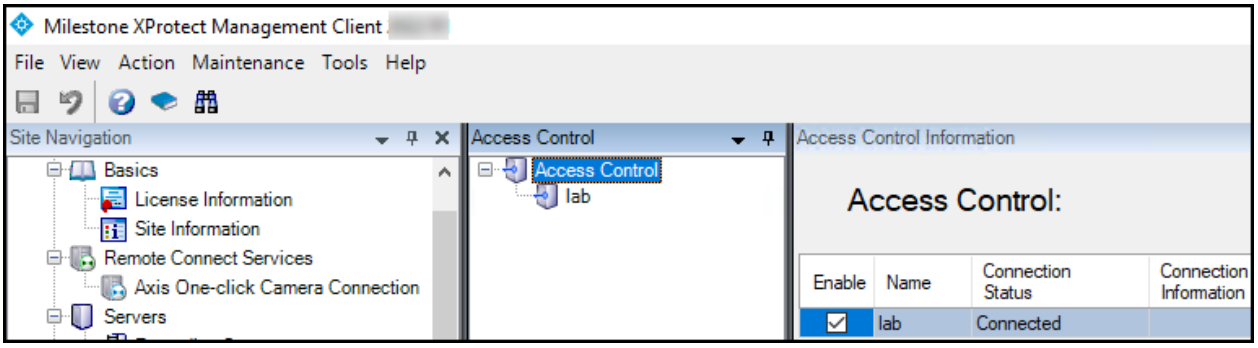
5. Associate doors with cameras. Select a camera and drag it to a door.



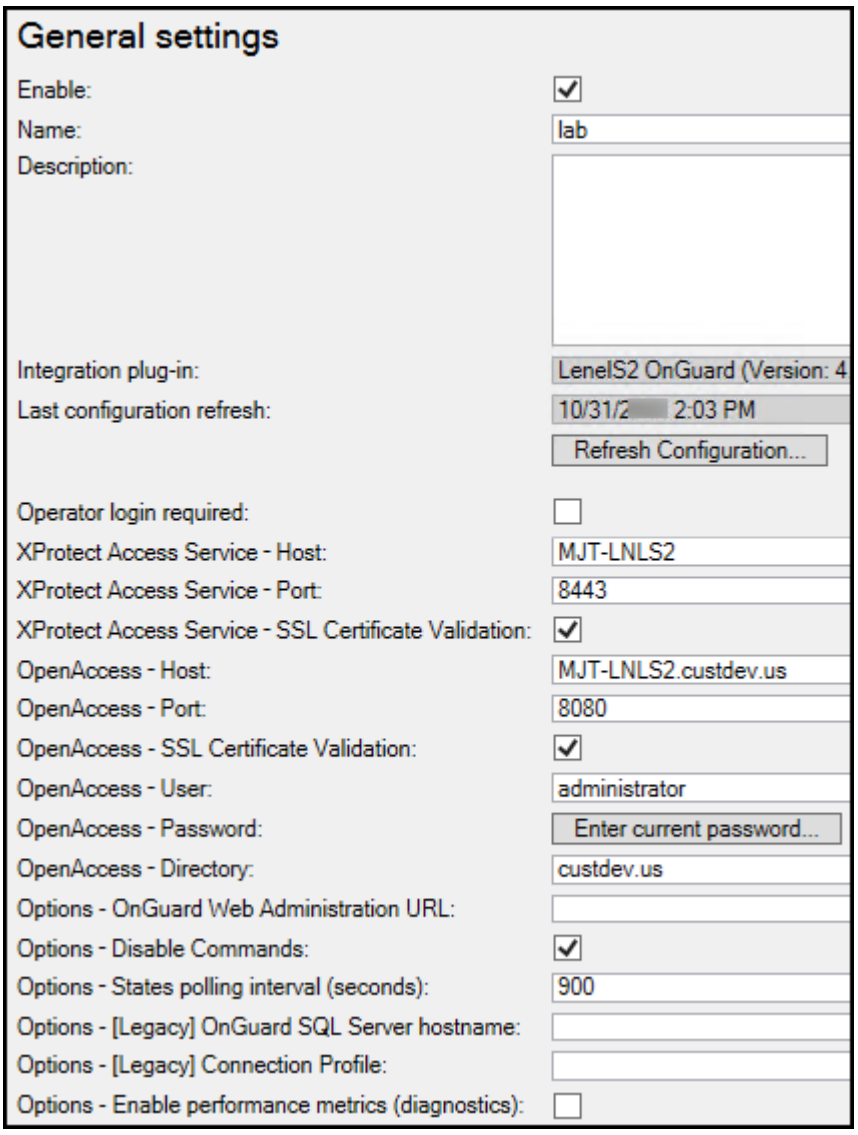
6. Click **Next** after association of doors and cameras.
7. The configuration is saved, and the wizard ends.

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.

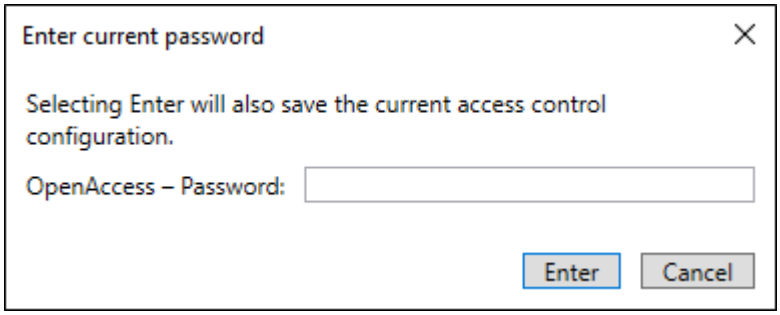


Select your OnGuard XProtect Access instance to view or edit the properties of the connection.



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. This field must use the Fully Qualified Domain Name of the server to support SSL authentication.
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 –	The password of an OnGuard user to log into the OnGuard OpenAccess web service. In

Password:	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. 
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:	The 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.

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.

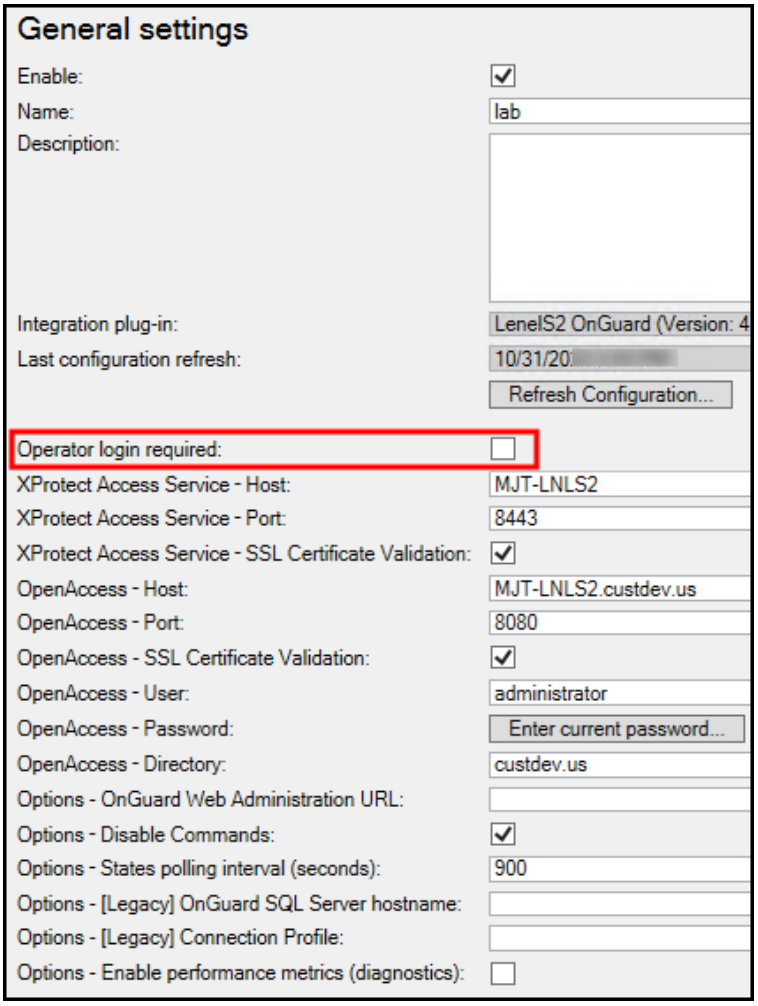
When a user logs into Smart Client, the personalized login feature presents a second login procedure that authenticates with the integrated OnGuard system. When the user presents valid OnGuard credentials, the Smart Client's XProtect Access features are narrowed to access control hardware, events, and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



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.

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:

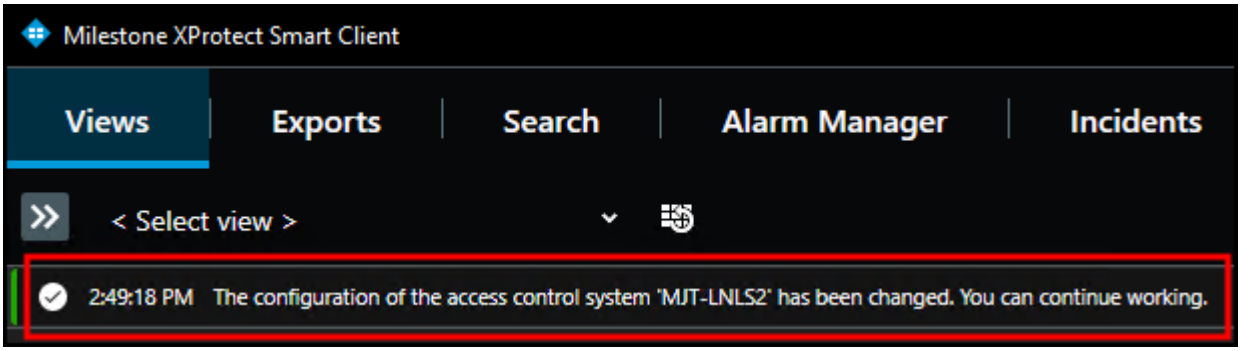
- Alarms related to hardware the user has privileges to view

- 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.

After the global configuration updates, all open Smart Clients using a personalized configuration display the following info message.



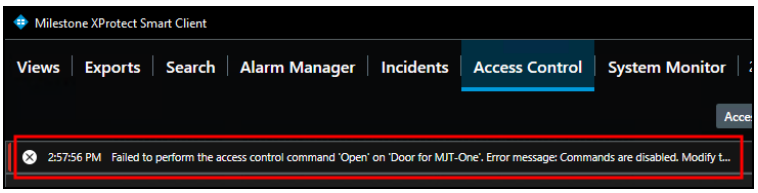
Log out of the Smart Client and log back in using the personalized configuration to load the updated configuration.

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 'COMAND**' on '**DEVICE**'. Error Message: Commands are disabled. Modify the plugin configuration in the XProtect Management Client to enable commands.**



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

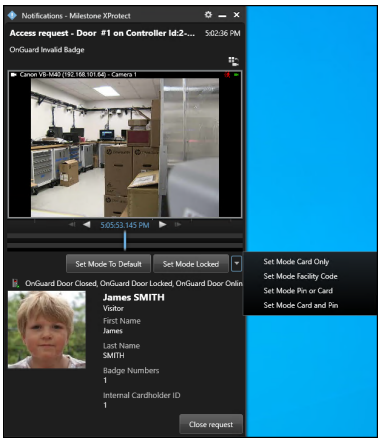
1. The XProtect rules system can trigger commands.
2. Access request notifications can include commands.
3. Any location in the Smart Client where doors are visualized, such as the access monitor or the access control workspace, can contain command buttons.
4. The map interface within the XProtect Smart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



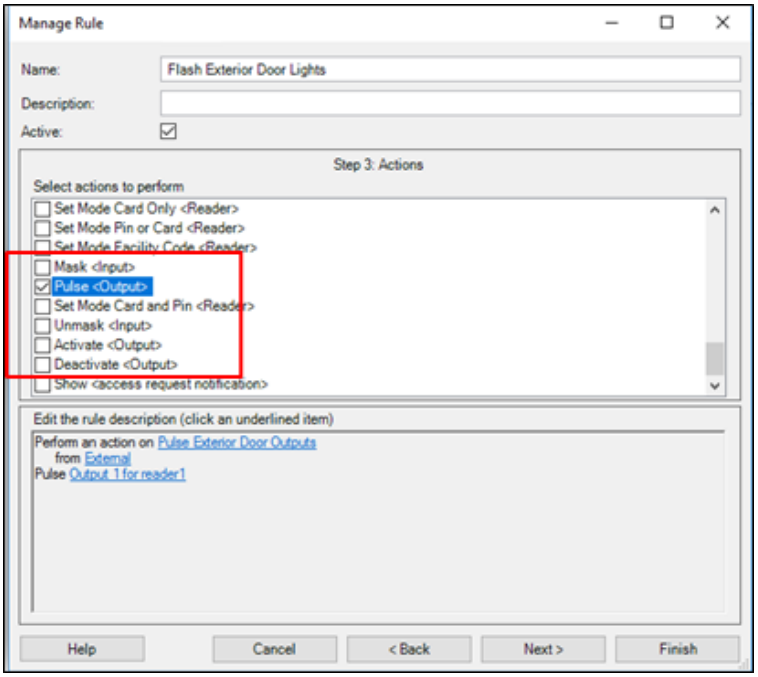
> **Set Mode** commands for readers change the authentication mode the reader responds to. For example: a rule can switch readers into unlocked mode during business hours.

Reader Inputs:

- Mask
- Unmask

Reader Outputs:

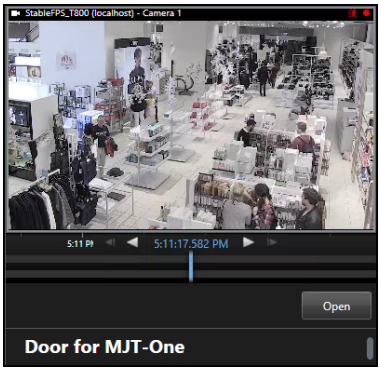
- Activate
- Deactivate
- Pulse



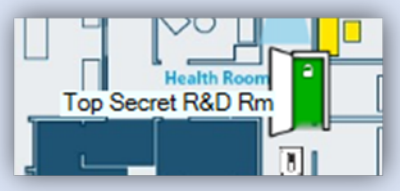
> Reader inputs have a state of masked or unmasked. A masked input doesn't report or save status in the OnGuardsystem. The masked input also has a "mask" icon attached to its own icon on the Smart Client map. Unmask enables status of that input to be reported and saved within OnGuard, and removes the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

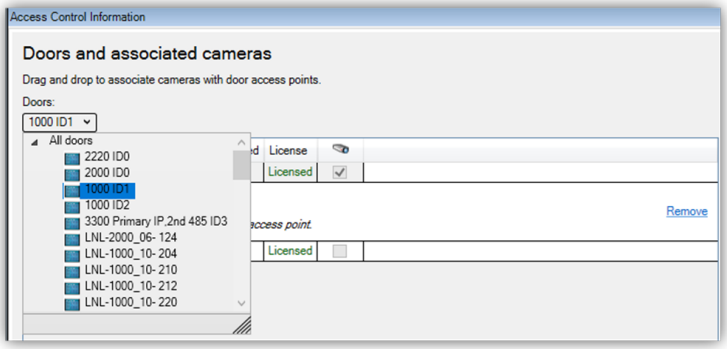


Administrative Configuration

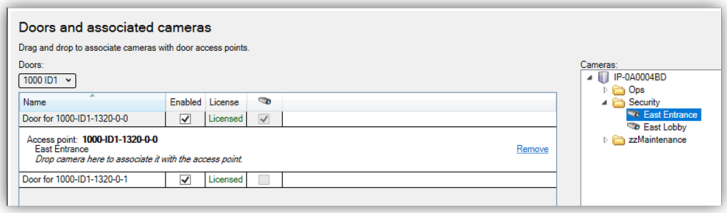
Door & camera association

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.



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.

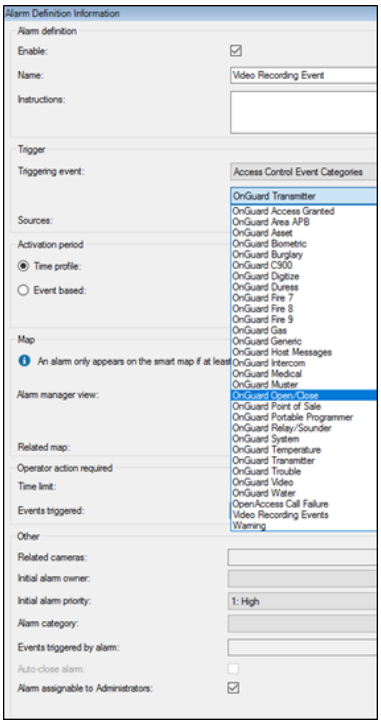
Categorize events

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.

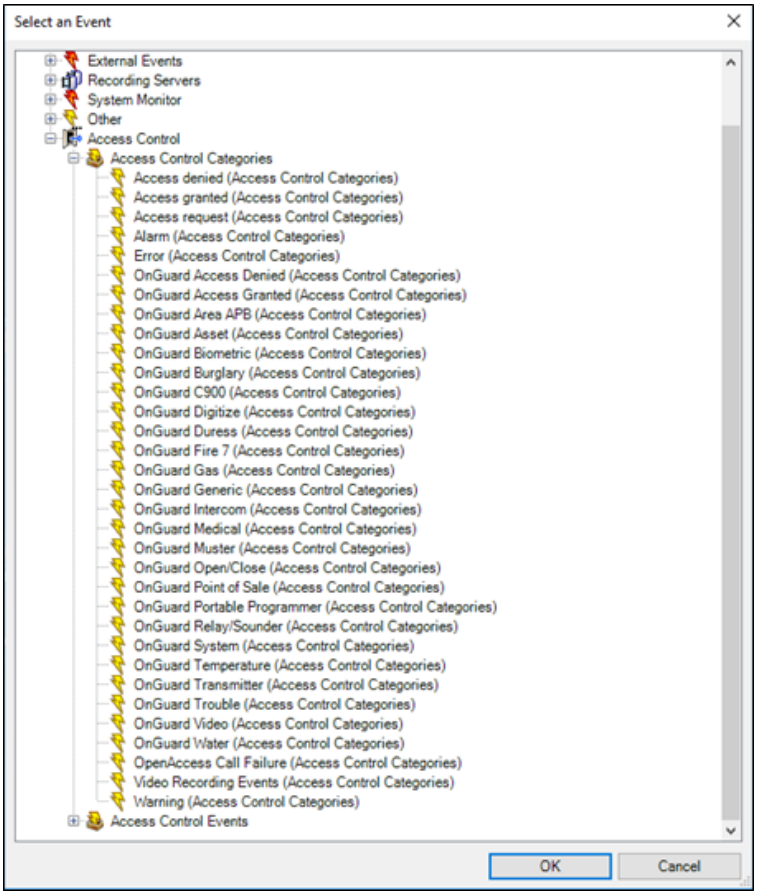
Categorize events to generate XProtect alarms or rule-based actions triggered by any OnGuard event from the chosen category. For example, the integration can start recording video based on any number of unique OnGuard hardware events: “Door Forced,” “Denied, Badge Not in Panel,” and “Access Denied Unauthorized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



- 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:

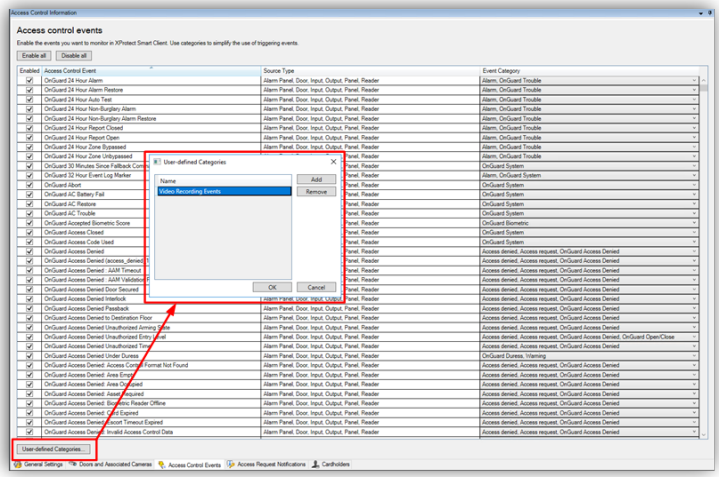
- OnGuard Access Denied
- OnGuard Access Granted
- OnGuard Area ABP
- OnGuard Asset
- OnGuard Biometric
- OnGuard Burglary
- OnGuard C900
- OnGuard Digitize
- OnGuard Duress
- OnGuard Fire 7
- OnGuard Fire 8
- OnGuard Fire 9
- OnGuard Gas
- OnGuard Generic
- OnGuard Host Messages
- OnGuard Intercom
- 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:

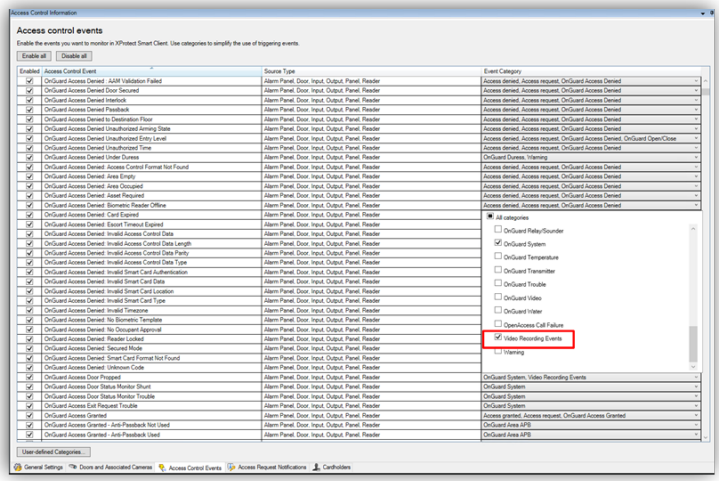
- User Defined Category...

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.



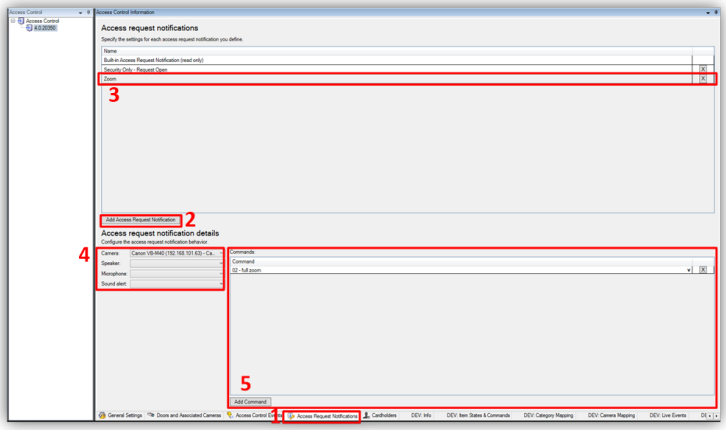
2. Click **Add**, name the category, and press **OK**. The user-defined category appears as an option in the **Event Category** list.



Access request notifications

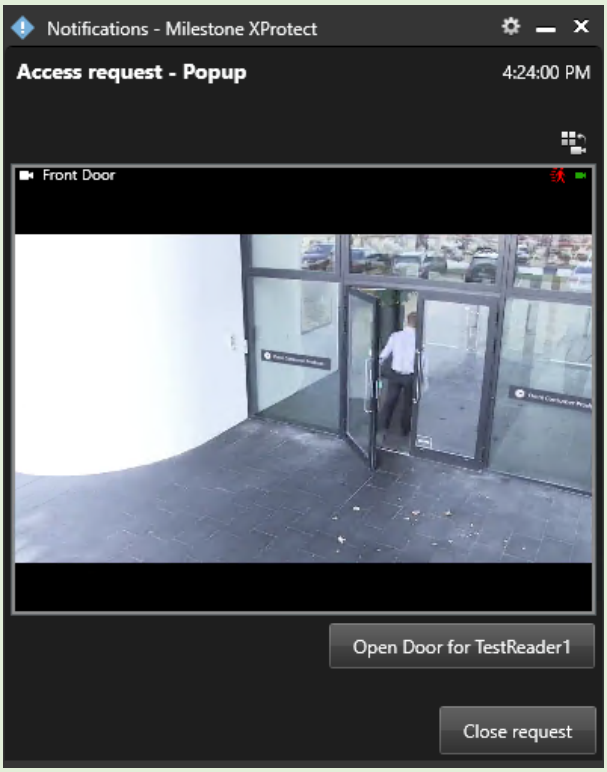
Access request notifications are pop-up notifications which appear in front of all other desktop applications for all users logged into the Smart Client with privileges to view XProtect Access features and devices. The XProtect Access integration includes a built-in access request notification. Use the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



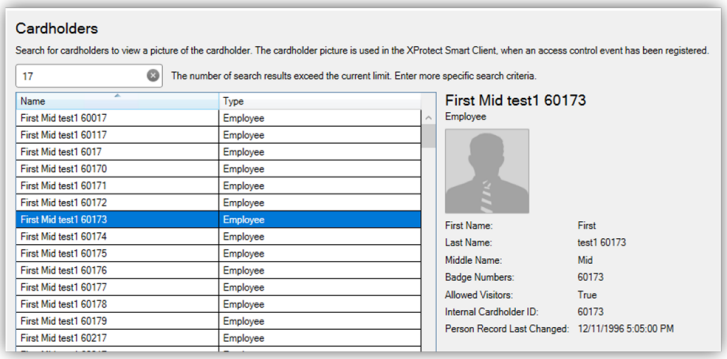
When the notification pops up on the desktop, a sound plays if you choose to include an audible notification. The built-in access request notification doesn't include a sound.

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:



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 100

Client profiles & Roles explained

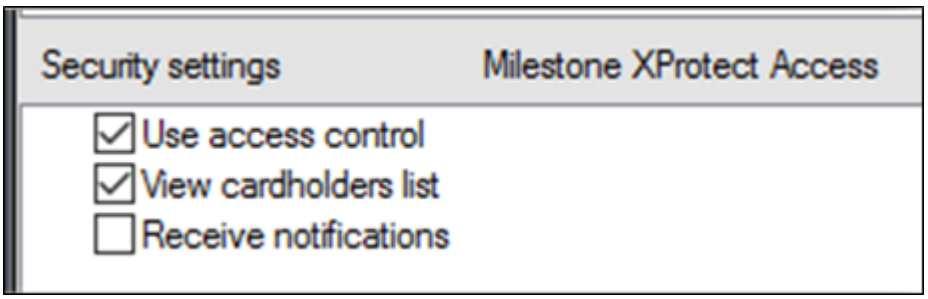
Smart Client profiles and user roles in XProtect let administrators manage the features available in the XProtect Smart Client.

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.

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.

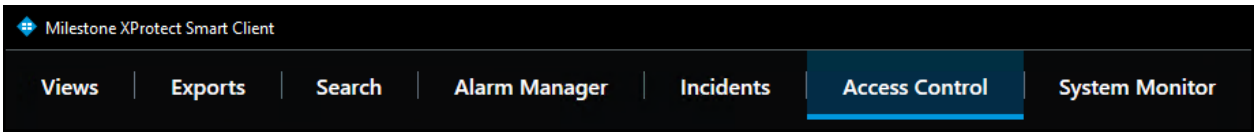


> The **Receive notifications** setting only applies to the XProtect mobile client.

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.

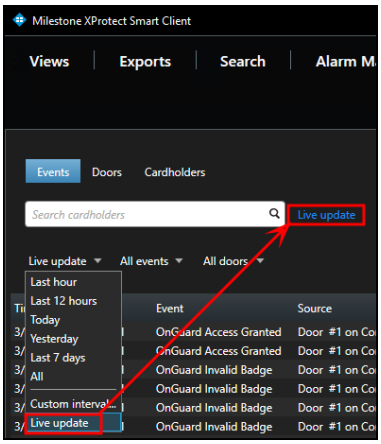


Use this workspace to search and filter the **Events**, **Doors**, and **Cardholders** categories. Select **Events**, **Doors**, or **Cardholders** to work with the list of events related to that category.

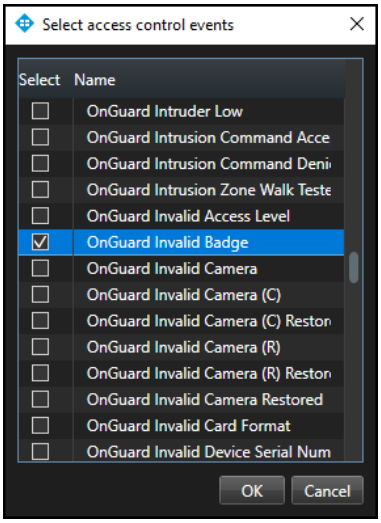
Access control workspace events

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.

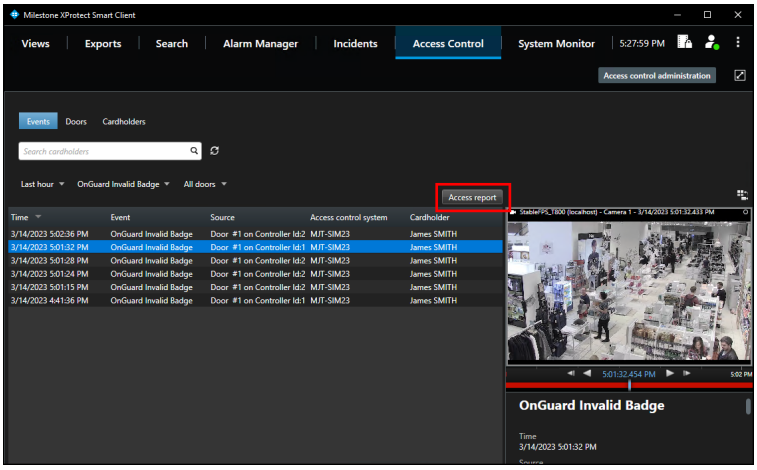
1. Choose the **Live update** time range to view a real-time display of access control events.



2. Filter for specific events including custom events and all integrated OnGuard events.
3. 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.



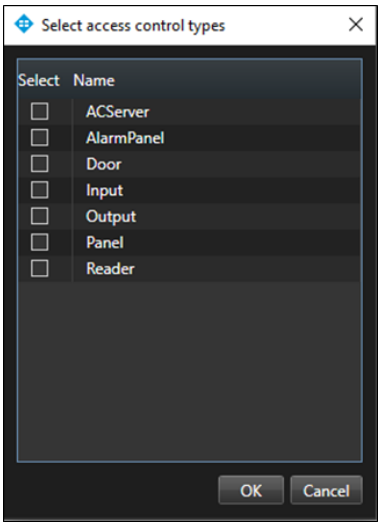
4. Filter for specific hardware devices.
5. Click the **Access report** button to create a PDF file of the events in the current list.



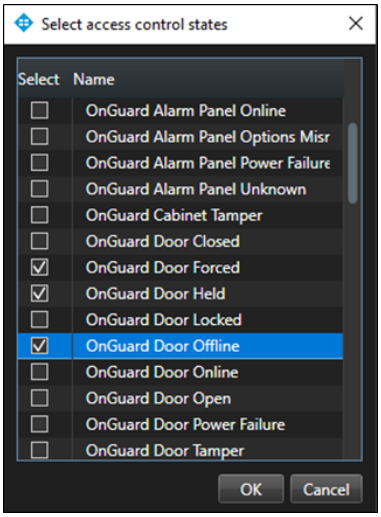
- In the **Access report window**: name the report, choose a destination to save the report, include comments, and select the option to include snapshots.

Access control workspace doors

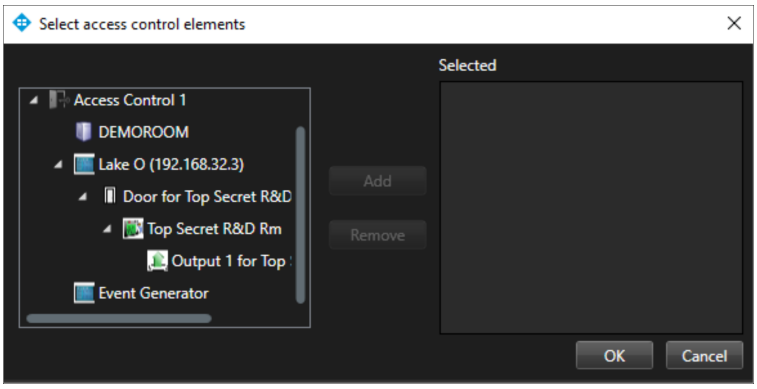
1. Open the **Door** list and select the access control hardware to display.
2. Choose the **Access control type...**, option to open the **Select access control types** window.
    - **Door** is the default option for this list. Use this menu to select servers, panels, and any access control hardware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



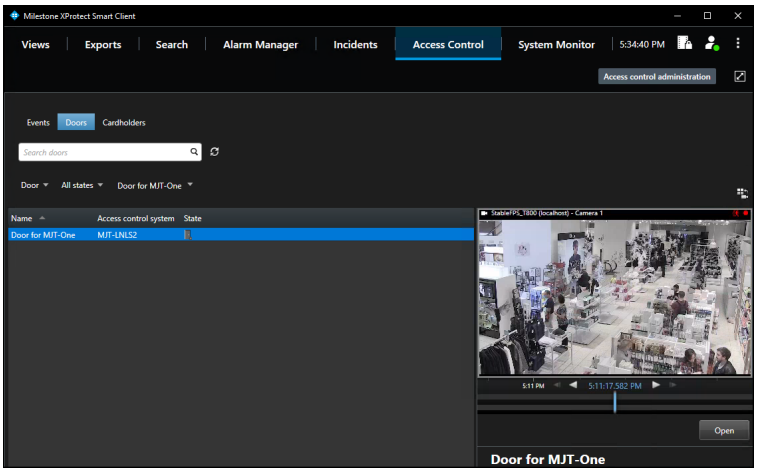
3. Open the **All** states list to filter hardware by status.
4. Choose the **Access control state...**, option to open the **Select access control states** window and select from all available OnGuard hardware states.



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.



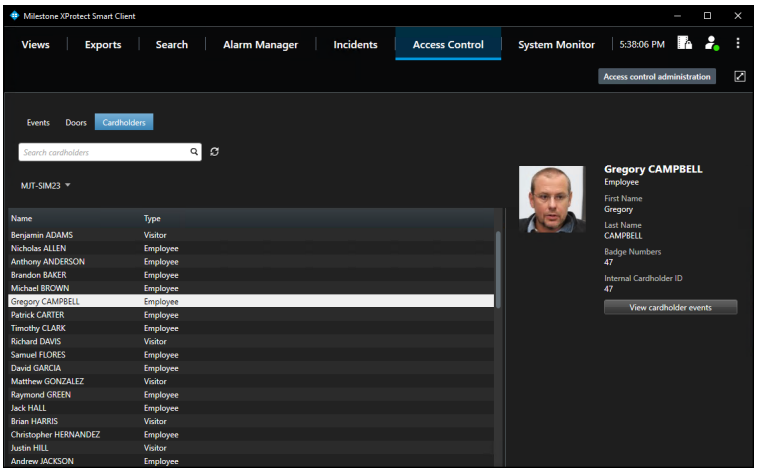
7. Select a Door in the list to see video from associated cameras, view door status information, and command buttons available for that door.



Access control workspace cardholders

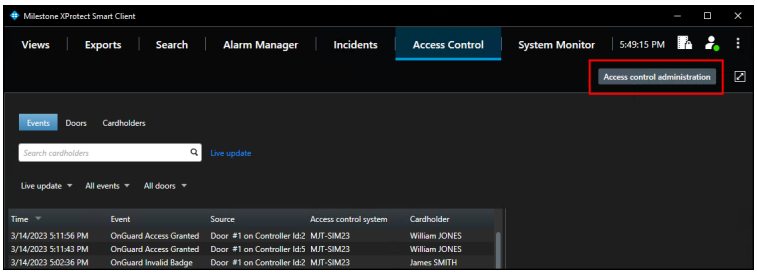
By default, this list displays all cardholders in the system.

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.

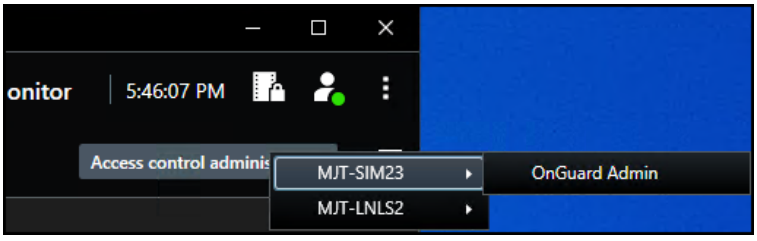


OnGuard web admin link

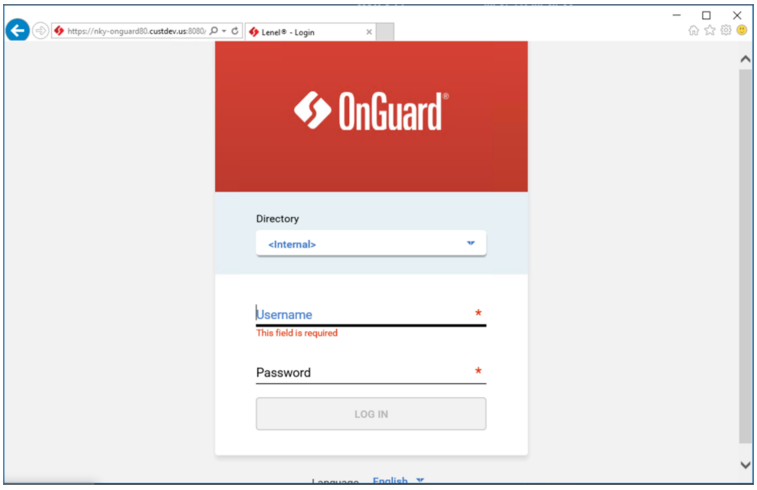
If a web portal link was added to the **General Settings** of the XProtect Access OnGuard integration within the XProtect Management Client, then the **Access control administration** link in the **Access Control** workspace of the XProtect Smart Client is active.



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.

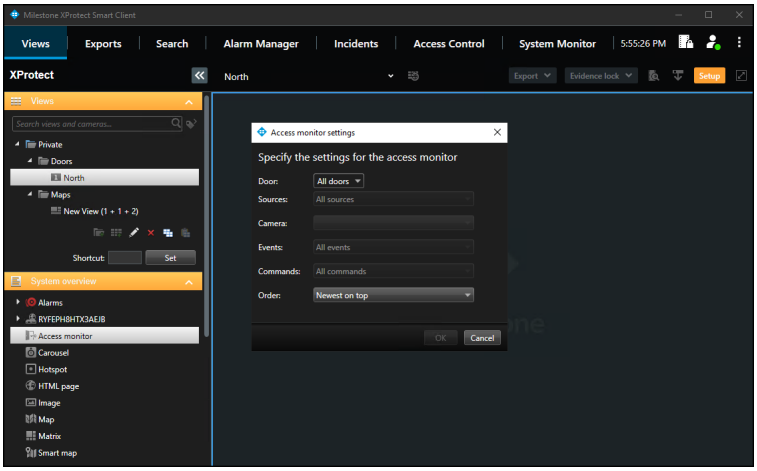


> If multiple XProtect Access systems integrate with the same XProtect VMS it's possible to have more than one button in the Smart Client after selecting the **Access control administration** link.

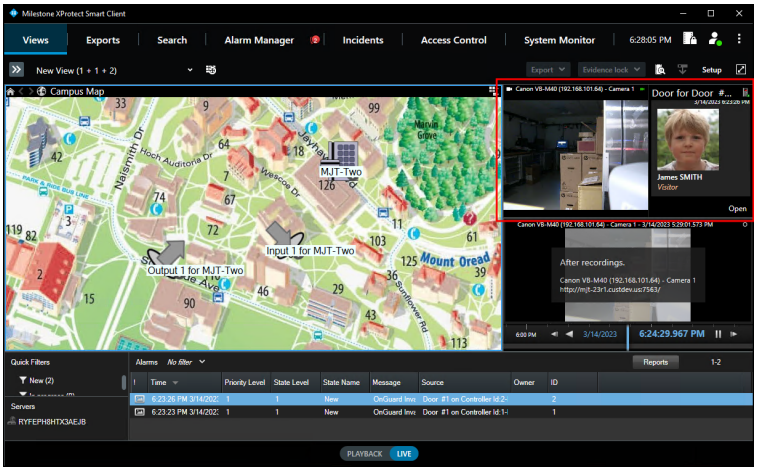
Access Monitor

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.

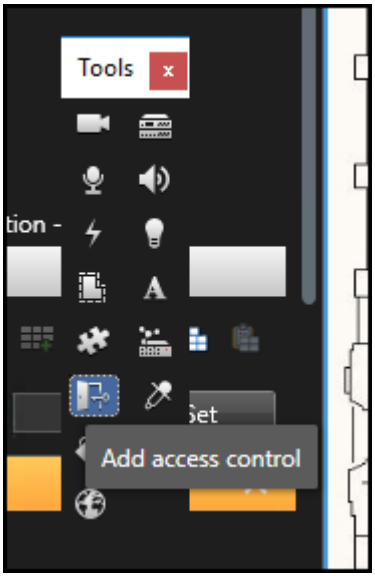


> After choosing a door the access monitor options change, based upon the available cameras, events, and commands. The access monitor view item can go into any available view pane and works in a view alongside all available view items.

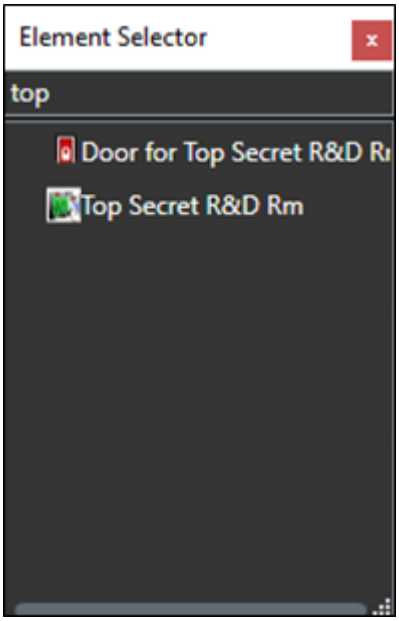
Maps

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.

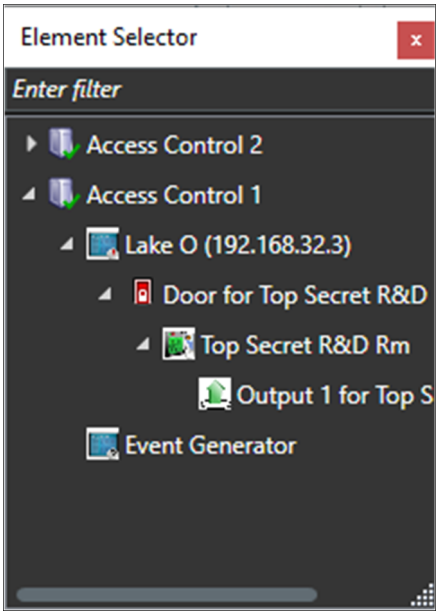
1. With the Smart Client in setup mode, a **Tools** window appears in the view pane.
2. From this window, select the **Add Access Control** icon:



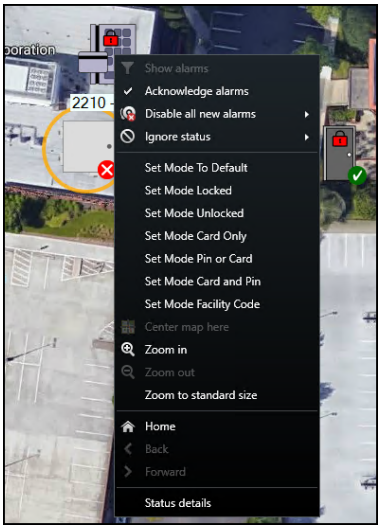
3. The **Element Selector** window appears.



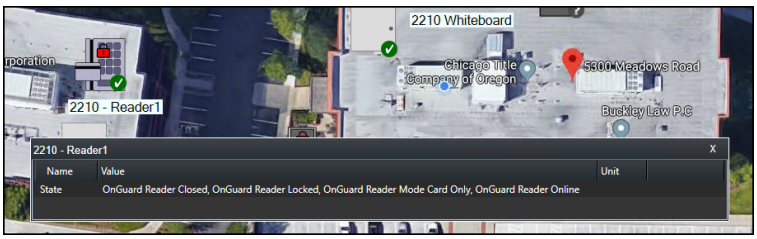
4. Type the name of a hardware device into the filter to find a device or expand the servers and panels to find all available hardware icons in the system.



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.



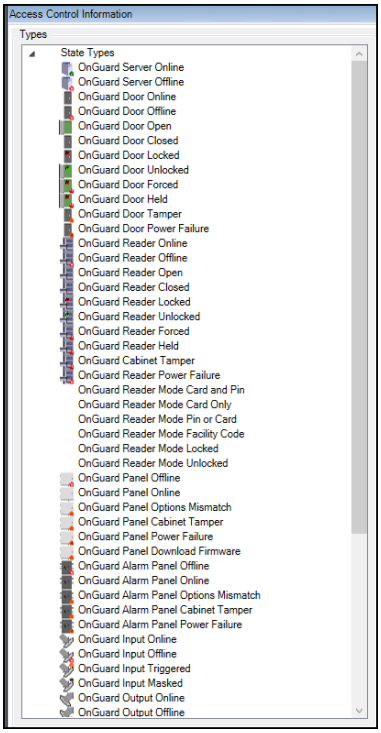
7. Right click the device icon and select **Status Details** from the shortcut menu to view more information. The pop-up window displays the device status information in the **Value** field.



> In version 4.2 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 75 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.

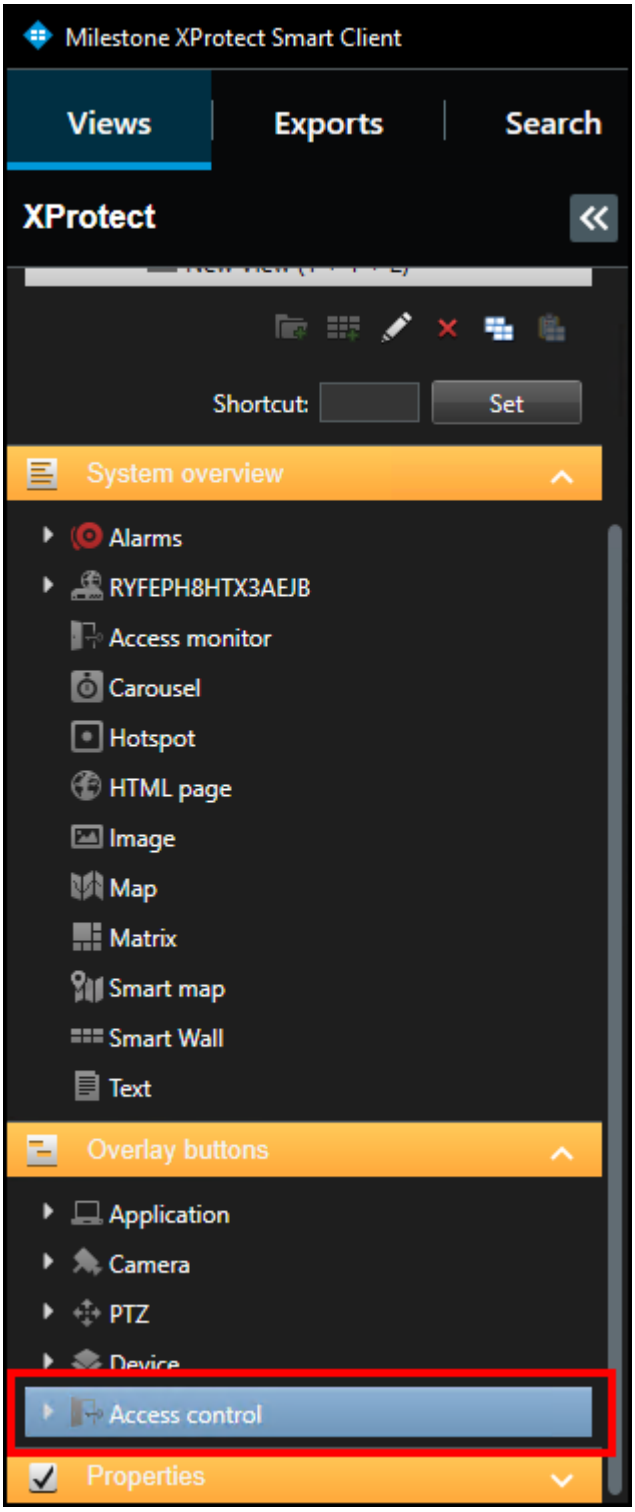
If you want to verify the list of available device icons and statuses in your XProtect Access system follow this process:

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.

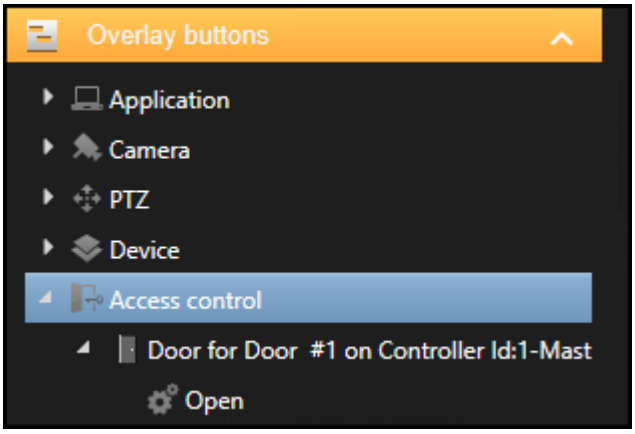
Overlay buttons & commands

Overlay buttons are software buttons capable of being added to video panes in the Smart Client. Anything triggered by a command, can be triggered manually by an overlay button.

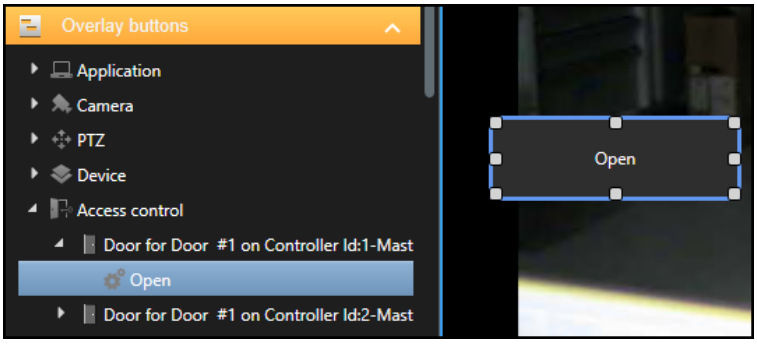
1. When the Smart Client is in setup mode, there is an **Overlay Buttons** panel on the left side of the client.
2. Select the **Access Control** icon.



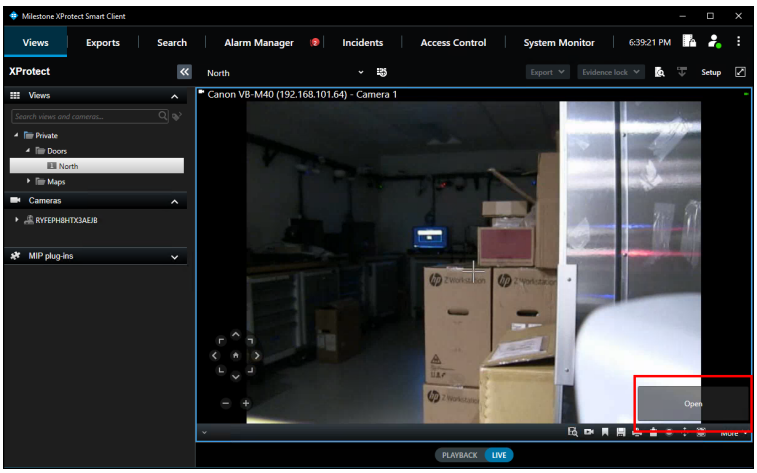
3. Expand the **Access Control** icon to find all the doors and readers, panels, and the connected inputs and outputs in the system.



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

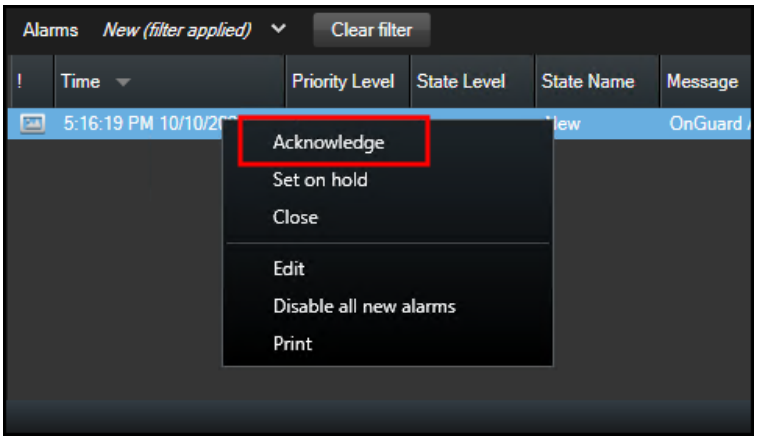
Alarm status between XProtect and OnGuard is shared. When alarms change state in XProtect that state is shared with OnGuard. Alarm status is shared in the opposite direction as well – from OnGuard to XProtect.

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.

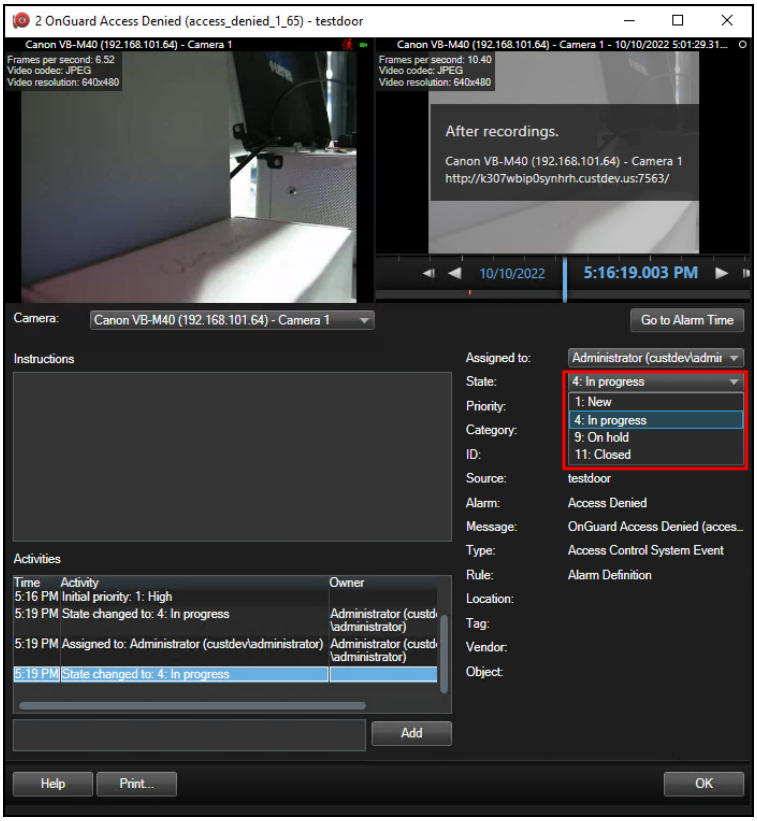
OnGuard Alarm Status	XProtect Alarm Status
• NEW	• NEW
• IN PROGRESS	• IN PROGRESS
	• ON HOLD
• ACKNOWLEDGED	• CLOSED

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

- Acknowledging an alarm in XProtectchanges the alarm state to in progress both in XProtect and in OnGuard.



- In XProtect alarms can change from closed to other states by 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.



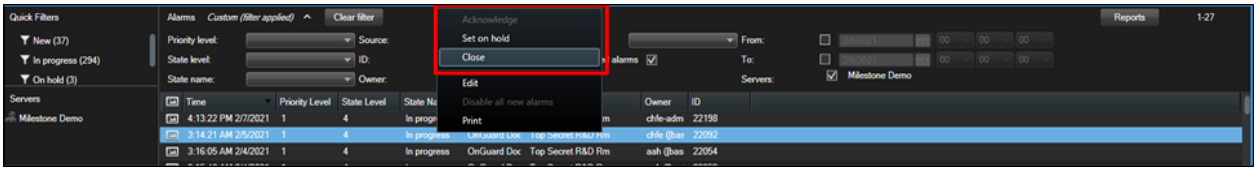
- Alarms in XProtect can return to the new state from any other state, if the alarm is edited. This isn't allowed in OnGuard. If a user changes an alarm state to new in XProtect from any other state, that change is not made in OnGuard.
- Although it's possible in XProtect to change a new alarm directly to on hold, this change does not take place in OnGuard integrated systems, the activity is not even logged in OnGuard. If an alarm is moved to on hold in XProtect and it should be moved back to in progress, edit the status in XProtect and it will be reflected in OnGuard.
- 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 82.

Acknowledge alarms in XProtect

In XProtectoperators 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.



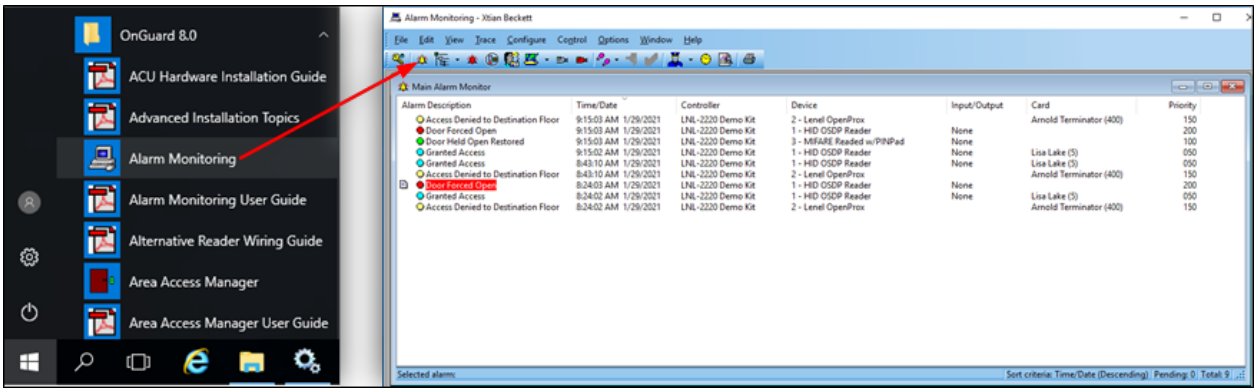
3. Alarm status synchronizes as much as possible between XProtect and OnGuard.

> Learn more about how the integration handles alarm acknowledgment here: Alarm acknowledgment explained on page 78.

Checking alarm acknowledgment status in OnGuard

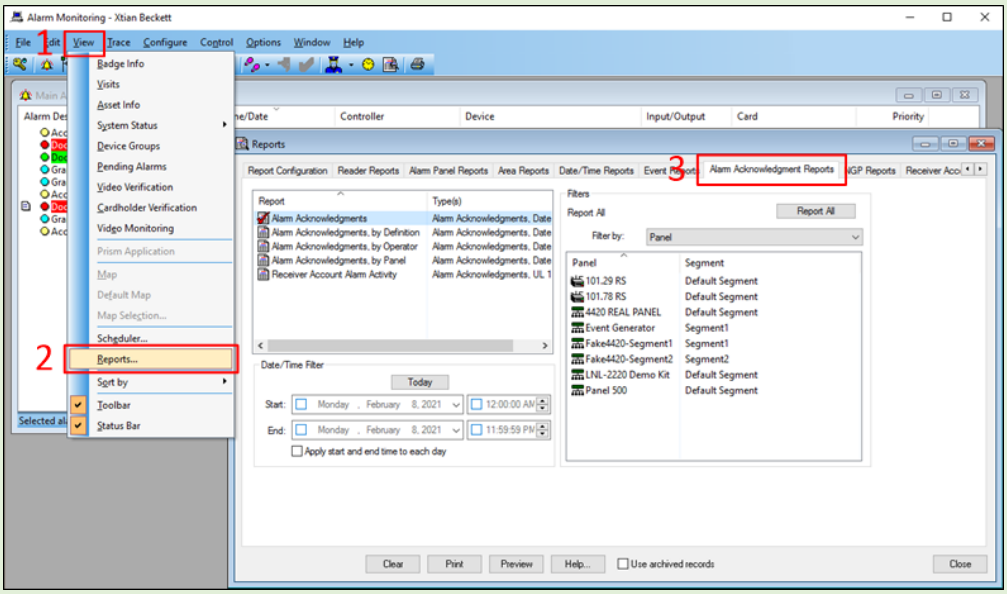
When alarms are acknowledged in OnGuard, the alarm is closed, and the associated alarm is also closed in XProtect. If the alarm is acknowledged within XProtect it changes state to in progress both in XProtectand in OnGuard. The status of the alarm in OnGuard changes to reflect the status in XProtect as much as possible. Learn more about how the integration handles alarm acknowledgment here: Alarm acknowledgment explained on page 78.

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.
3. In the **Alarm Acknowledgement Reports** tab choose a time range and export a report of all acknowledged alarms in the OnGuard system.



Changing alarm acknowledgment behavior

Edit the **PluginSettings.json** file to change the behavior of the alarm acknowledgment between OnGuardand 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 OnGuardwas 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.

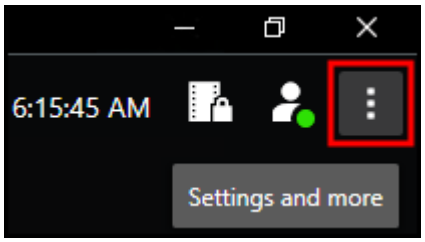
Possible alarm states in XProtect and OnGuard weren't the same. In XProtect alarms could be new, acknowledged, set on hold, or closed. In OnGuard alarms were either active or acknowledged. For the XProtect AccessOnGuard integration, acknowledged alarms in OnGuard were the same as closed alarms in XProtect.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

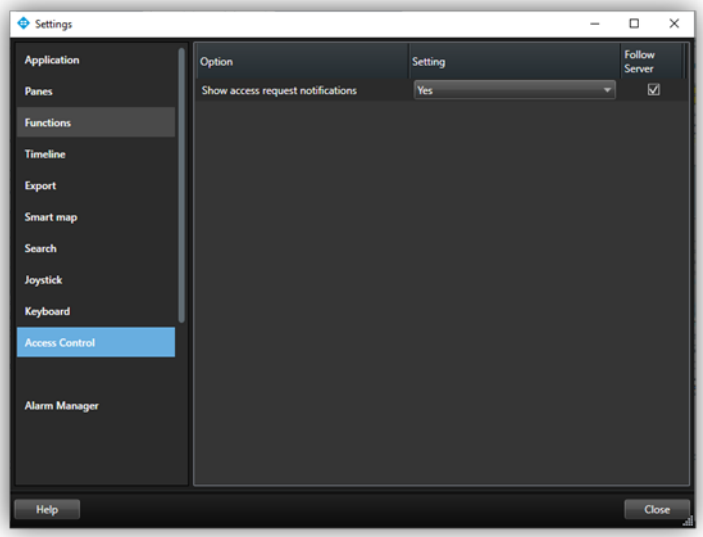
Smart Client access control options

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.

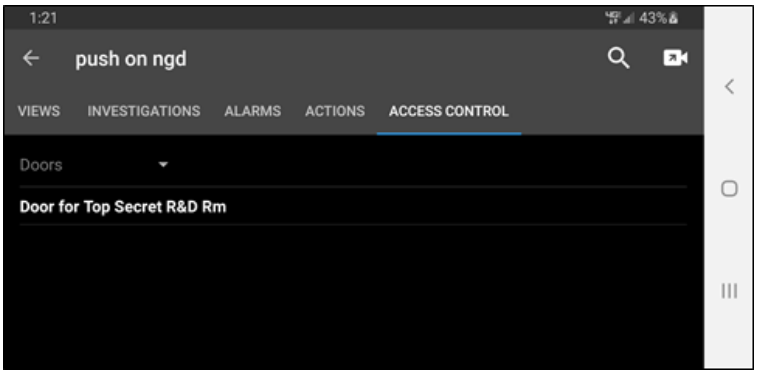
Mobile Client

XProtect Mobile application

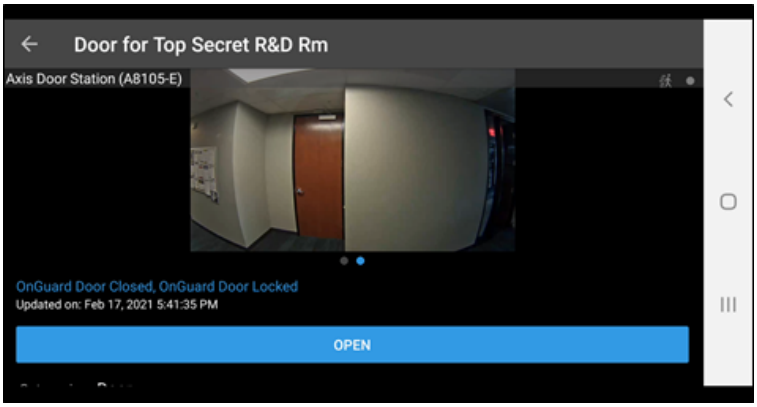
XProtect Mobile is a mobile device app that connects to your VMS system. The XProtect Access OnGuard integration adds capability to XProtect Mobile. Using XProtect Mobile it's possible to receive a push notification from the access control system, view live video related to the notification, and open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

Using the access control tab in XProtect Mobile

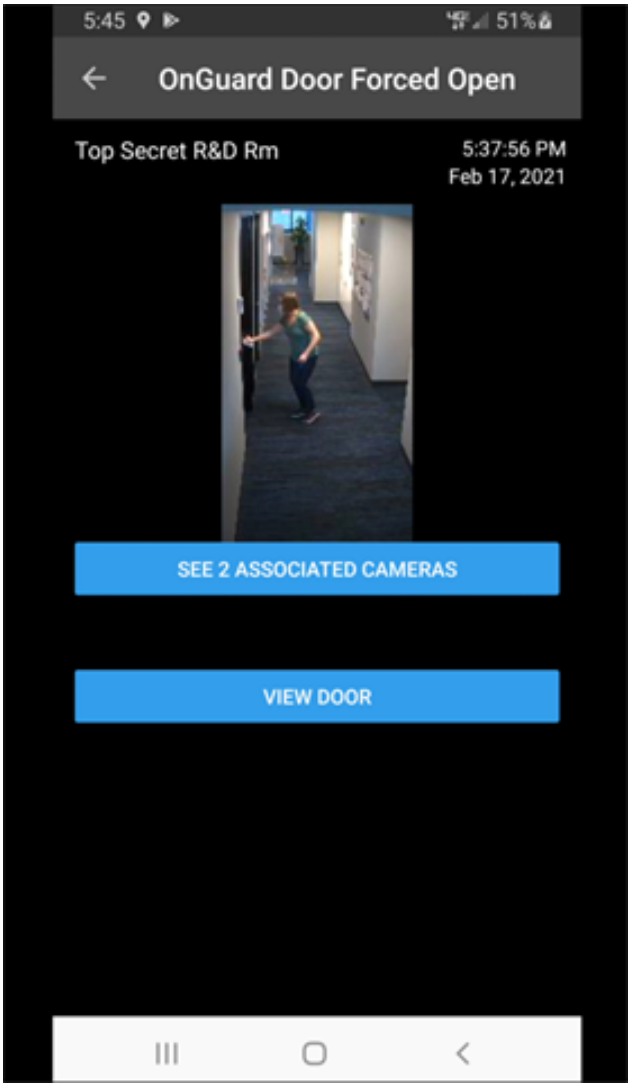
1. Log into the VMS with XProtect Mobile. By default the **Views** tab appears.
2. Select the **Access Control** tab. The **Access Control** tab shows the list of doors available.



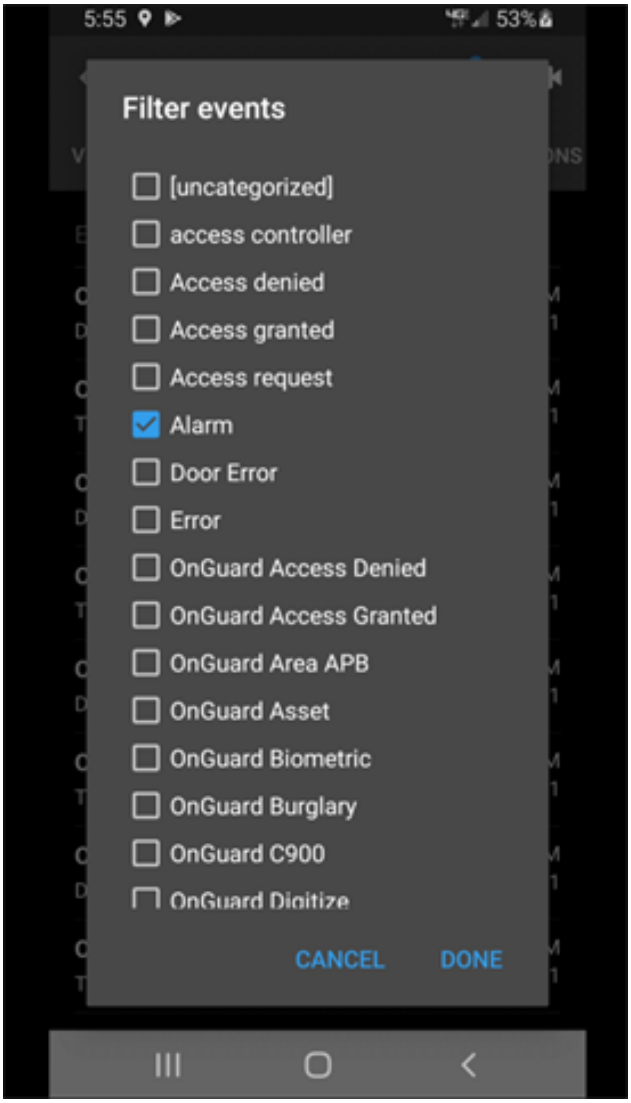
3. Filter for specific doors or select a door to view cameras associated to that door or interact with commands available for the selected door.



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.



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

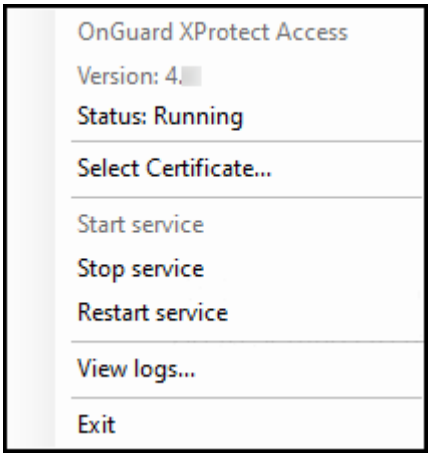


Access requests are visible if the Smart Client profile assigned to the role of the current user can view access requests.

Service Tray Icon

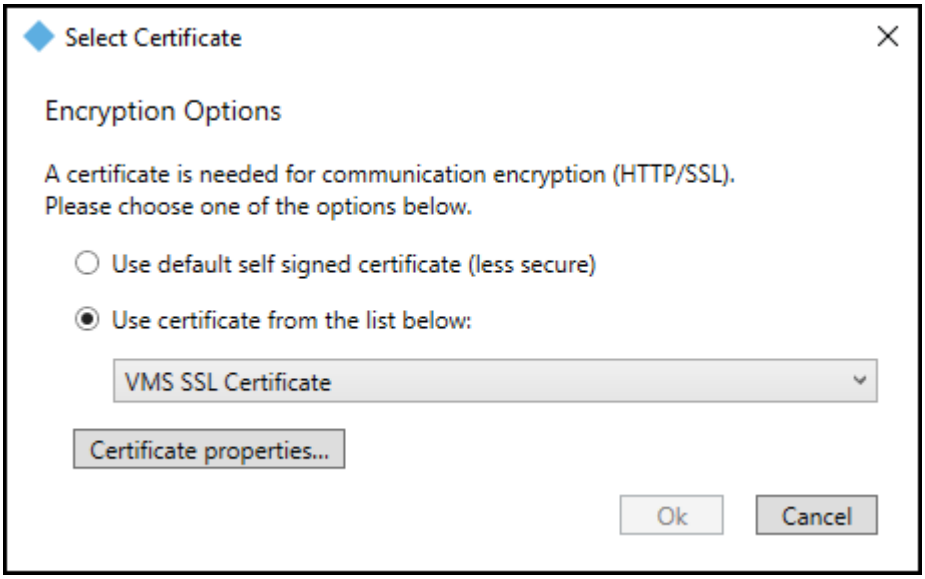
Service tray icon (explained)

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.



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 Serviceand choose the **Select Certificate...**option.
2. This opens the **Select Certificate** dialog. Initially, the **Use default self signed certificate** option is selected.



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.

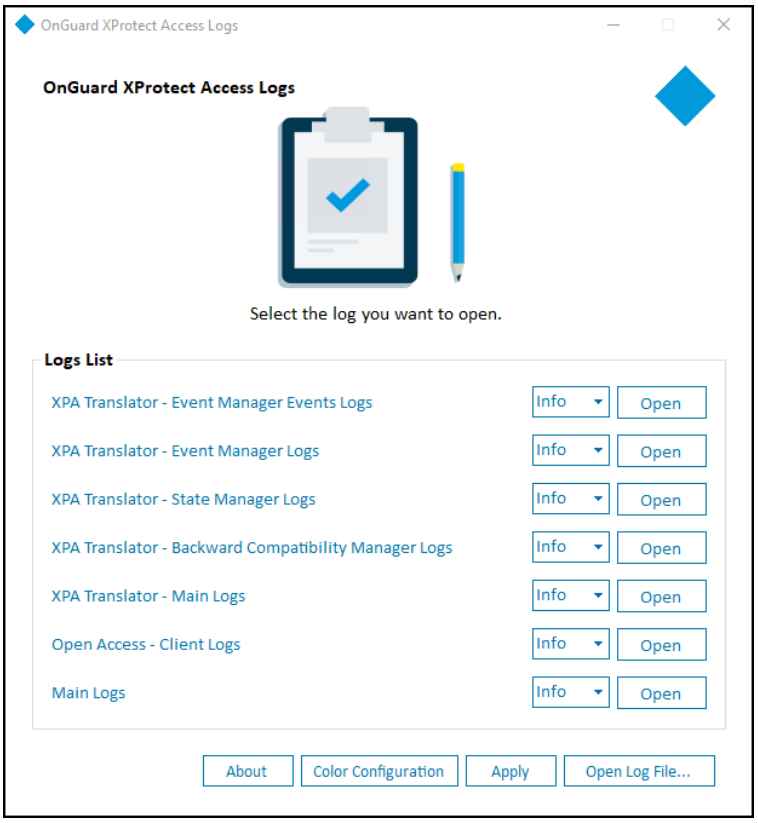
> If there are no certificates available in the list, please refer to Secure communications explained on page 22 and read about creating compatible certificates.

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

Using the log viewer application

> When upgrading the integration to 4.2, 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.

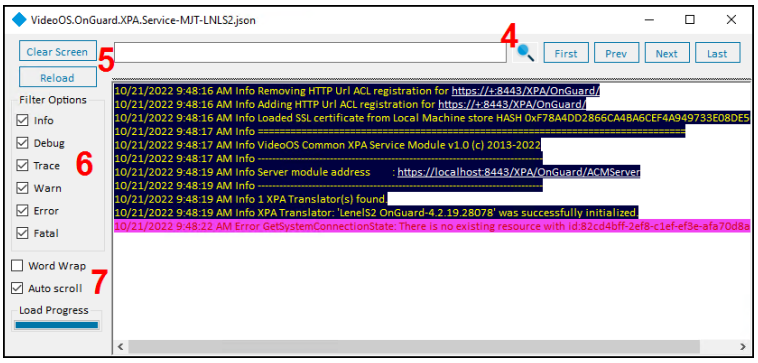
1. Choose the **View logs** option from the shortcut menu of the service tray icon to launch the log viewer.



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.

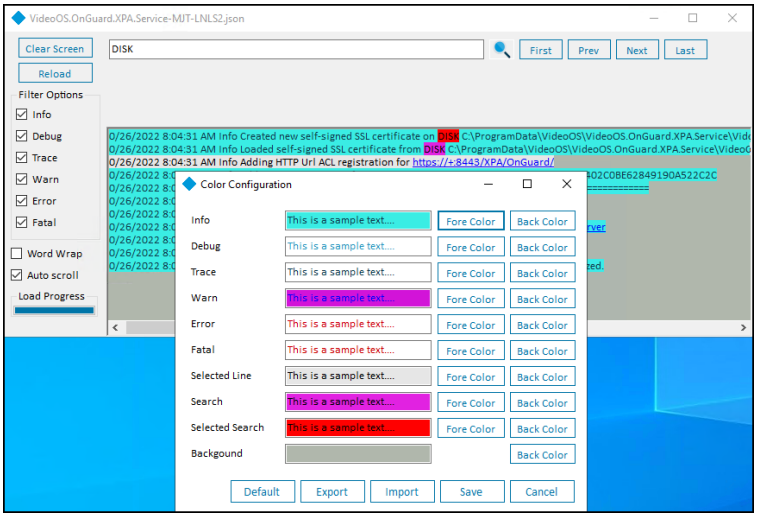


- Type in the text field at the top of the menu and hit enter or click the magnifying glass icon to start a text search. Use the **First**, **Prev**, **Next**, and **Last** buttons in the top right to navigate the search results.
- The **Clear Screen** button empties the main text display window, and 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.OnGuard.XPA.Service-MJT-LNLS2.json
Clear Screen
Reload
DISK
First
Prev
Next
Last
Filter Options
Info
Debug
Trace
Warn
Error
Fatal
Word Wrap
Auto scroll
Load Progress
0/26/2022 8:04:31 AM Info Created new self-signed SSL certificate on DISK C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\Vid
0/26/2022 8:04:31 AM Info Loaded self-signed SSL certificate from DISK C:\ProgramData\VideoOS\VideoOS.OnGuard.XPA.Service\VideoO
0/26/2022 8:04:31 AM Info Adding HTTP Url ACL registration for https://+:8443/XPA/OnGuard/
Color Configuration
Info
Debug
Trace
Warn
Error
Fatal
Selected Line
Search
Selected Search
Backgound
This is a sample text....
Fore Color
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 version 4.2 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

OnGuard loses communication with access control hardware

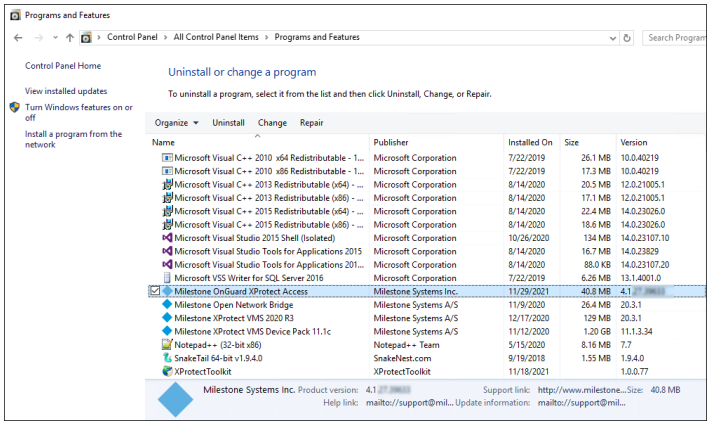
Communication can fail for the following reasons:

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 4.2 version of the plugin.

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

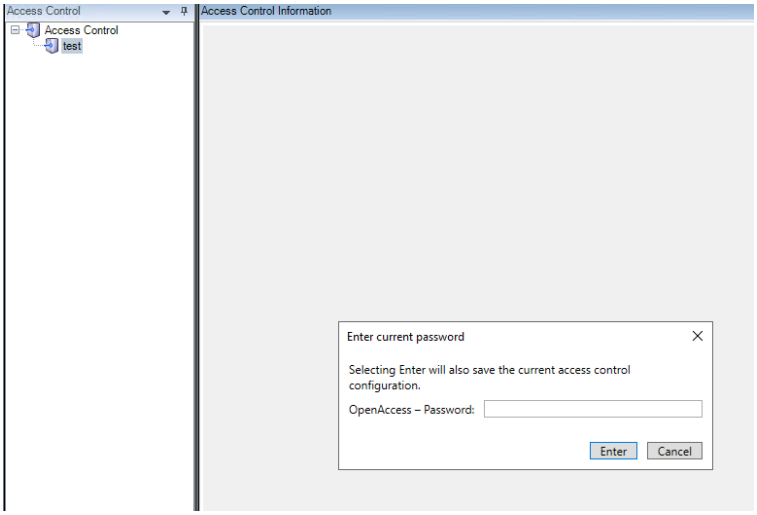


2. Go to the **Program and Features** menu on the OnGuard server. Uninstall the Milestone OnGuard XProtect Access component
3. Download the old version of the integration.
4. On the OnGuard server: re-install the OnGuard XProtect Access Service.
5. On the Milestone server: re-install the OnGuard XProtect Access MipPlugin.
6. 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.

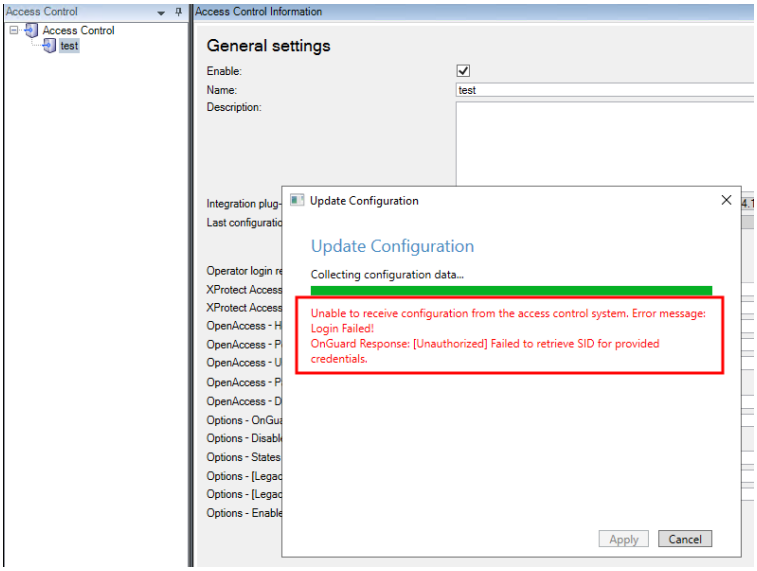
XProtect 2021 R1 and R2 shows no error if OpenAccess - password is incorrect.

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.



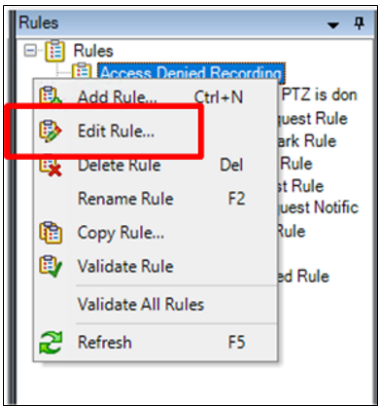
To verify the correct settings are in place for the password and all other parameters controlling the connection between integrated access control systems and the XProtect Event Server, use the **Refresh Configuration** feature each time after entering the password, and each time the settings on the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



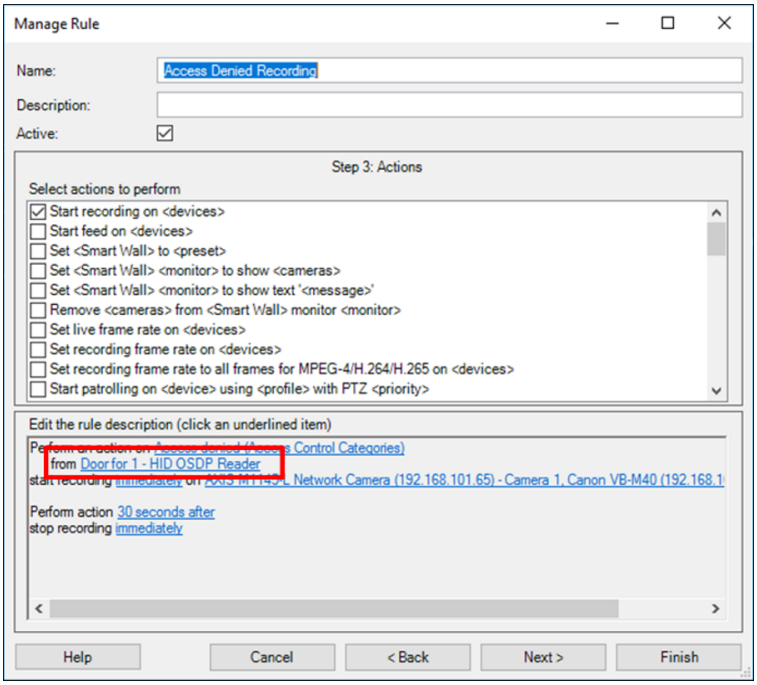
Access control rules stop working after upgrade to 4.0 or newer.

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.

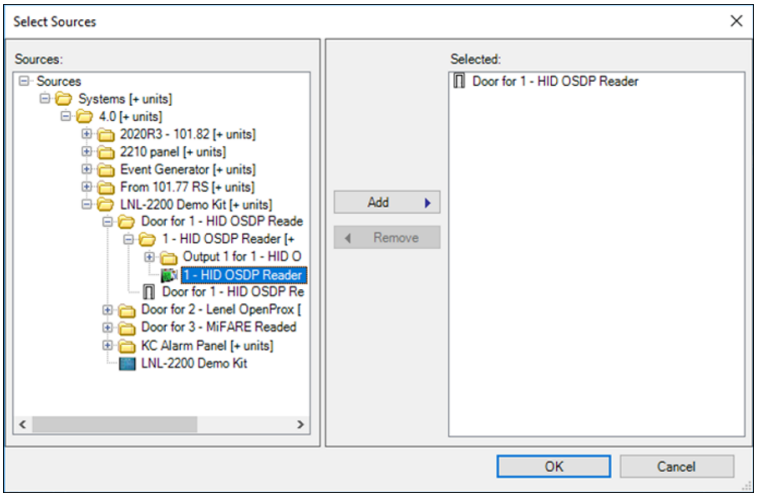
1. Find all access control related rules in the XProtect **Rules** menu. Right-click each individual rule, and select **Edit Rule...** from the shortcut menu.



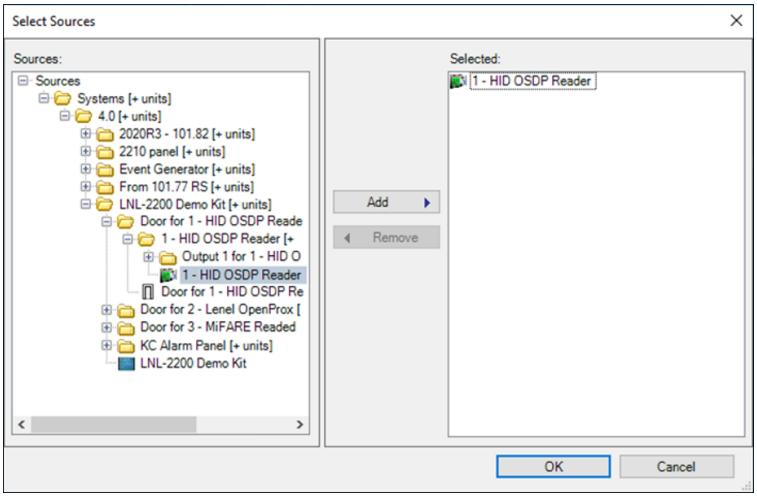
2. Click the door hardware object used as the source of the event.



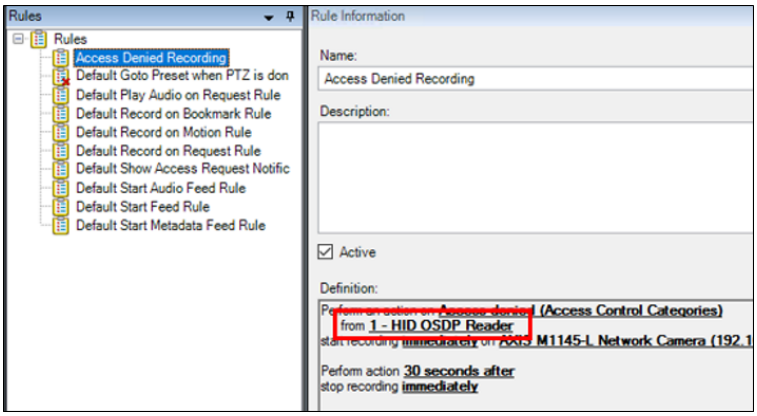
3. The **Select Sources** window opens. Expand the source directory to identify the door hardware object(s) matching the **Selected** hardware objects. Associated to that door hardware object are one or more reader hardware objects.
4. Choose the correct reader associated to the door for this rule.



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.



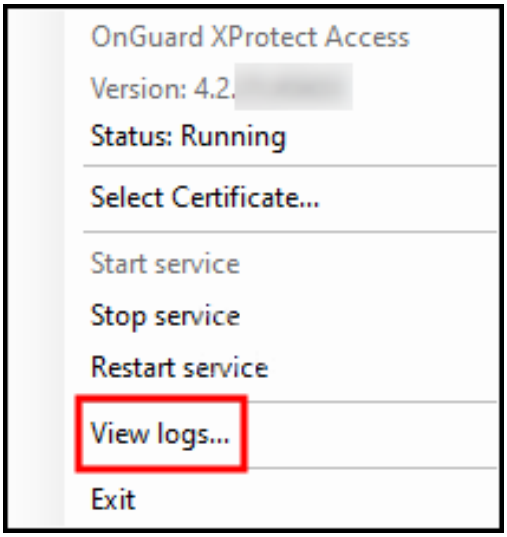
7. Finish editing the rule.
8. Perform this same process for all access control related rules in the XProtect VMS. Check the rules by selecting a rule and verifying the hardware object used as the source.



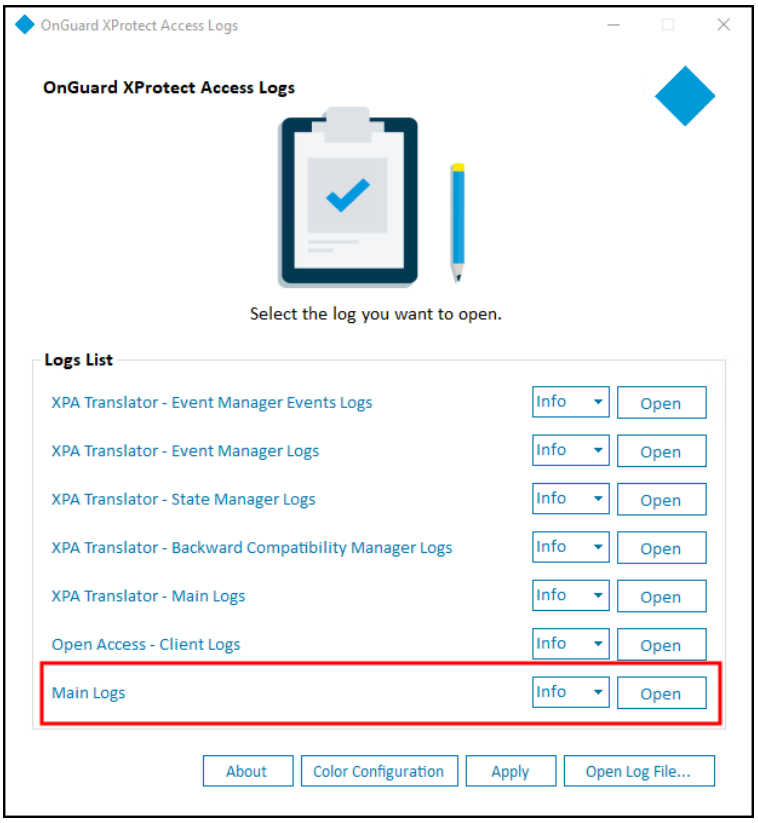
OnGuard XProtect Access Service: MipPlugin post-install verification

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.



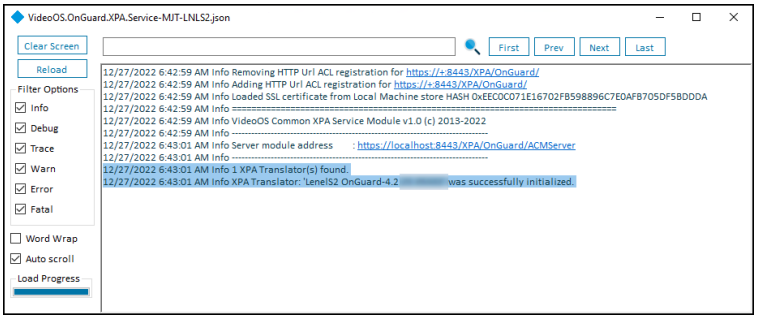
2. Choose to open the **Main Logs** from the log viewer application.



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

Info 1 XPA Translator(s) found.

Info XPA Translator: 'LenelS2 OnGuard-4.2.xx.xxxxx' was successfully initialized.



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:

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

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 OnGuardXProtect Access integration to version 4.2 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 wont 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.

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
4.2	Current documentation refers to integration versions 4.2 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

# Private certificate for signing other certificates (in certificate store)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyusageProperty All `
                                            -KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS CA Certificate' `
                                            -TextExtension @("2.5.29.19={critical}{text}ca=TRUE")

# 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"
```

```powershell
# 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/.