Milestone XProtect Access

OnGuard User Manual

Prepared by:

Custom Development Americas

milestone

Table of Content

Copyright, Trademarks & Disclaimers **4**
Copyright 4
Trademarks 4
Disclaimer 4
General Description **5**
Solution overview 5
Scalability **5**
Planning your Installation **6**
Single System Scenario 6
Multiple Single Systems 7
Milestone XProtect Federation with OnGuard Enterprise 9
Distributed deployment options 10
Single system with ACM Server 11
Milestone XProtect Clustered with Single Clustered OnGuard 11
Version Notes **12**
Version Compatibility **12**
OnGuard Version support 12
Recommended OnGuard Versions 12
XProtect Version Support **13**
Hardware Support **13**
Secure Communication **13**
FIPS-140-2 Compatibility **14**
Prerequisites **14**
Time Synchronization 14
.NET Framework for OnGuard 14
Milestone XProtect License 14
Event Server DNS / Name resolution 15
Smart Client Profiles 15
OnGuard License Options – PLEASE CONSULT CARRIER FOR LICENSING 15
Required OnGuard Services 16
Generate software events 16
Create Single Sign-On (SSO) Directory 16
Create Single Sign-On (SSO) User 18
Installation **20**
ACM Server Installation 21
OnGuard Plugin Installation 22
XProtect ACM MIP Plugin 23
MIP Plugin Upgrades 25

milestone

Upgrading to 4.0 from DataConduIT 26
MIP Plugin Downgrades 27
XProtect ACM MIP Plugin Configuration 30
ACM Server Wizard 30
Installing an ACM Server 30
XProtect Management Client Configuration 34
XPA Instance Creation Wizard 34
XPA Instance Status & Properties 38
Personalized Login 40
Commands: 42
Administrative Configuration 46
Door & Camera Association 46
Categorize Events 47
Access Request Notifications 50
Searching for Cardholders 52
Client Profiles & Roles 53
Smart Client Features 54
Access Control Workspace 54
Access Monitor 59
Maps 61
Overlay Buttons & Commands 63
Alarm Acknowledgment 65
Access Control Options 67
Mobile Client 68
Access Control Tab in Milestone Mobile 68
Logging 70
Log File Locations 70
Changing logging level 70
Troubleshooting Guide 72
ACM Server: OnGuard Plugin Post-Install Verification 72
Connection Status displays “Not connected” or is empty. 73
OnGuard loses communication with access control hardware 76
Not receiving cardholder or badge changes 76
ACM integration flooding OnGuard user transaction report 77
OnGuard ACM instance not displayed in the XProtect Management Client 77
LS OpenAccess service automatically stops seconds after starting 78
I/Os connected to OSDP readers are no longer detected 78
LS OpenAccess events fail in OnGuard Enterprise systems 78
All other support issues 78
Known issues: 78

milestone

Copyright, Trademarks & Disclaimers

Copyright

© 2021 Milestone Systems.

Trademarks

XProtect® is a registered trademark of Milestone Systems.
Microsoft and Windows are registered trademarks of Microsoft Corporation.
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.

General Description

This document describes the XProtect Access (XPA) integration between Milestone XProtect video management system (VMS) and the OnGuard access control (AC) system. This integration supports the following standard XPA 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...etc., triggered by door forced, access granted, access denied...etc.
- 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.

Solution overview

The solution provided is split in 3 components:

1. The "ACM Server MIP Plugin" that runs in the XProtect Event Server (Milestone.ACMServer.MipPlugin.msi)
2. The "ACM Server" that runs on the OnGuard server (Milestone.ACMServer.x64.msi)
3. The "OnGuard ACM Server Plugin" that runs on the OnGuard server (Milestone.ACMServer.OnGuard.msi)

Scalability

This section details the size of the test system at the LenelS2 certification labs and lists the performance that can be expected.

The software interface between the Milestone and OnGuard has been optimized for throughput of events and system status messages. However, server components and computer hardware resources can still limit total throughput.

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

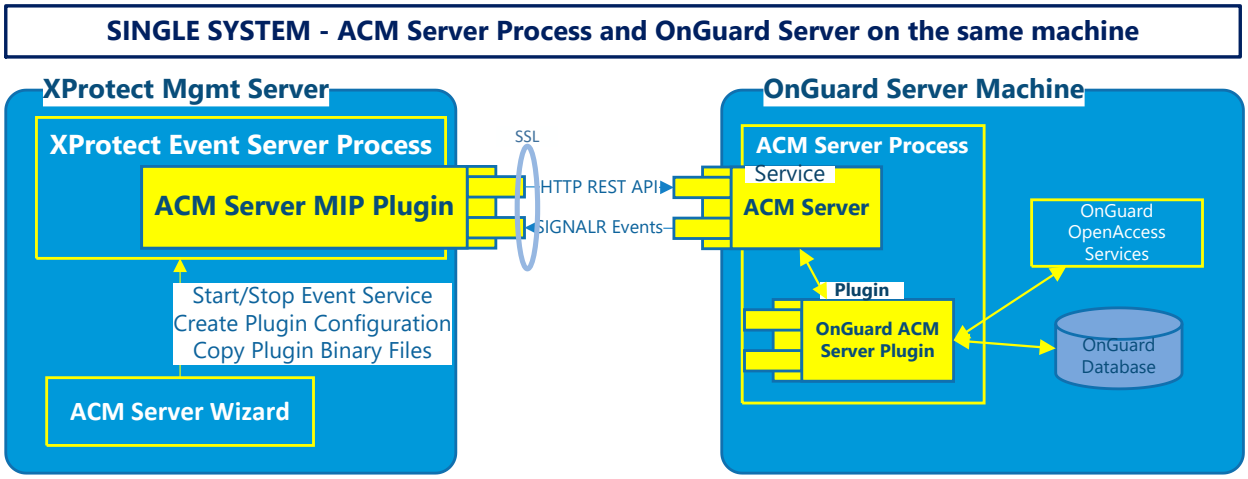
Eventing	Events/sec
OpenAccess	100
OpenAccess – Peak	300+

Planning your Installation

There are many 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.

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 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 – ACM Server and OnGuard Server on separate machines	There is a need to run the ACM Server 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

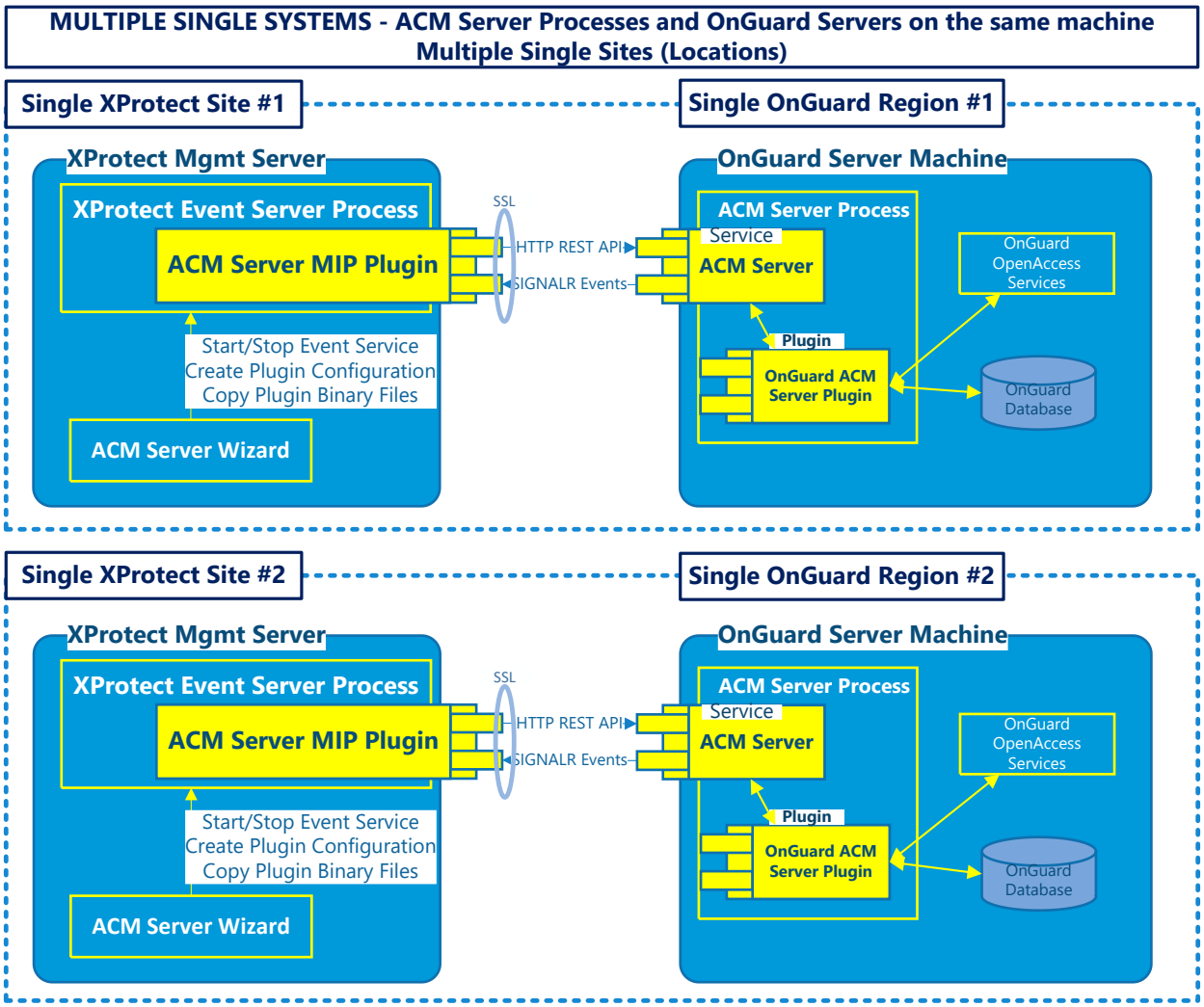


For most systems, this is the recommended installation scenario.

- The ACM Server MIP Plugin is installed on the XProtect Event Server machine.
- The ACM Server and its OnGuard plugin are installed on the SAME machine as the OnGuard communication server and OpenAccess Services.

Multiple Single Systems

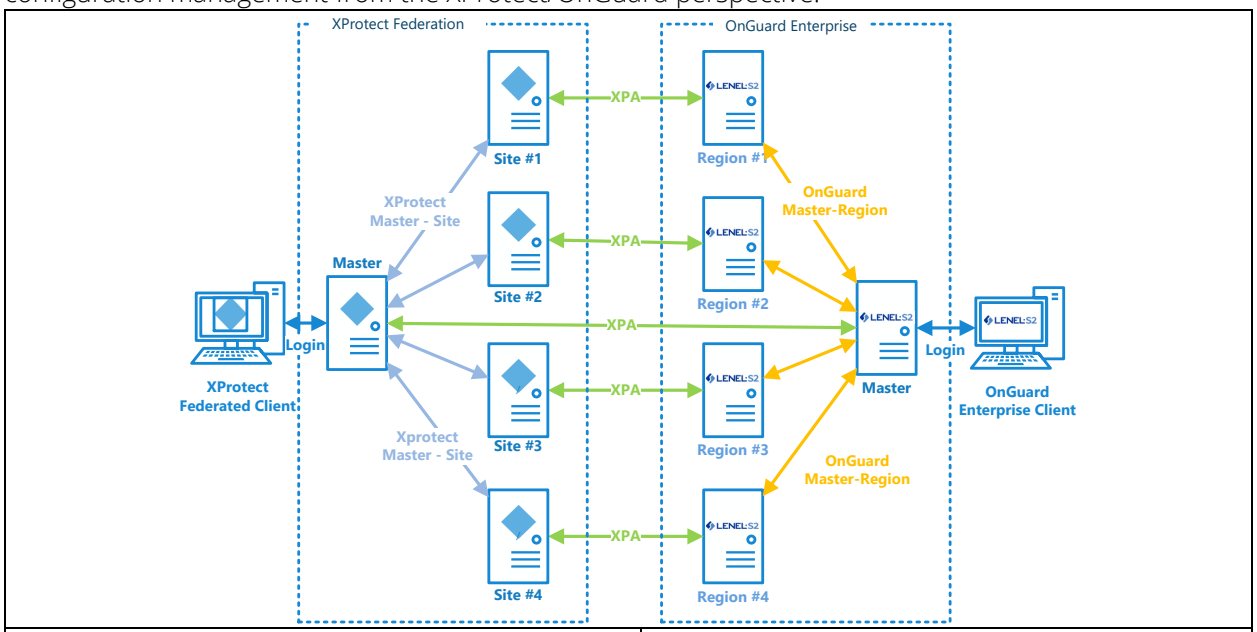
Scaling the default scenario means adding more OnGuard systems and XProtect systems in a 1:1 ratio. The OnGuard and XProtect systems are independent of each other, keeping the ACM Server process on the OnGuard machine. The customer is NOT interested in centralized configuration or alarms, his multiple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



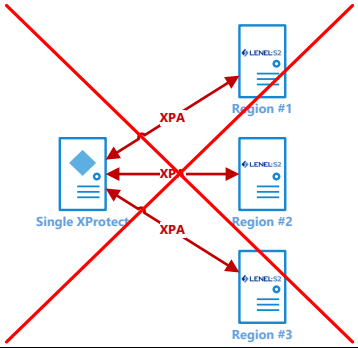
Site #1 and Site #2 are independent of each other and are not communicating with each other, or commonly managed. The same is true for both the XProtect and the OnGuard systems in this scenario.

Milestone XProtect Federation with OnGuard Enterprise

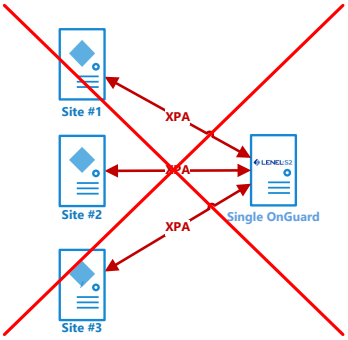
This scenario has multiple uses. It will be common for large scale deployments. This should be the default scenario when the customer already has an Enterprise deployment of OnGuard and wants to integrate XProtect. Also, it should be used when the customer wants centralized alarm and configuration management from the XProtect/OnGuard perspective.



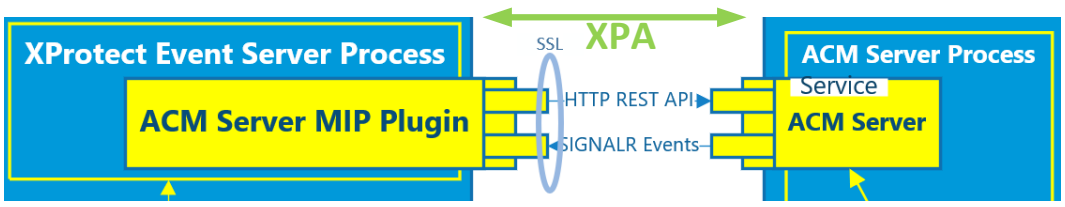
We DO NOT support one single XProtect Site to connect to multiple OnGuard Regions. We do not recommend running more than one XProtect Access integration per event server, (whether it be OnGuard or other AC system) for performance reasons.



We DO NOT support multiple XProtect Sites to connect to a single OnGuard region.

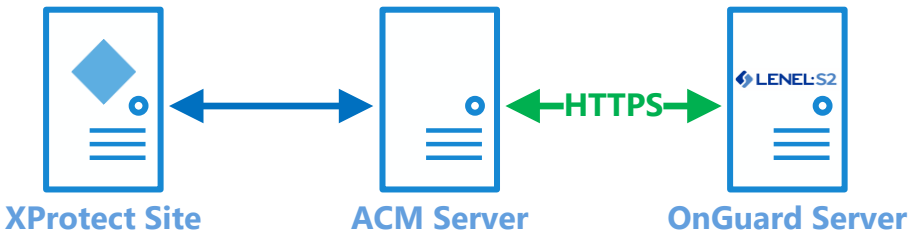


Each green XPA line represents the HTTP/SignalR connection between the Event Server in XProtect and the ACM server on the OnGuard Server (there are some scenarios where ACM server may not live on the same OnGuard server, see Distributed deployment options for details).

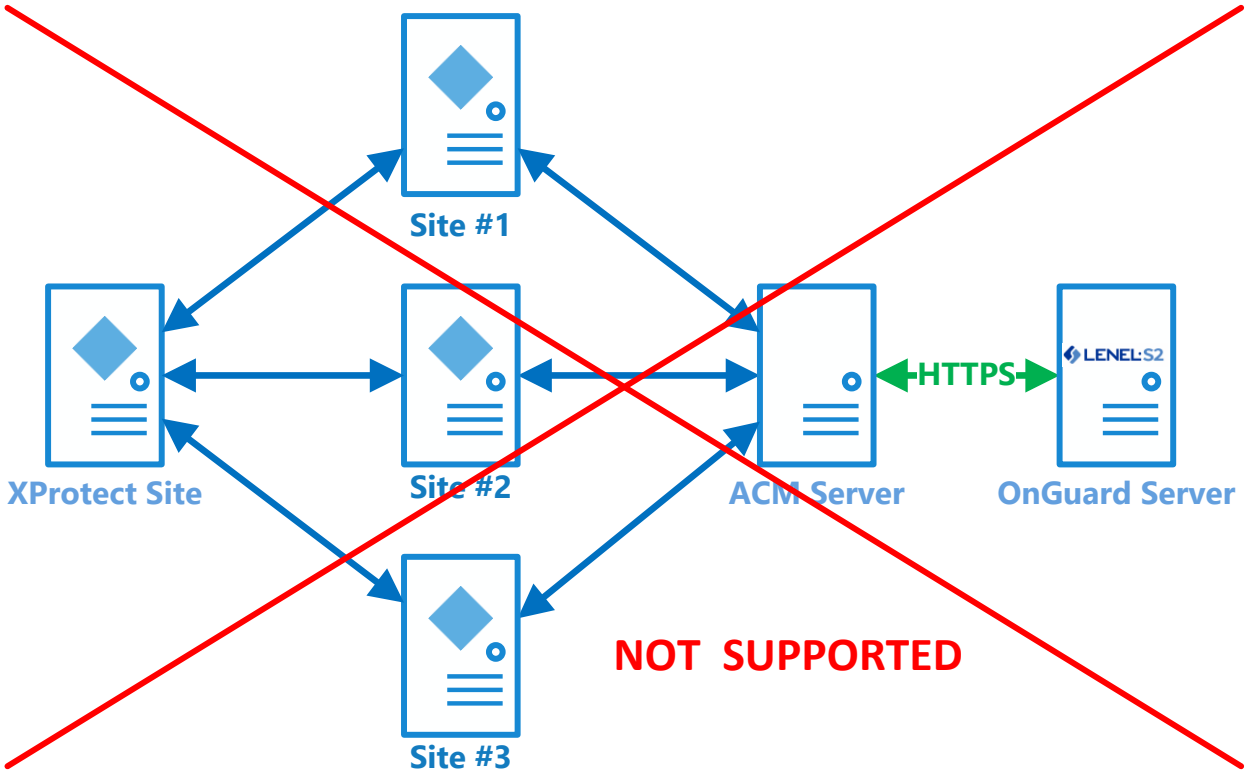


Distributed deployment options

It is possible to have the "integration" ACM server on a different machine than the XProtect server and the OnGuard server. These scenarios allow OnGuard segmentation of hardware and events to multiple XProtect sites and OnGuard clustering support.

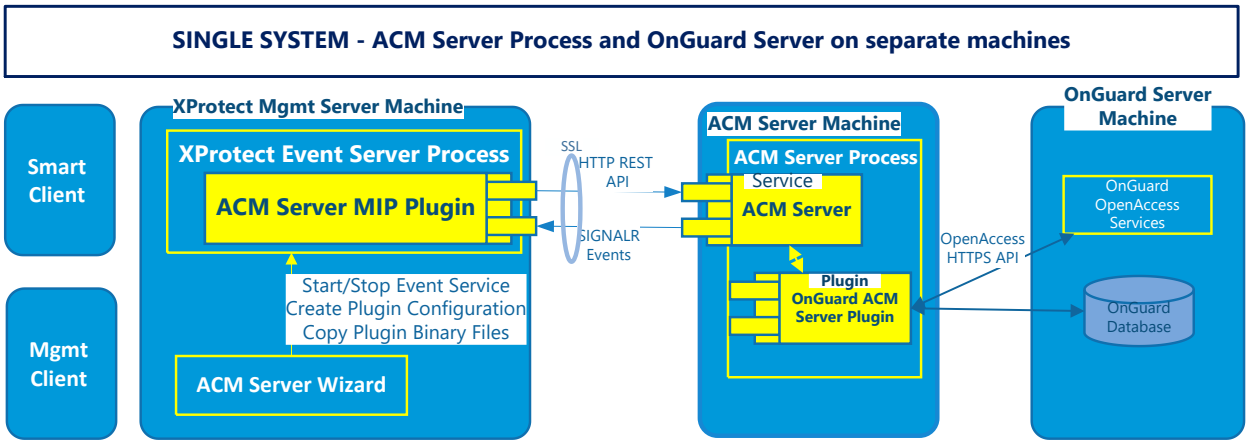


For design, scaling and performance reasons, we do not support connecting multiple XProtect sites to the same ACM Server instance.



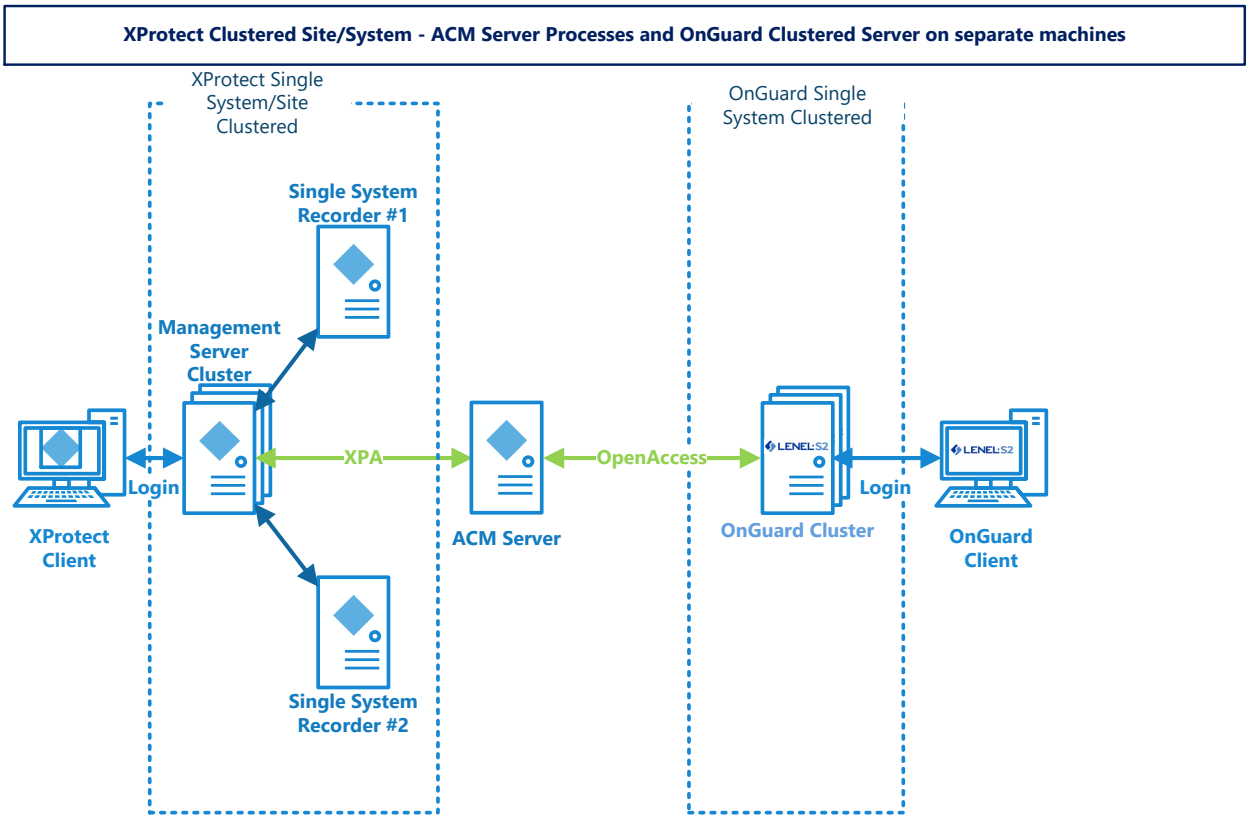
Single system with ACM Server

This scenario is used when it is required to run the ACM Server on a different machine than the OnGuard Server.



Milestone XProtect Clustered with Single Clustered OnGuard

When server clusters are used for redundancy, ACM Server must be removed from both the XProtect and OnGuard servers. This is the scenario architecture if both XProtect and OnGuard use server clusters:



Version Notes

Version	Notes
4.0	Current documentation refers to integration versions 4.0 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.

Version Compatibility

Here is the compatibility matrix between OnGuard and Milestone XProtect.

OnGuard	XP 2018 R1-R3	XP 2019 R1-R3	XP 2020 R1-R2	XP 2020 R3
7.4	S	S	S	T
7.5	S	T	T	S
7.6	S	S	T	T
8.0	S	T	T	T

T: [Tested]	Integration is fully tested and supported on these versions
S: [Supported]	Integration is fully supported on these versions
U: [Unsupported]	Integration may or may not exist but is not supported/maintained on these versions

OnGuard Version support

Version	Minimum update / patch level	Support statement
OnGuard 7.4	7.4.457.0 and up	These versions are fully supported
OnGuard 7.5	7.5.375.0 and up	These versions are fully supported
OnGuard 7.6	7.6.382.0 and up	These versions are fully supported
OnGuard 8.0	8.0.458.0 and up	These versions are fully supported

Recommended OnGuard Versions

The following OnGuard versions have been tested to provide the best performance. These versions contain all documented hotfixes.

Version	Minimum update / patch level	Support statement
OnGuard 7.4	7.4.457.626 and up	Contact Carrier partner support for download
OnGuard 7.5	7.5.375.477 and up	Contact Carrier partner support for download
OnGuard 7.6	7.6.382.271 and up	Available through partner center downloads
OnGuard 8.0	8.0.458.29 and up	Available through partner center downloads

XProtect Version Support

Here is the XProtect version compatibility matrix between Milestone Yearly Release Versions and Milestone XProtect VMS Product Versions.

XProtect Version	XProtect Essential+	XProtect Express*	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
XProtect 2018 R1-R3	U	S	S	S	S	S
XProtect 2019 R1-R3	U	S	S	S	S	S
XProtect 2020 R1-R3	U	S	S	S	S	S

S: [Supported]	XProtect is fully tested and supported in these versions
U: [Unsupported]	XProtect is not supported in these versions

*Free XProtect Editions: Go, Essential and Essential+ are NOT supported.

Hardware Support

The following OnGuard panels have been tested and are known to be supported. More hardware models are compatible. Only the specific models listed below are known to be supported by Milestone Technical Support.

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

Secure Communication

End-to-end encryption, also known as secure communication, is compatible with all versions of the OnGuard XProtect Access integration.

You can encrypt two-way connection between the management server and any remote server (i.e., event server, recording server...etc.) in the XProtect System. You can encrypt two-way connection between a

recording server and all clients, servers, and integrations that retrieve data streams from a recording server. You can encrypt two-way connection between mobile servers and all clients, servers and integrations that retrieve data streams. For more information, see the XProtect Certificates Guide.

All versions of the OnGuard XProtect Access integration support XProtect systems configured for secure communication.

FIPS-140-2 Compatibility

Here is the FIPS-140-2 compatibility matrix between OnGuard XProtect Access Integration and Milestone XProtect. 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. However, XProtect and OnGuard are individually both FIPS-140-2 compliant.

OnGuard XProtect Access Integration Version	XP 2018 R1-R3	XP 2019 R1-R3	XP 2020 R1-R2	XP 2020 R3
3.5 and below	U	U	U	U
3.6 and above	U	U	U	S

S: [Supported]	FIPS-140-2 is fully tested and supported on these versions
U: [Unsupported]	FIPS-140-2 is not supported on these versions

Prerequisites

Time Synchronization

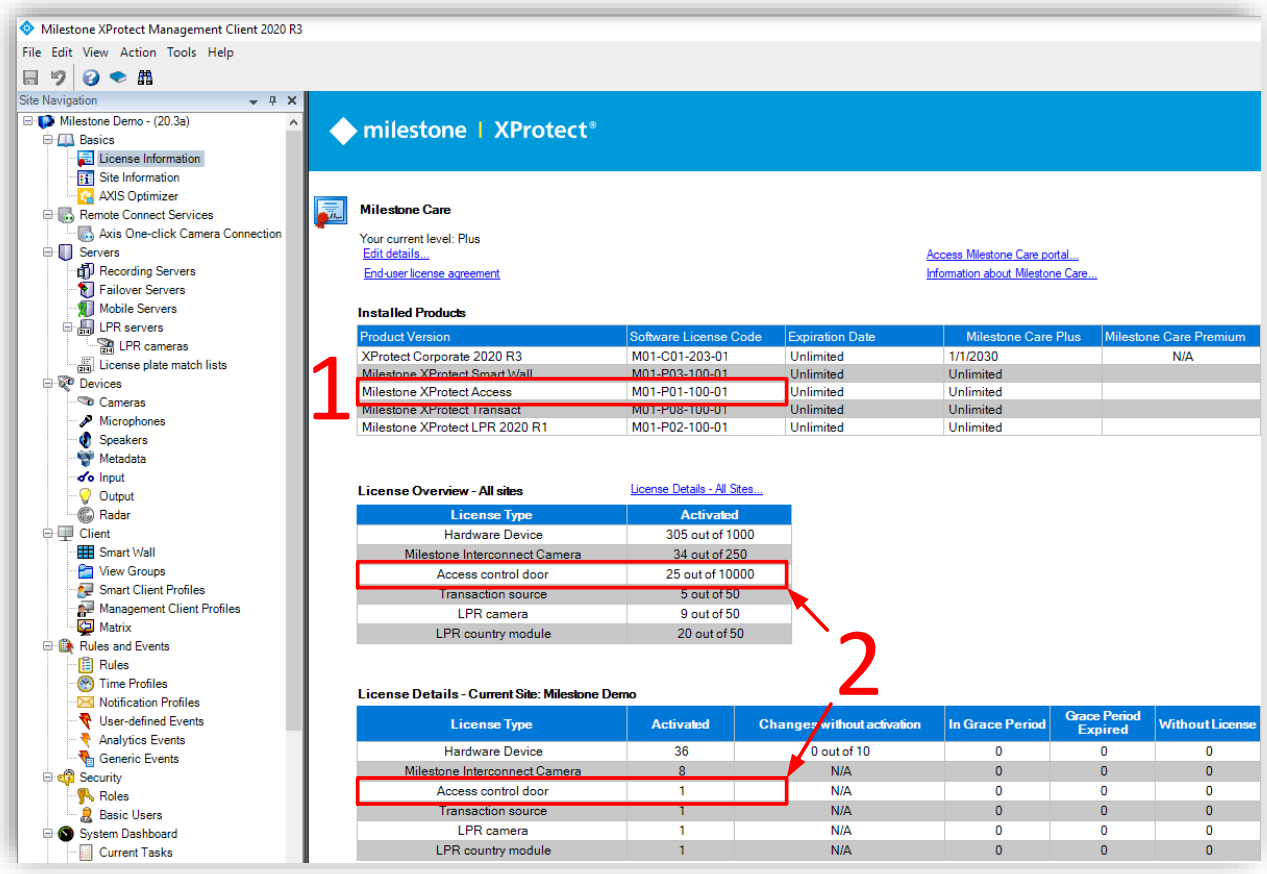
All servers (i.e. the OnGuard and Milestone machines) must be time-synchronized to within a couple of minutes of one another. See Kerberos V5 time skew recommendations here.

.NET Framework for OnGuard

.NET Framework 4.7.2 must be installed on the OnGuard server machine (NDP472-KB4054530-x86-x64-AllOS-ENU.exe). This is mostly for older OS editions; anything above Windows 10 April 2018 Update and Windows Server version 1803 will have it already installed as part of the OS. Milestone recommends that you use Microsoft Windows Server Editions of the OS.

Milestone XProtect License

The customer must have Milestone 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 Milestone Event Server.

Smart Client Profiles

If you customize/add Smart Client Profiles, you need to include Access Control – Show access request notifications = Yes (default setting) if you want your users to see Access Control notifications.

OnGuard License Options – PLEASE CONSULT CARRIER FOR LICENSING

To enable the integration to work the following license options must be enabled in the OnGuard license:

Type of 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 only supported connection mode is OpenAccess. The OnGuard license must have the OpenAccess license options for the integration to function. If you are upgrading to version 4.0 please refer to Milestone Knowledge Base article 30105.

Required OnGuard Services

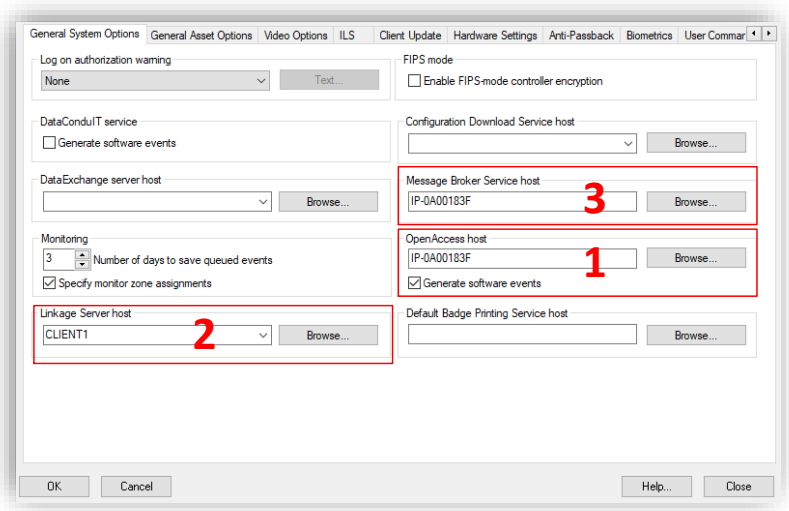
The following Windows services must be running on the OnGuard machine:

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

Under Administration, 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.

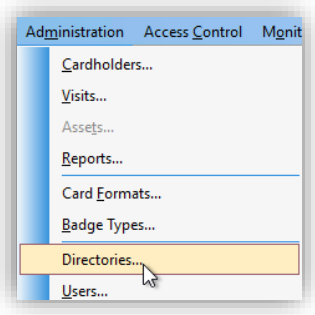


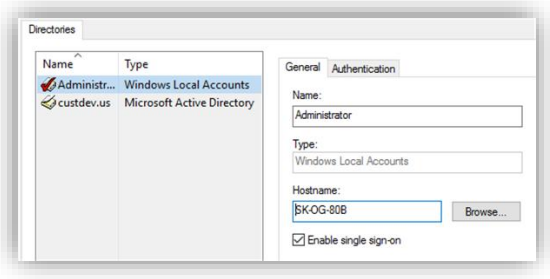
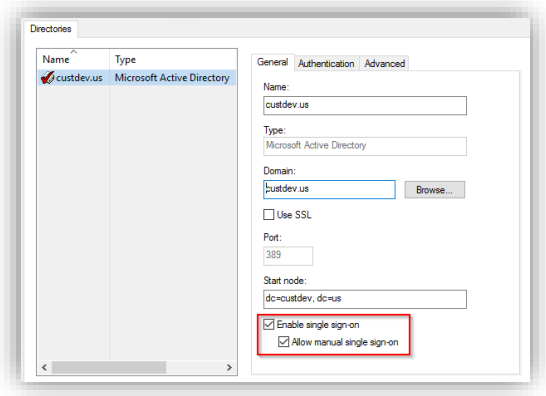
Create Single Sign-On (SSO) Directory

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

For an OnGuard Enterprise system, you can only create directories on the master. server.

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



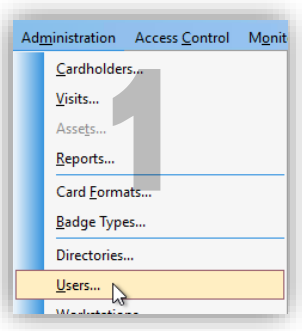
Windows Local Account	Domain User Account
For Windows Local Account support, the single sign-on account MUST be a "Windows Local Account".	For Domain User Account support, the single sign-on account MUST "Allow manual single sign-on" as shown below.
	

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

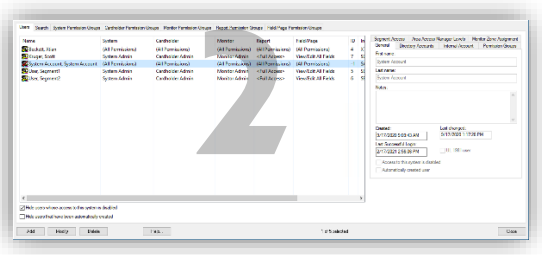
Create Single Sign-On (SSO) User

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

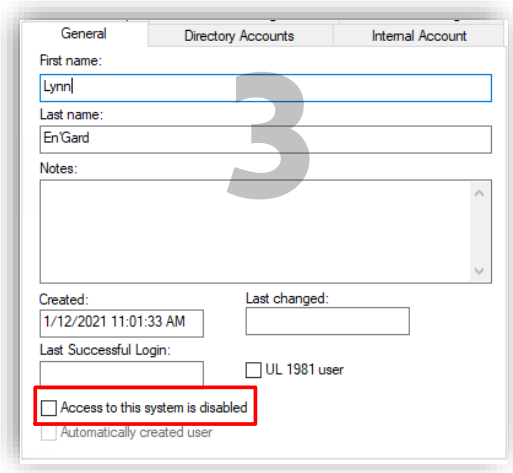
Go to the Administration menu and select Users...



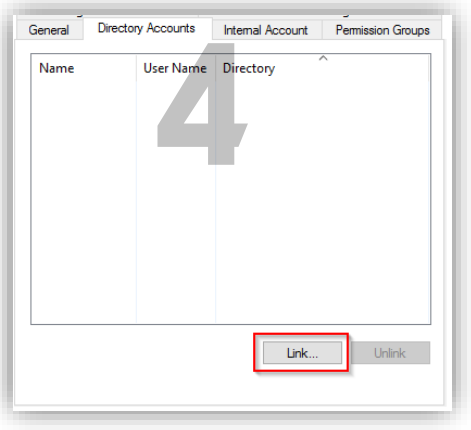
Add a new user, or modify a user from the list of internal system users.



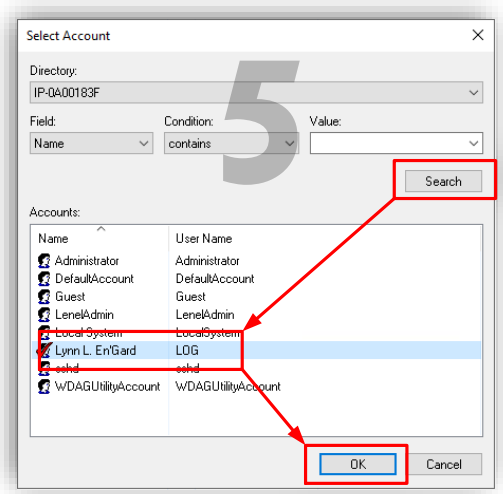
On the General tab "Access to this system is disabled" should NOT be selected.



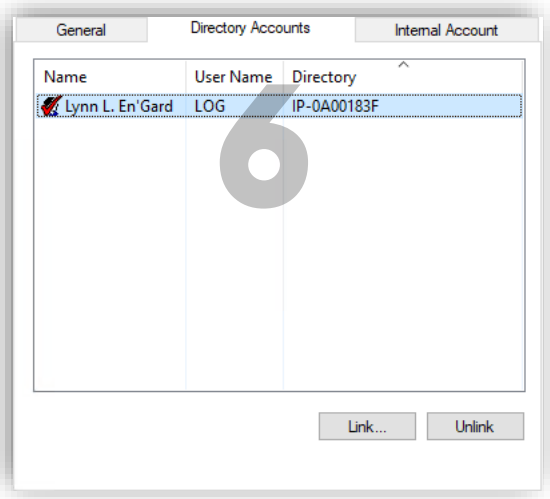
On the Directory Accounts tab click "Link" to associate the user to the directory user (or local account user) from the directory created above.



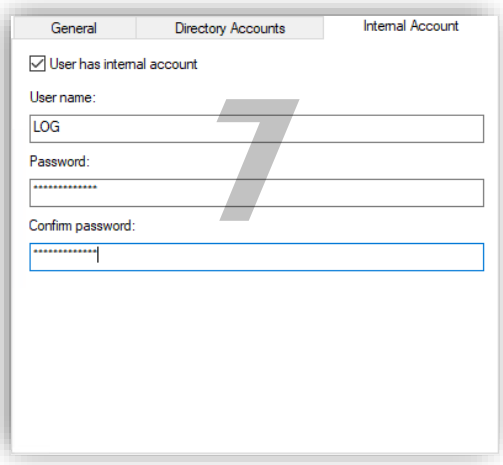
In the Select Account dialog select the directory from the Directory list. Click Search and select a user in Accounts then click OK.



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

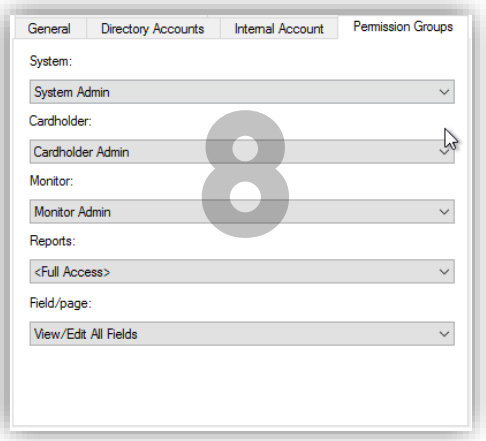


On the Internal Account tab, make sure that the "User has internal account" option is selected. Next, enter the account credentials.



On the Permission Groups tab assign the following permission groups:

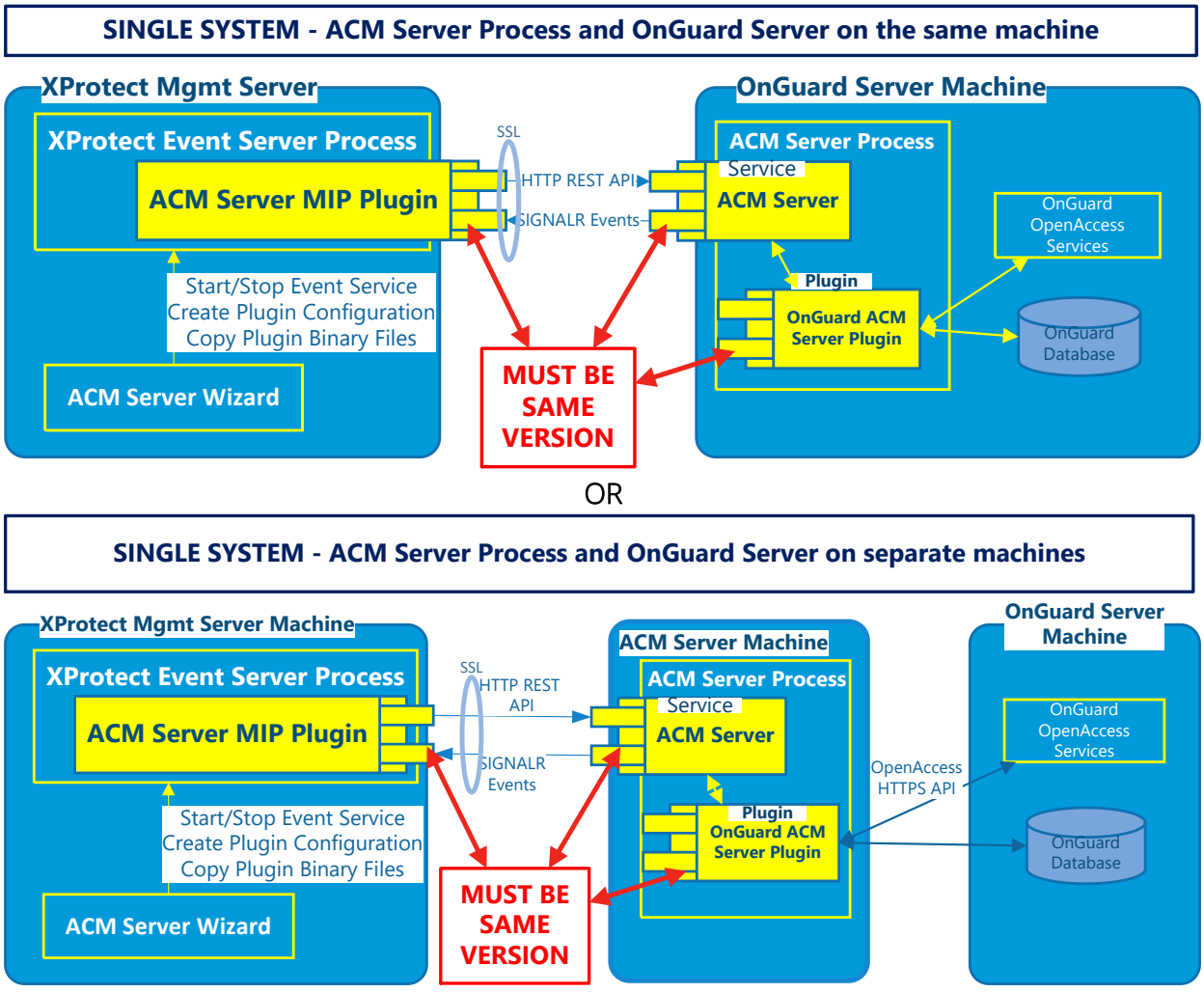
- System = System Admin
- Cardholder = Cardholder Admin
- Monitor = Monitor Admin
- Reports = Full Access
- Field/page = View/Edit All Fields



Installation

The installation package consists of three independent installers:

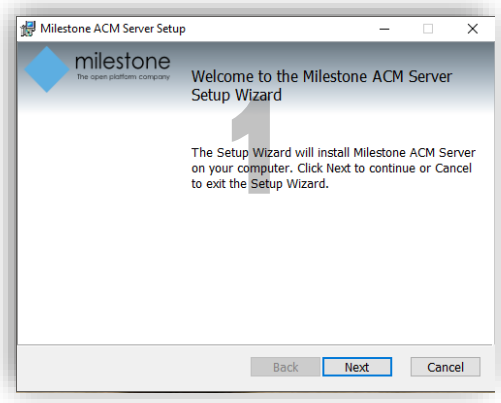
1. Milestone.ACMServer.x64.msi: Installer for the ACM Server
   – Installed on the OnGuard server machine, or its own machine.
2. Milestone.ACMServer.OnGuard.msi: Installer for the OnGuard ACM Server plugin
   – Installed on the OnGuard server machine, after the ACM Server. On its own machine (i.e. the same machine as ACM Server) after the ACM Server.
3. Milestone.ACMServer.MipPlugin.msi: Installer for the XProtect Event Server ACM MIP Plugin
   – Installed on the XProtect Machine that hosts the Event Server Windows service.



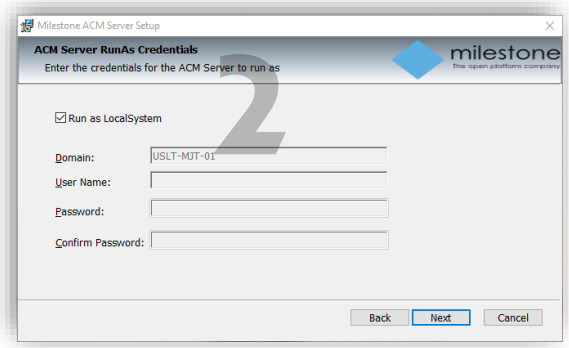
It is required that the exact same versions of the OnGuard ACM integration software components are installed on both the XProtect and OnGuard machines.

ACM Server Installation

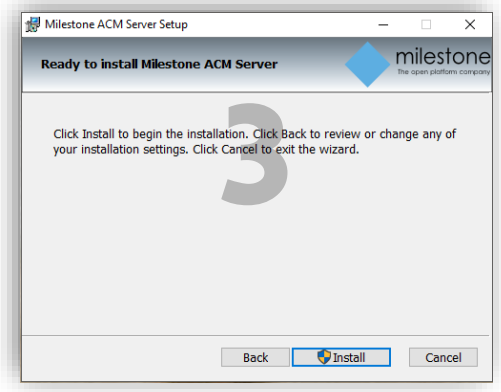
Double-click the Milestone.ACMServer.msi file to begin:



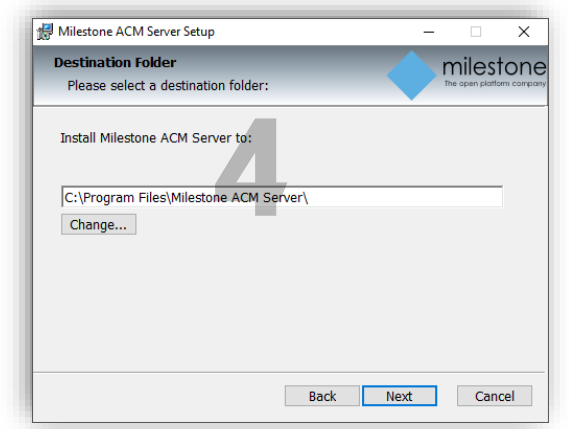
By default, the ACM server runs as LocalSystem. If required by Group Policy, choose a specific account.



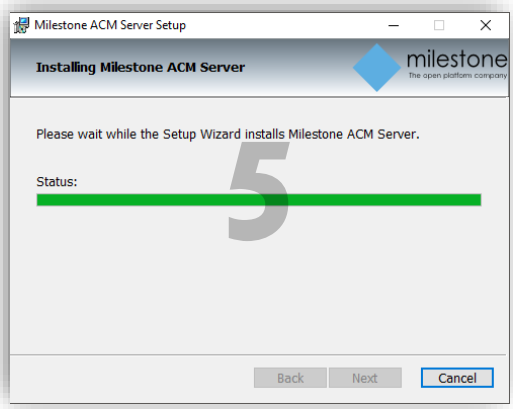
Optionally, click Back to change installation location and move to step 4. Or click "Install" and move to step 5.



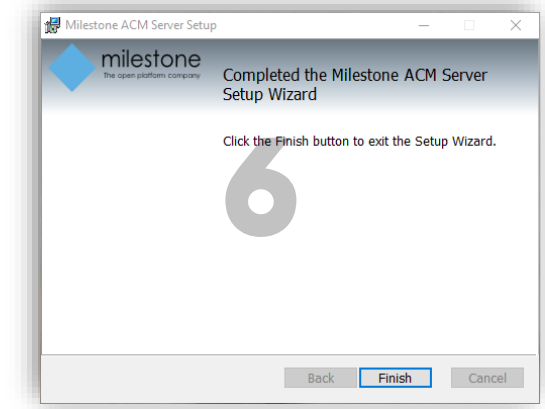
Define the installation location at this step. You will return to step 3.



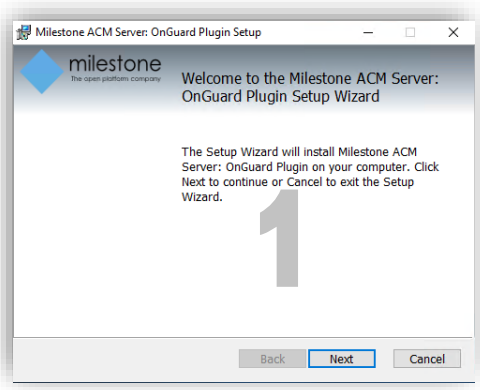
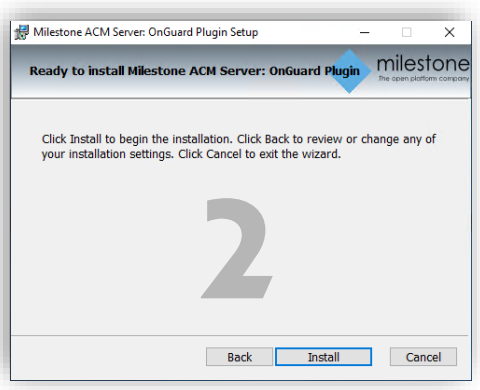
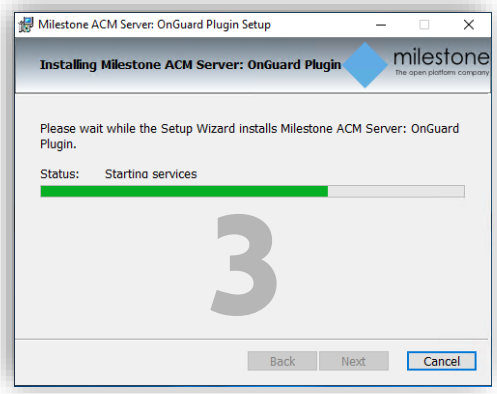
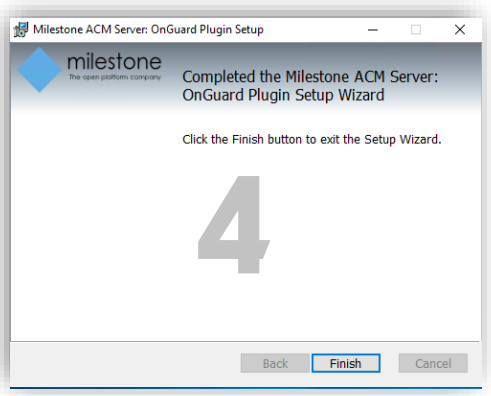
Install progress...



Click Finish to complete the wizard.

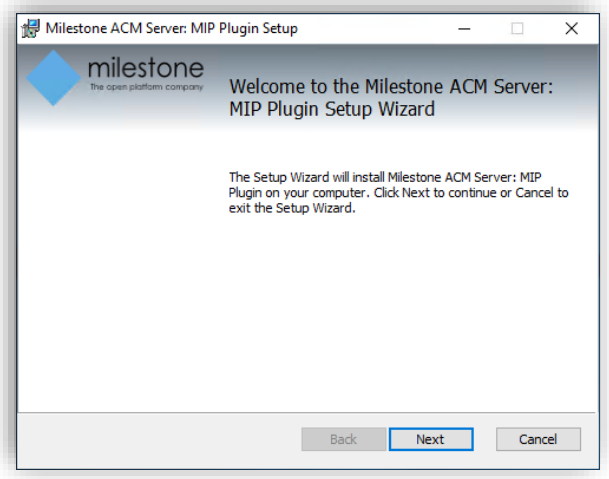


OnGuard Plugin Installation

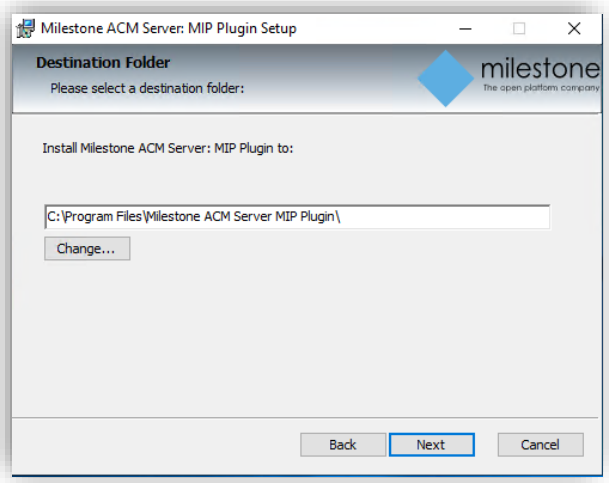
Double-click the Milestone.ACMServer.OnGuard.msi file to begin:  The OnGuard plugin automatically detects the presence of both the OnGuard server and the pre-installed ACM Server. If either is missing it will refuse to install.	There are no configurable options in this installer. When ready, press install. 
Install progress...  	You have successfully installed the Milestone ACM Server OnGuard Plugin 

XProtect ACM MIP Plugin

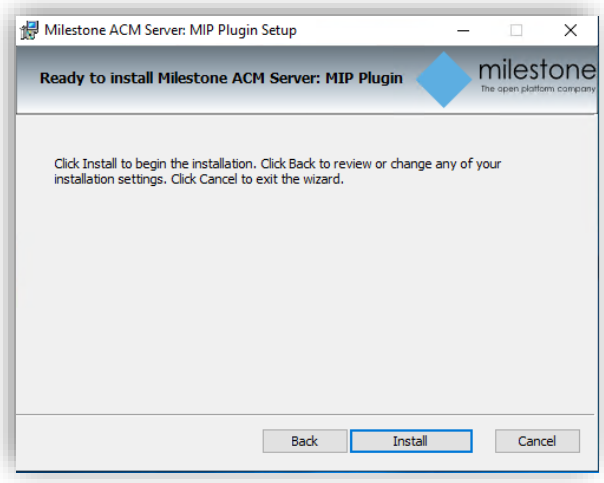
Place the Milestone.ACMServer.MipPlugin.msi file on the server where the XProtect Event Server is installed (in a typical deployment, this is the XProtect Management Server), and double-click to begin.



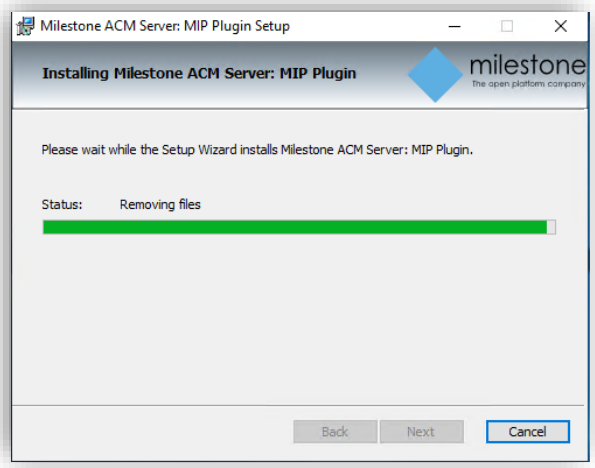
The installer checks if the XProtect Event Server is installed on the machine, it will refuse to continue if it is not found. Unless otherwise required, it is recommended to leave the default install location as displayed below, and click next.



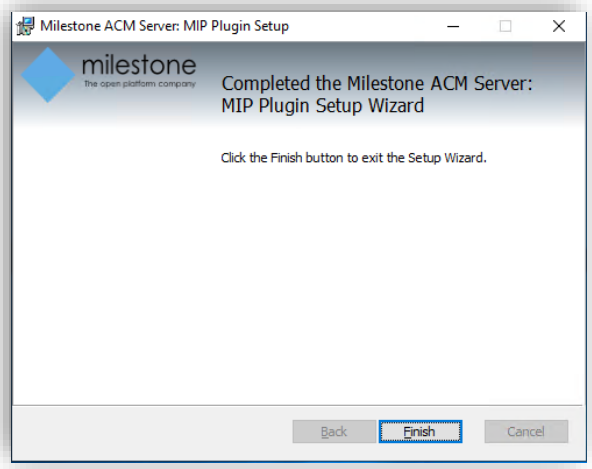
If ready to install click "Install"



Installation progress...



You have successfully installed the ACM MIP Plugin for ACM Server



MIP Plugin Upgrades

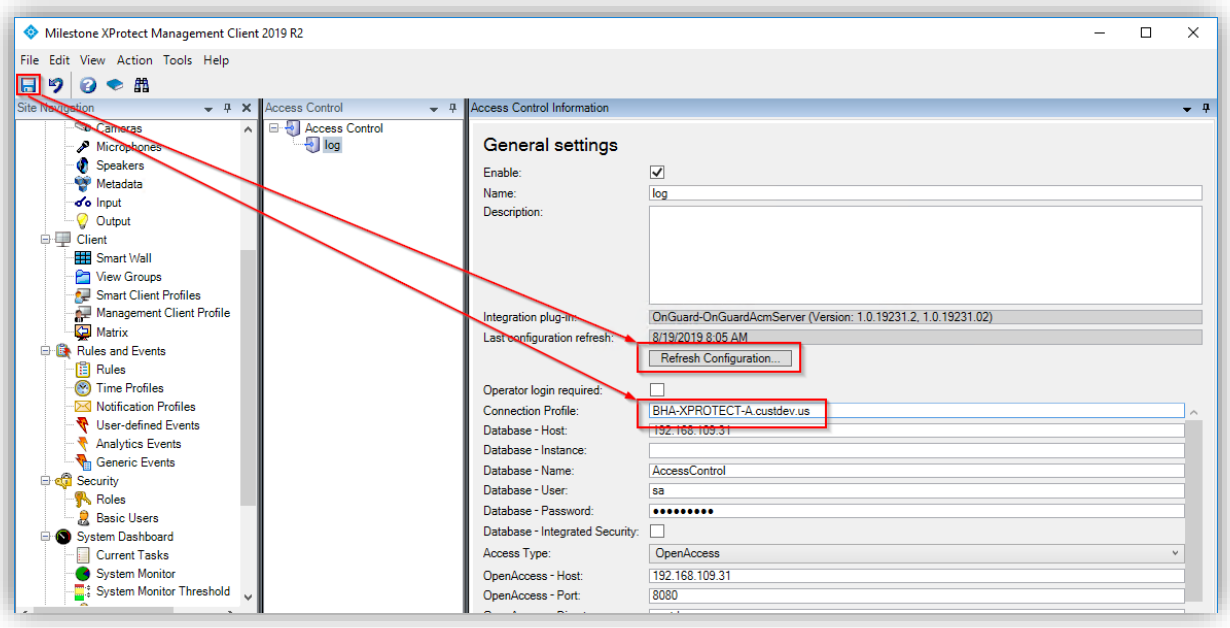
All components are updated with every new OnGuard ACM release. Always upgrade both the ACM Server and OnGuard ACM plugin on the OnGuard machine before upgrading the MIP Plugin on the XProtect Event Server.

The process for upgrading is the same as for a first time install:

1. ACM Sever (OnGuard - Milestone.ACMServer.x64.msi)
2. OnGuard ACM Plugin (OnGuard - Milestone.ACMServer.OnGuard.msi)
3. MIP Plugin (XProtect - Milestone.ACMServer.MipPlugin.msi)
4. Management Client Configuration (XProtect)

Automatic MIP Plugin upgrades of configured and installed instances in the Management Client are supported for all versions of the OnGuard ACM integration. Simply run the MIP Plugin installer; it will upgrade any installed ACM Servers.

After running the MIP Plugin installer, for each ACM instance in the Management Client. Set the ”Connection Profile” property to the name of the ACM Server machine. Press Save to save the configuration change. Click Refresh Configuration to update the configuration.

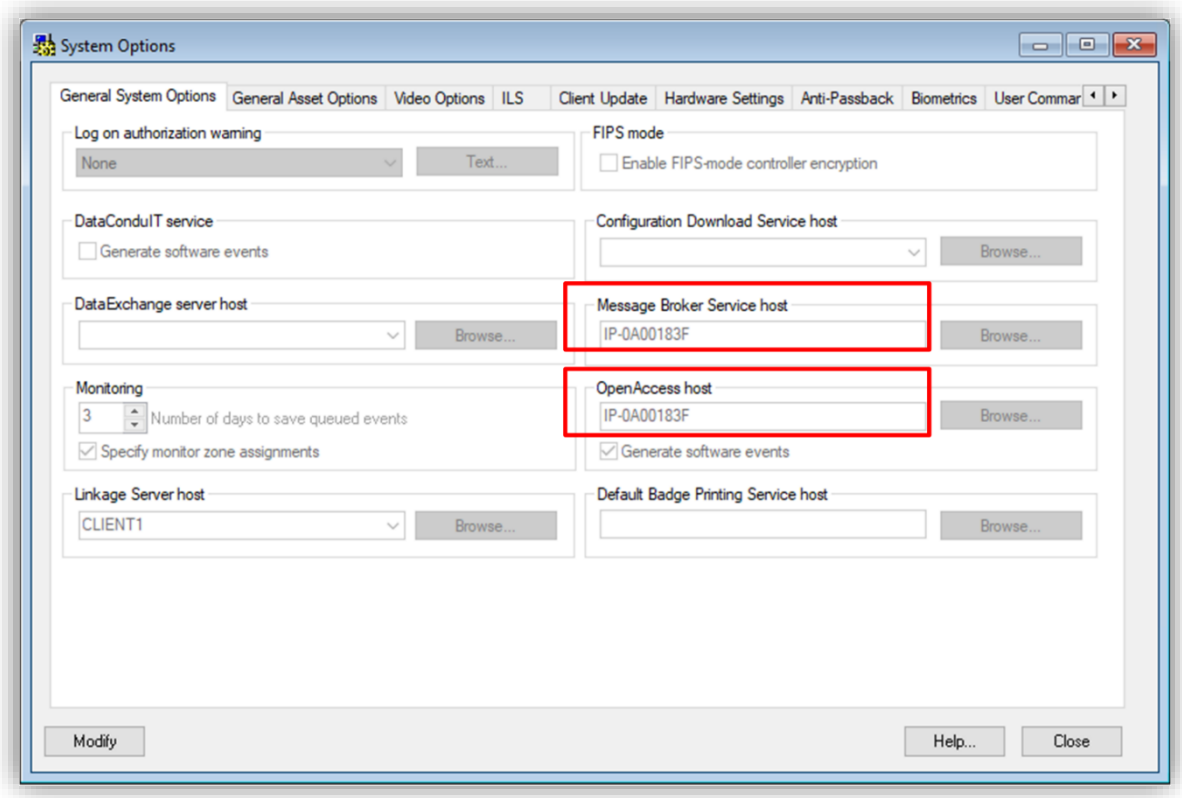


Upgrading to 4.0 from DataConduIT

XProtect Access integrations using versions 3.5 and 3.6 with Open Access connection mode, may upgrade directly to 4.0. Any XProtect Access integration currently using the DataConduIT connection mode cannot upgrade directly to version 4.0. DataConduIT is only compatible with XProtect Access version 3.4 or earlier. All systems running XProtect Access versions 3.4 or earlier and DataConduIT need to perform the following procedure to upgrade.

Obtain 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 application on the OnGuard server. Go to Start > All Programs > OnGuard (X.X), select License Administration and then login. On the left side of the web interface select "Install new license." Upload the new license file to enable the OpenAccess features.

Verify that OpenAccess is configured 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:



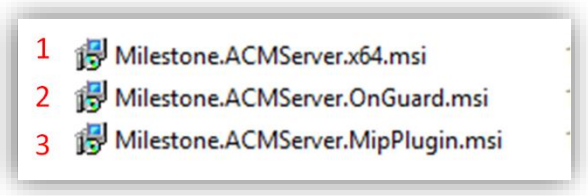
On the host(s) Confirm that the following services are all running:

OnGuard Service Name	Known Good Service Locations

LS Message Broker	On the host identified above
LS OpenAccess	On the host identified above
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.

Verify prerequisites are installed to support the 3.6 version of the OnGuard XProtect Access Plugin. Each downloadable .ZIP file available at download.milestonesys.com/lenelacm/ contains a Prerequisites folder containing any required installation programs.

Upgrade your OnGuard XProtect Access Plugin to Version 3.6. Always upgrade the ACM Server and the OnGuard ACM plugin on the OnGuard machine before upgrading the XProtect Event Server ACM MIP plugin. On the OnGuard Server, first install the Milestone ACM Server, second install the Milestone ACM Server: OnGuard Plugin. Lastly, move to the XProtect Event Server and install the XProtect Event Server ACM MIP Plugin. Here is the order of installation for all three software components of the plugin:

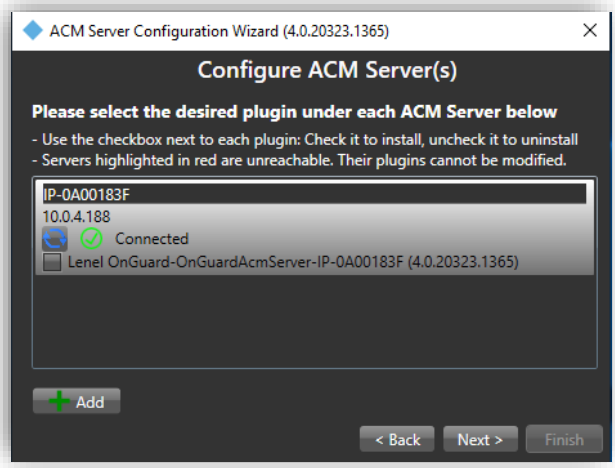


Refresh the configuration on the OnGuard XPA instance in the Management Client. Now, the active OnGuard XPA instance is configured to use OpenAccess connection mode, and is running on version 3.6. An upgrade directly to version 4.0 is supported.

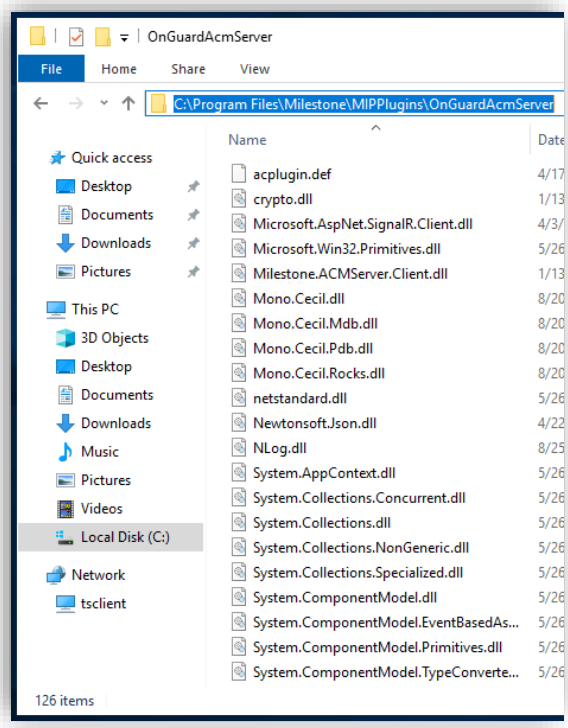
Verify prerequisites are installed to support version 4.0. On the OnGuard Server first install the Milestone ACM Server, second install the Milestone ACM Server: OnGuard Plugin. Next move to the XProtect Event Server, and lastly, install the XProtect Event Server ACM MIP Plugin. Refresh the configuration on the OnGuard XPA instance in the Management Client.

MIP Plugin Downgrades

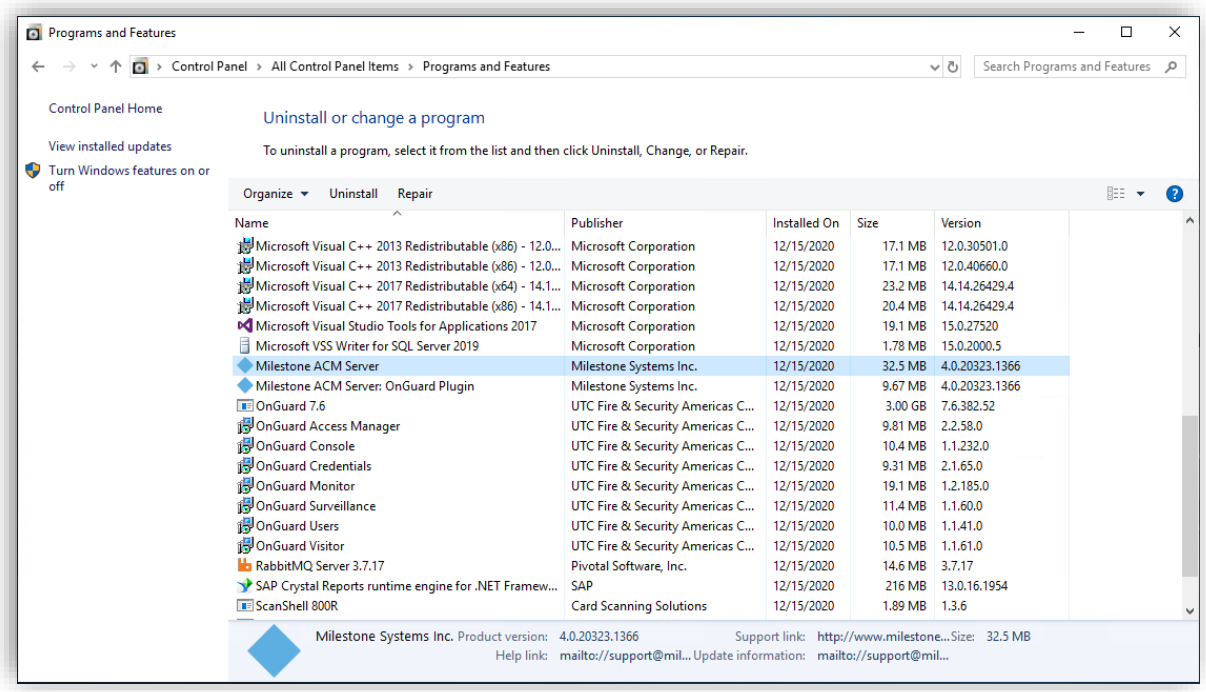
Here is the process required to uninstall the 4.0 version of the plugin. Open the Milestone ACM Server Wizard on the XProtect Event Server and remove the 4.0 version of the XProtect Event Server ACM MIP plugin. Remove the checkbox and complete the ACM wizard to uninstall.



Verify the C:\Program Files\Milestone\MIPPlugins\OnGuardAcmServer folder has been deleted from the Event Server host. If it has not been deleted, manually delete this folder and contents.



On the OnGuard server, go to Control Panel and select Programs and Features to uninstall first the Milestone ACM Server: OnGuard Plugin, and second, the Milestone ACM Server.



When uninstalling the ACM Server application on the OnGuard Server – DO NOT run the installation wizard and choose the "Remove" option. Doing this will put the system into an inoperable state. Always use the Programs and Features menu in Windows.

Re-install the 3.6 or 3.5 versions of the plugin, IN REVERSE ORDER. On the OnGuard Server, first install the Milestone ACM Server, and second the Milestone ACM Server: OnGuard Plugin. Then move to the XProtect Event Server and install the XProtect Event Server ACM MIP plugin. Restart the Event Server service and run the ACM Wizard on Event Server to add the 3.6 or 3.5 profile.

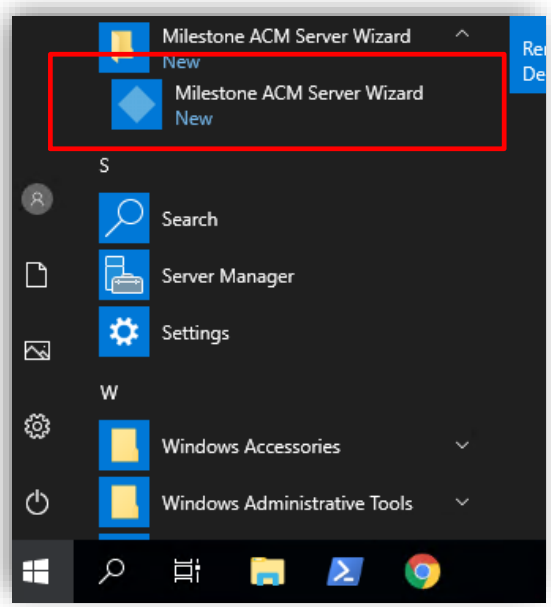
Open the XProtect Management Client, go to the OnGuard XPA instance and modify any field in the General Settings menu. It is recommended to modify the Description field if no changes are necessary. Save the settings to refresh the connection properties. Refresh Configuration within Management Client to finalize the downgrade procedure.

XProtect ACM MIP Plugin Configuration

ACM Server Wizard

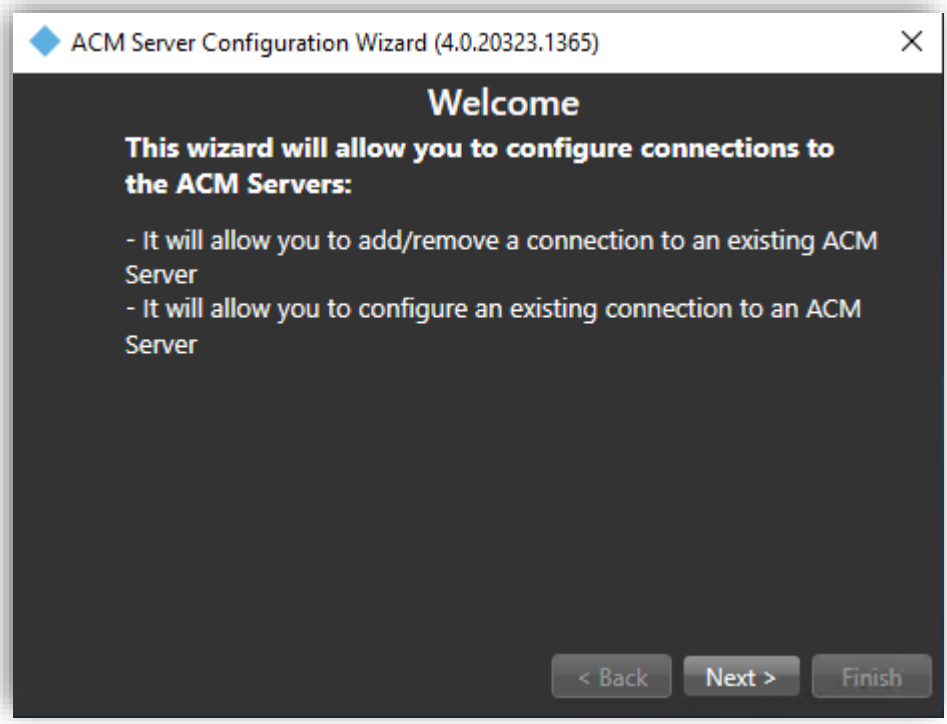
Once all three software programs have been installed (see Installation section), it is time to configure and install the ACM MIP Plugin. There is a wizard used to connect and configure the XProtect ACM MIP Plugin package.

Go to the start menu on the XProtect Event Server host, open the Milestone ACM Server Wizard folder and select the Milestone ACM Server Wizard application.

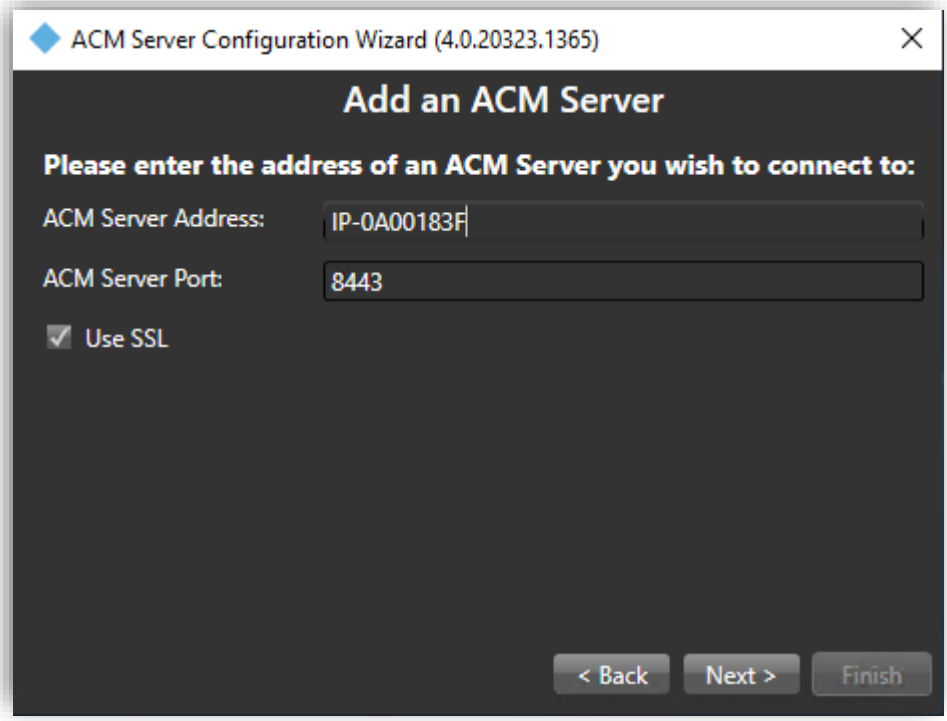


Installing an ACM Server

Once you start the wizard application you will see the following:

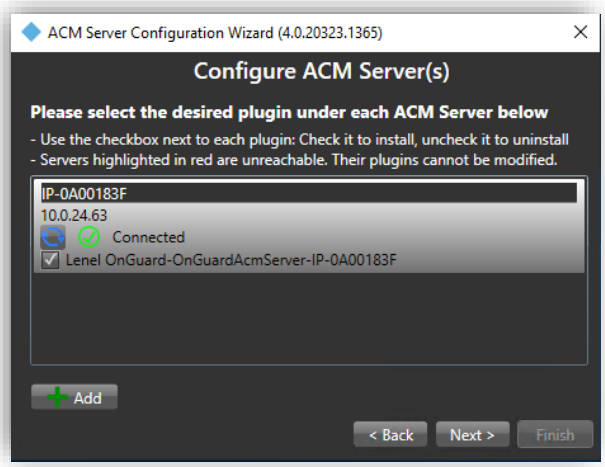


Click next to provide the IP address / host name of the OnGuard server on which the ACM Server software was installed. If you used an integration server as described in Distributed deployment options, use the IP Address or host name of the integration server instead.

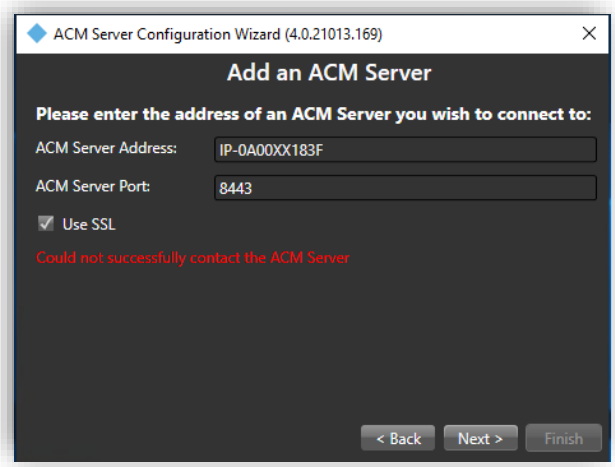


After you enter the IP address or host name and click next, the wizard validates the connection to the ACM Server. The green checkmark confirms a successful connection. However, a red x means it failed to connect to the provided address. The wizard will not allow you to proceed without a valid connection.

Valid Connection

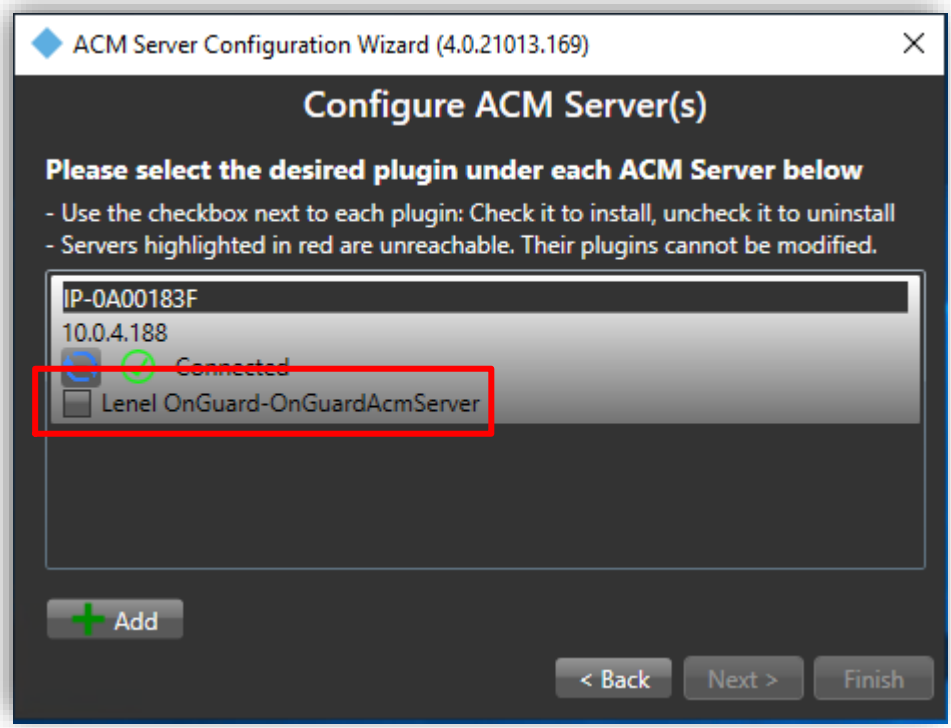


Failed Connection

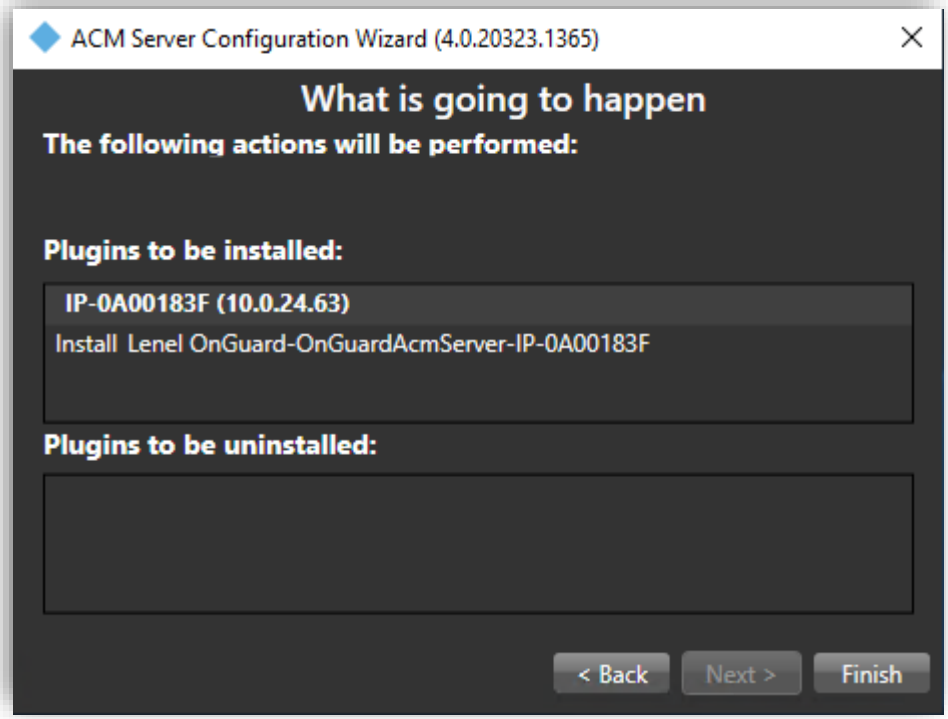


Note that the most common causes of the wizard not being able to connect to the provided server is that 1) Server hostname/address information is incorrect, or 2) the ACM Server is running with insufficient privileges.

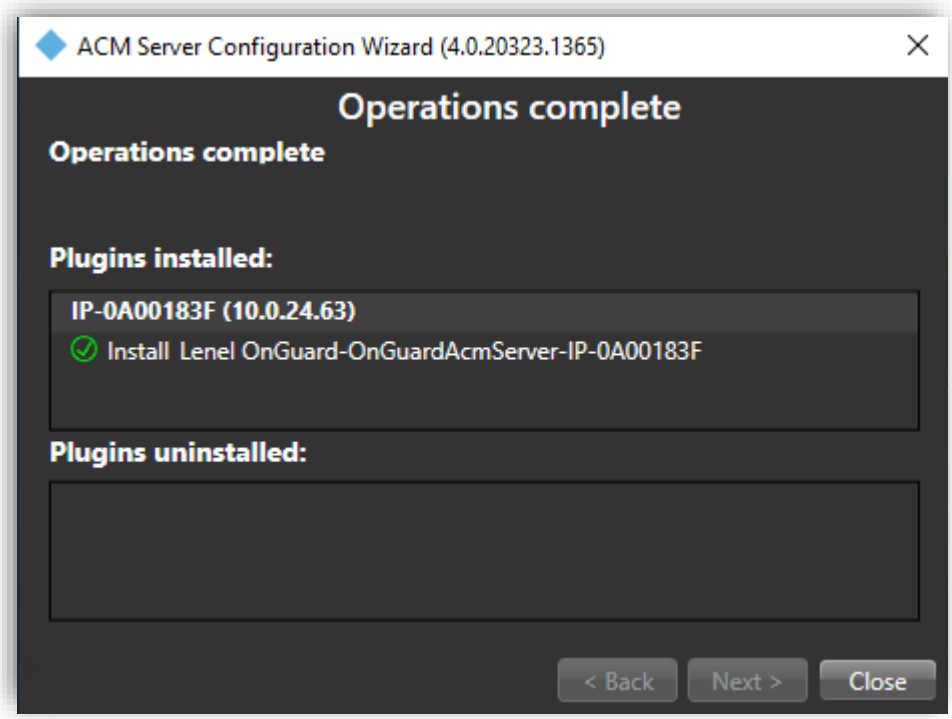
Once the connection is made a checkbox will appear under the server name. It represents the ACM server plugin installed at that address.



Check the box and press next to install a MIP plugin on the XProtect Event Server host. The next step will confirm the installation. Click finish to complete the installation.



Once the installation is complete, the wizard will display a green checkmark.

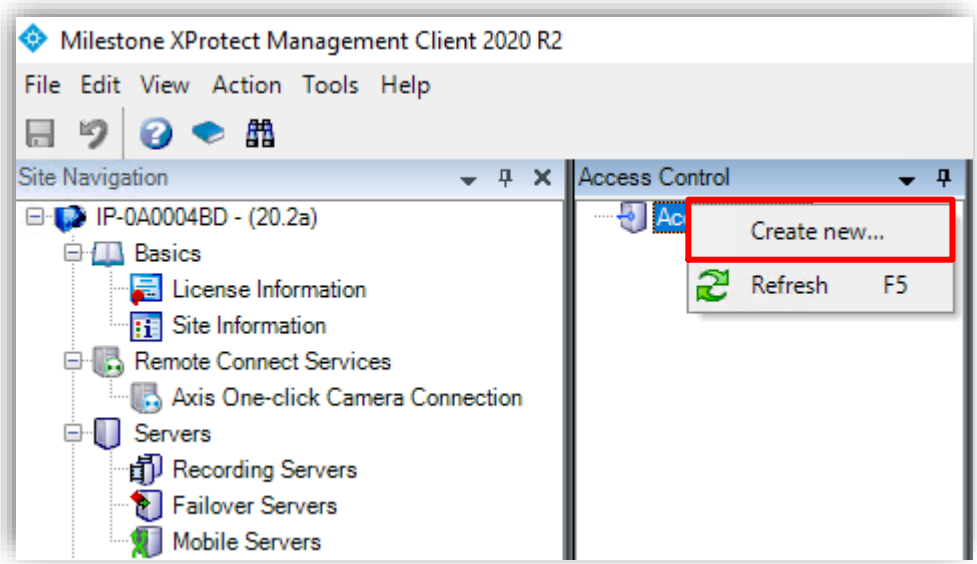


You have successfully installed the ACM Server: XProtect MIP ACM Plugin.

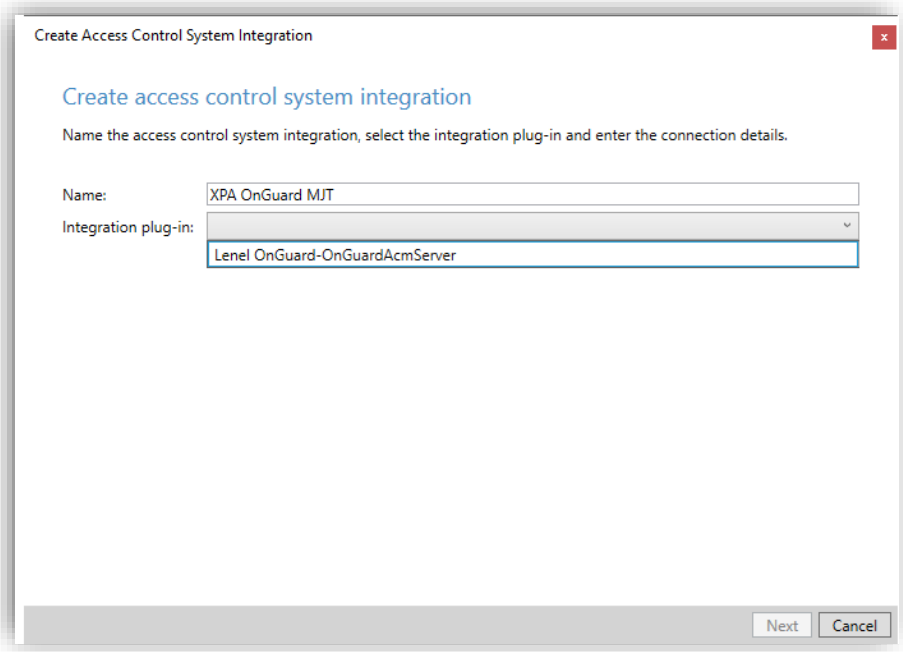
XProtect Management Client Configuration

XPA Instance Creation Wizard

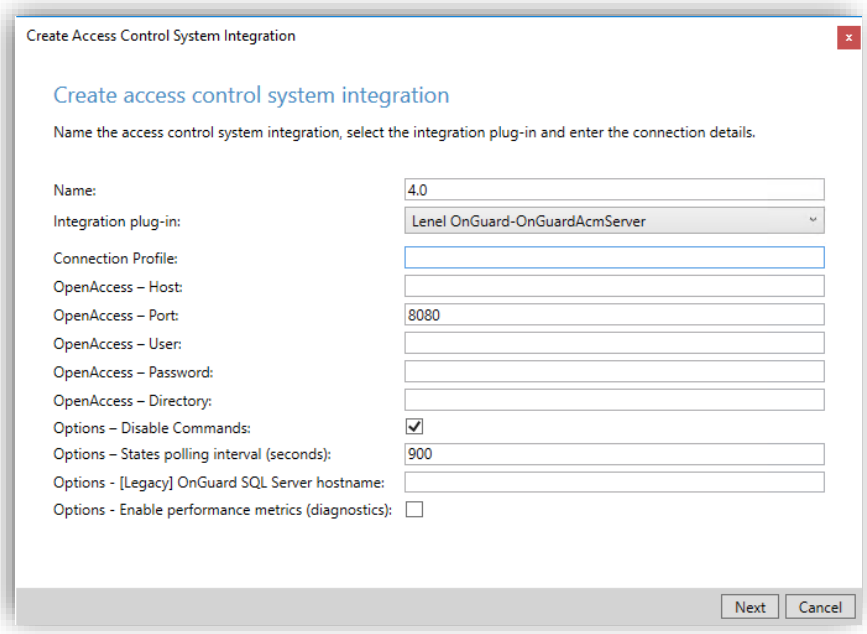
After the MIP ACM Plugin is installed and configured on the XProtect Event Server, the Access Control instance can be created in the XProtect Management Client. Right-click on the Access Control Root Node and select Create new... to begin the wizard.



Enter a name for the instance and select the Integration plug-in. Note that you will find a plugin named Lenel OnGuard-OnGuardAcmServer.



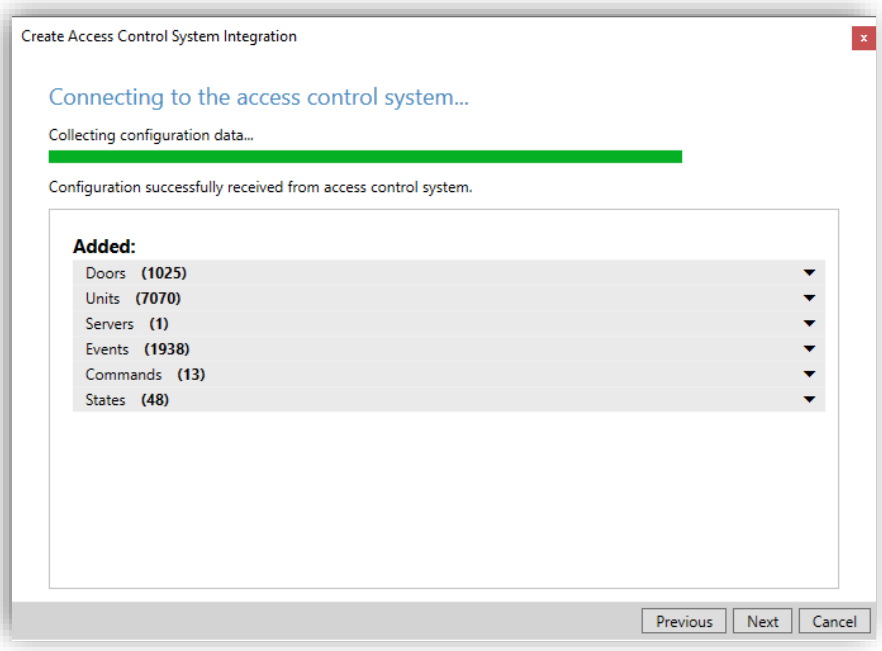
After naming and selecting the plugin there are a set of required credentials, parameters, and options to complete. These are required to define the connection to the OnGuard server. All the properties used for all versions of OnGuard are shown in the Management Client wizard.



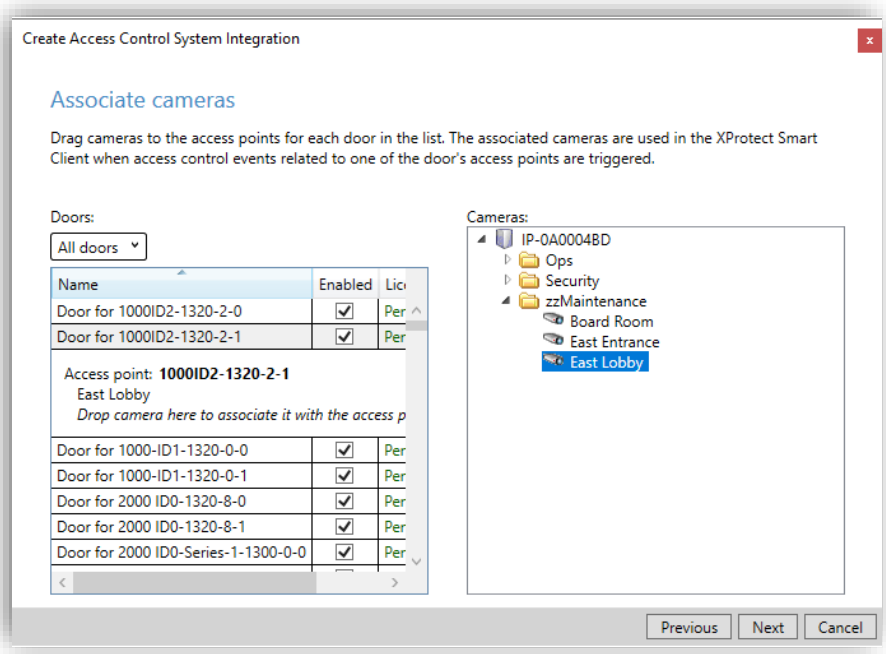
Fields required to establish the connection are listed below.

Empty Field Names	Required Values
Connection Profile	Host name of OnGuard Server
OpenAccess - Host	IP address of OnGuard Server
OpenAccess - User	SSO user created to login into ACM Server
OpenAccess - Password	Password for SSO user
OpenAccess - Directory	Directory for SSO user. Can be blank for local users.

After the connection is created, the wizard will import data from the OnGuard server. This includes Doors, Units, Servers, Events, Commands, and States. Click Next.



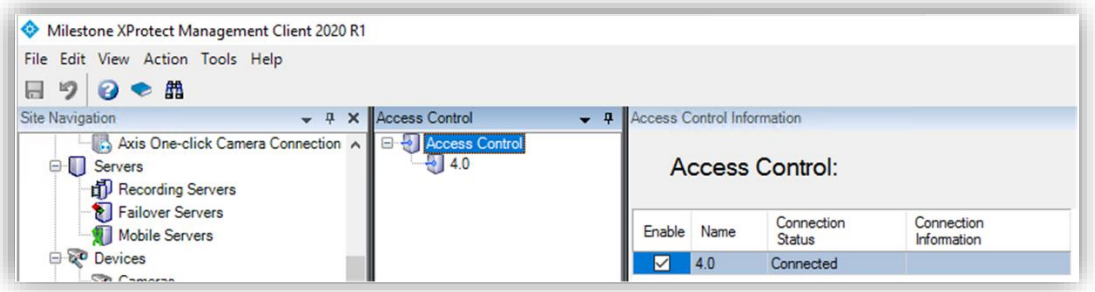
On the following page you can associate doors with cameras. This is done by selecting a camera and dragging it to one of the imported doors. Click Next after association of doors and cameras. The configuration will be saved, and the wizard is complete.



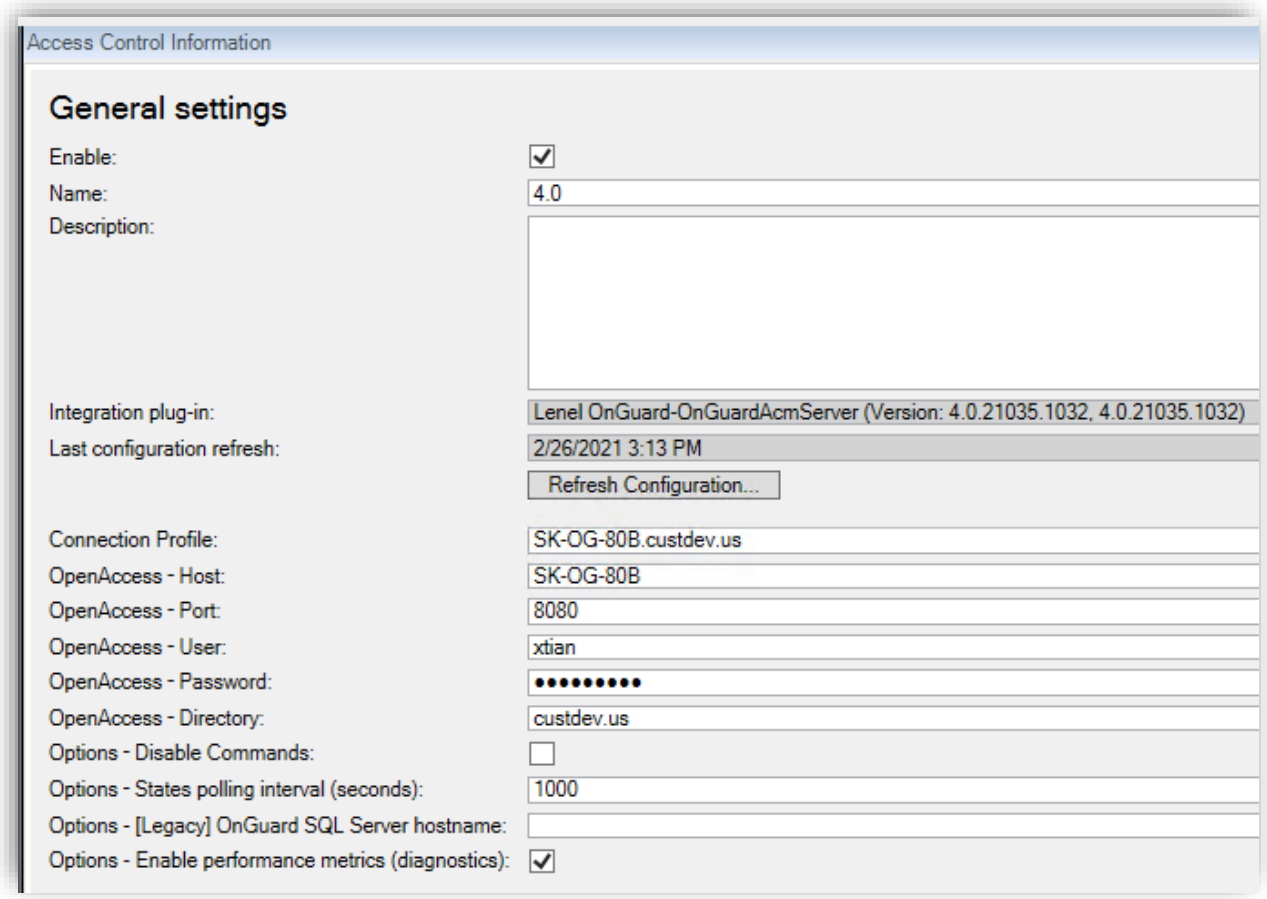
milestone

XPA Instance Status & Properties

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

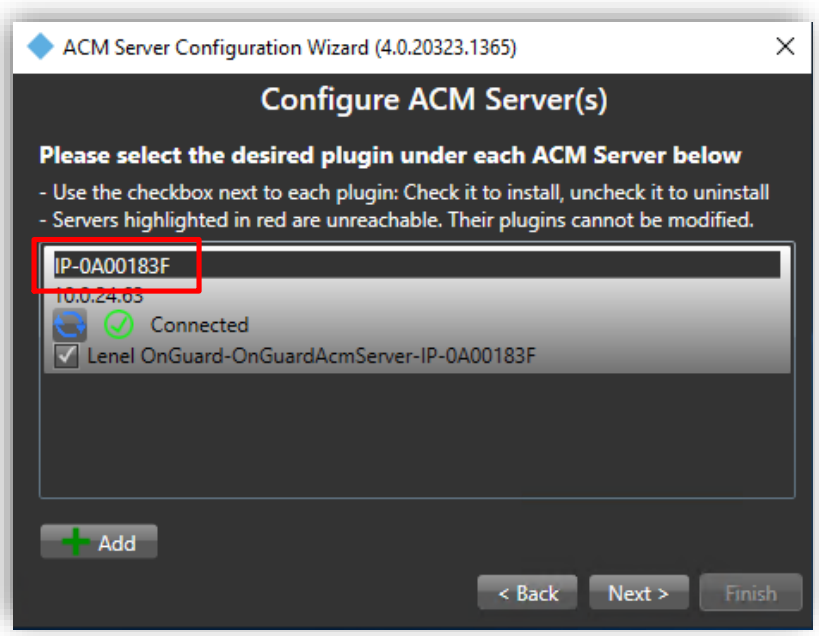


Click on your OnGuard XPA Instance to view or modify the properties of the connection.



Below, the properties are listed.

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 XProtect Event Server ACM MIP Plugin.
Last configuration refresh	Displays the date and time the last system configuration refresh was performed.
Operator login required	Not selected by default. This option should be selected to enable the personalized login feature.
Connection Profile	Should be set to the same as was shown in the ACM Wizard when you added the ACM server, and may include a domain. For example: 
OpenAccess – Host	Host name or IP address of the machine hosting the OnGuard OpenAccess service.
OpenAccess – Port	The port the OnGuard OpenAccess service is listening on. 8080 is the default port.
OpenAccess – User	An OnGuard administrative user to log into the OnGuard OpenAccess web service. This user should have access to all hardware, cardholders, etc in the system. Windows user account if using Directory users, OnGuard internal user account if using internal directory.
OpenAccess – Password	The password of an OnGuard user to use to log into the OnGuard OpenAccess web service.
OpenAccess – Directory	The name of the OnGuard directory to be used when loging into the OnGuard OpenAccess web service. If left blank, the OnGuard internal directory will be used.
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 60 seconds. Frequency of status updates retreived for AC hardware devices. Increase this value to provide 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 does not require a SQL server hostname to establish the connection.
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

Personalized login is an optional feature of XProtect Access. Personalized login takes advantage of OnGuard segments to divide system users, access control hardware, events and alarms into groups, or "segments."

When a user logs into Smart Client, personalized login adds a second login into OnGuard. The user presents valid OnGuard credentials, and the Smart Client's XPA features will only work with access control hardware, events and alarms within that user's segment.

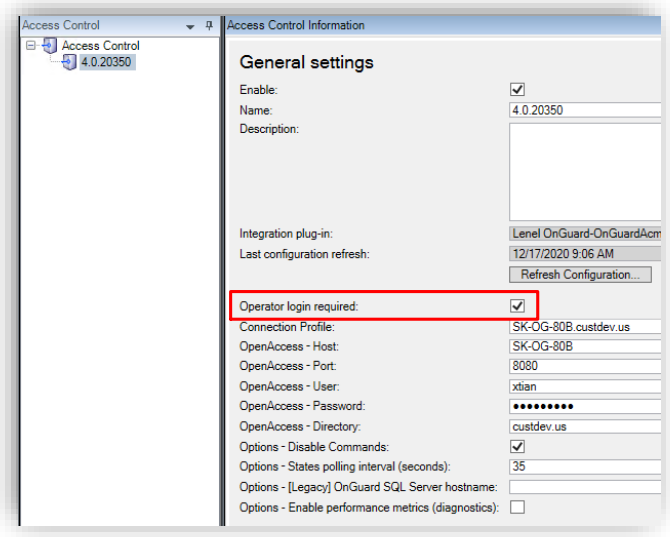
Personalized login manages two configurations. First, is the global configuration used by the Management Client. Second, is the personalized configuration used in the Smart Client. Personalized configurations are subsets of the global configuration. This helps ensure accurate event handling, command execution...etc.

Personalized login has specific requirements:

- OnGuard 7.4 or higher
- XPA 3.5 or higher

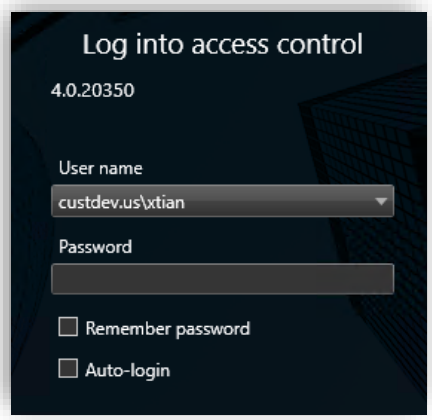
Enable/Disable Personalized Login

Enabling/disabling personalized login for a specific access control plugin is done in the Management Client. The option is located in the General setting menu and is titled "Operator login required:"



Smart Client Personalized Login

A second Log into access control dialog is required. It occurs immediately after the standard Smart Client login dialog.



OnGuard requires three pieces of data:

1. directory
2. user name
3. password

The XProtect Smart Client dialog only has boxes 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 allows special non-alphanumeric characters, control characters, and spaces in directory names. Use of these characters is NOT COMPATIBLE with XProtect. If these types of characters are included in the OnGuard directory, authentication will fail.

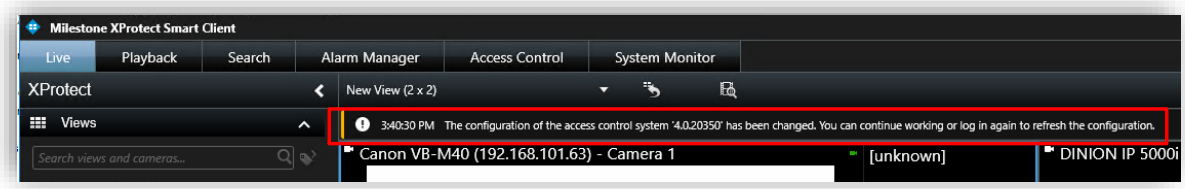
After entering the directory\user name and password, the XProtect Smart Client validates the credentials. If you click Skip this step, the Smart Client is opened without using personalized login, and no XPA features are available in the Smart Client. After authentication with OnGuard, Smart Client loads a personalized configuration. The Smart Client will only display access control information from the same segment of the user account that logged in during the personalized configuration login dialog. This includes:

- Alarms related to hardware in their segment.
- Events related to hardware in their segment.
- Devices in the map element selector that are in their segment.

Refreshing Personalized Configurations

The XProtect Event Server stores personalized configurations for XProtect Smart Client users. Stored personalized configurations are cleared when the Event Server restarts. When the global configuration of the XPA instance is refreshed, the Event Server updates all stored personalized configurations.

After the global configuration is updated all open Smart Clients using a personalized configuration will have the following info message displayed.



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

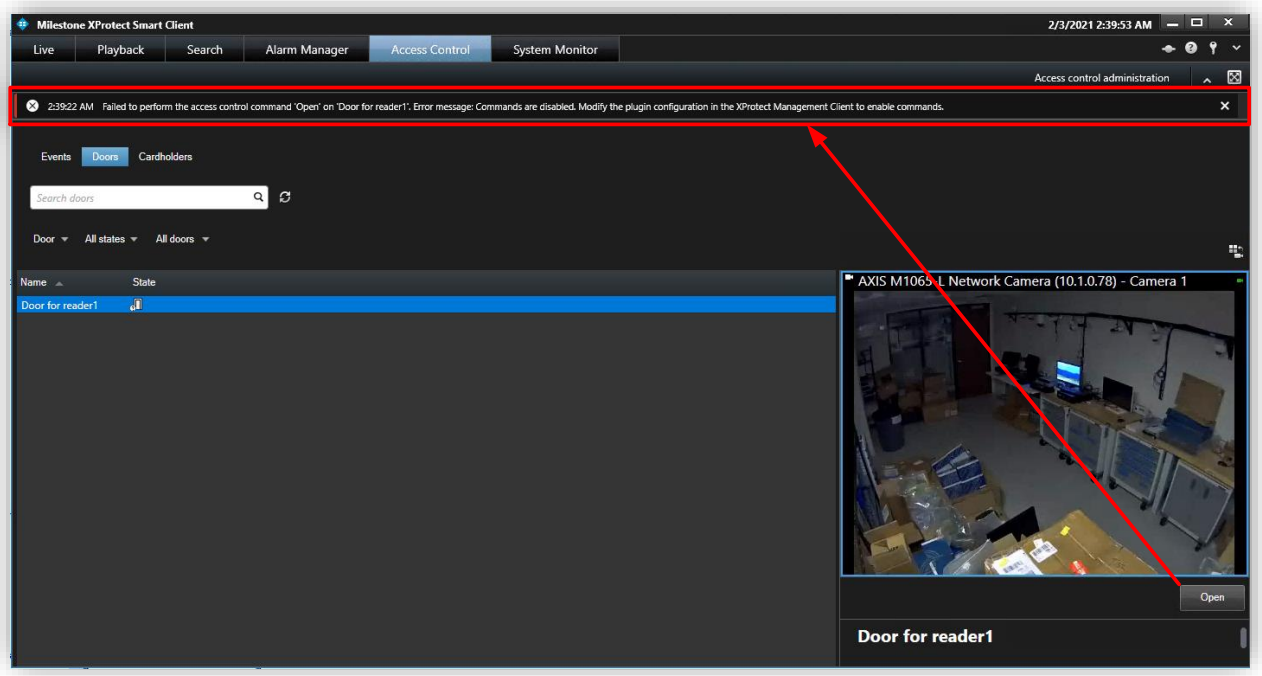
Commands:

Commands are used in the XProtect Access OnGuard integration to 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" check box.

If Commands are disabled, none of the functionality will work, however it is still possible to view Command buttons in the Smart Client and create rules in XProtect which use Commands. These rules will

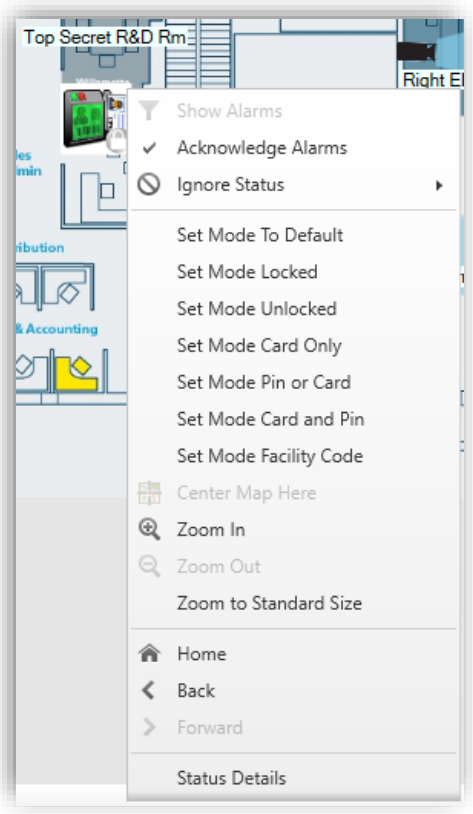
validate, and the buttons can be clicked, but nothing will happen. In the Smart Client users will receive the following error message:

*"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."*

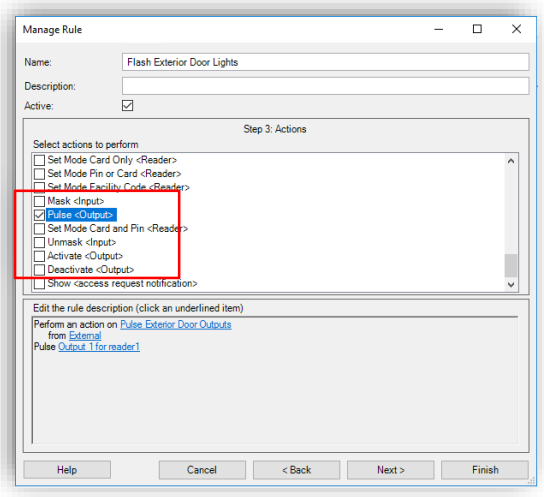


Commands trigger state changes in the access control hardware devices. Commands can be triggered in four ways with the XProtect Access OnGuard integration. The XProtect Rules system can be used to trigger Commands. Access Request Notifications can include commands. Any location in the Smart Client where doors are visualized, such as the Access Monitor or the Access Control workspace, can contain Command buttons. And lastly, the Map interface within the XProtect Smart Client can include Access Control device icons which can be used to trigger commands.

The following are the devices and their supported commands.

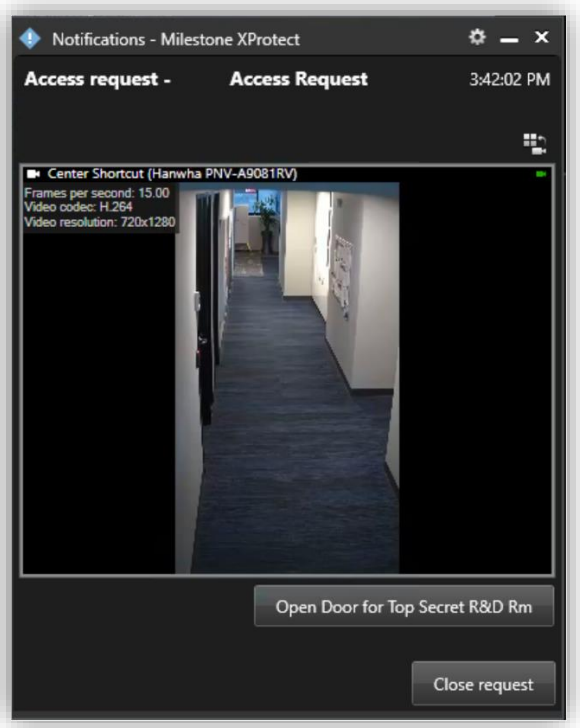
Readers:	• Set Mode To Default • Set Mode Locked • Set Mode Unlocked • Set Mode Card Only • Set Mode Pin or Card • Set Mode Card and Pin • Set mode Facility Code	

Set Mode Commands for readers will change the type of authentication mode the reader can respond to. For example: a rule could be used to switch readers into unlocked mode during business hours.

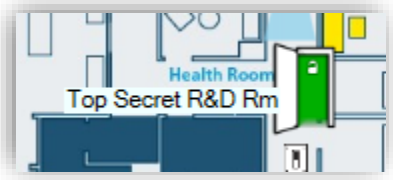
Reader Inputs:	• Mask • Unmask	
Reader Outputs:	• Activate • Deactivate • Pulse	

Reader inputs can be masked or unmasked. When an input is masked, status of that input is not reported or saved in the OnGuard system. When it is masked, the reader input has a "mask" icon attached

to it on the Smart Client Map. Unmask removes the mask on the icon and allows the status of that input to be reported and saved within OnGuard. Reader outputs can be activated, de-activated and pulsed using the respective commands. The Pulse Command will activate the output temporarily, then deactivate it. An activated output will have a red circle icon attached to it when viewed on the Smart Client Map.

Doors:	• Open	

Doors can be opened via the Command. When the door is opened, the door icon animation displays this status on the Smart Client Map.



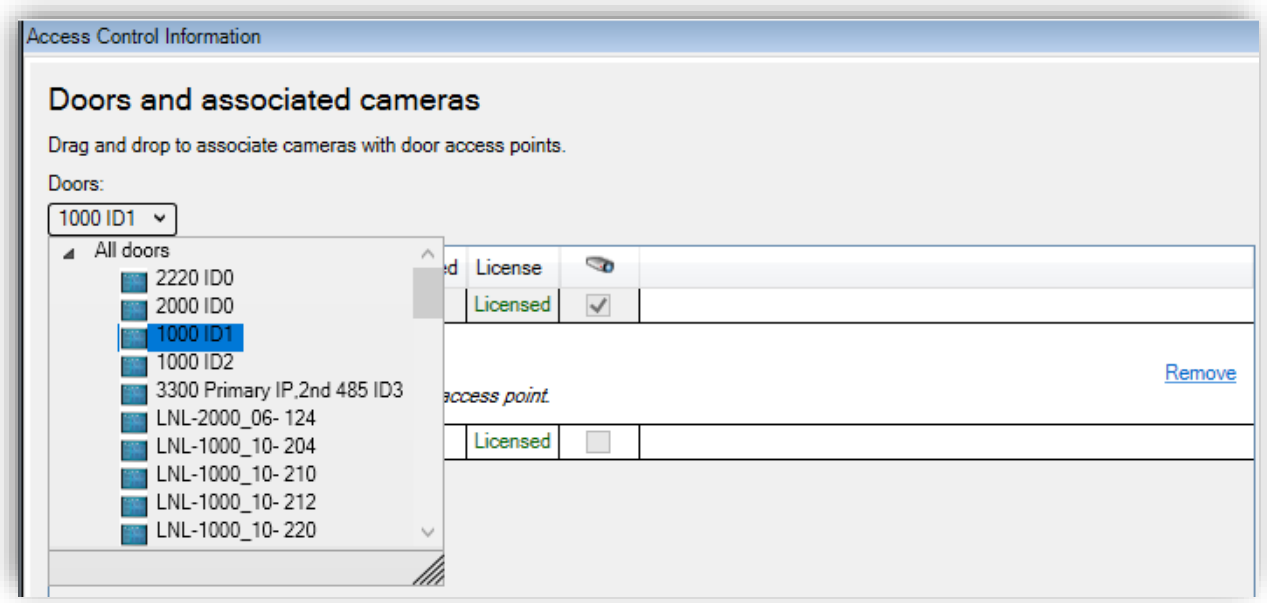
Administrative Configuration

Door & Camera Association

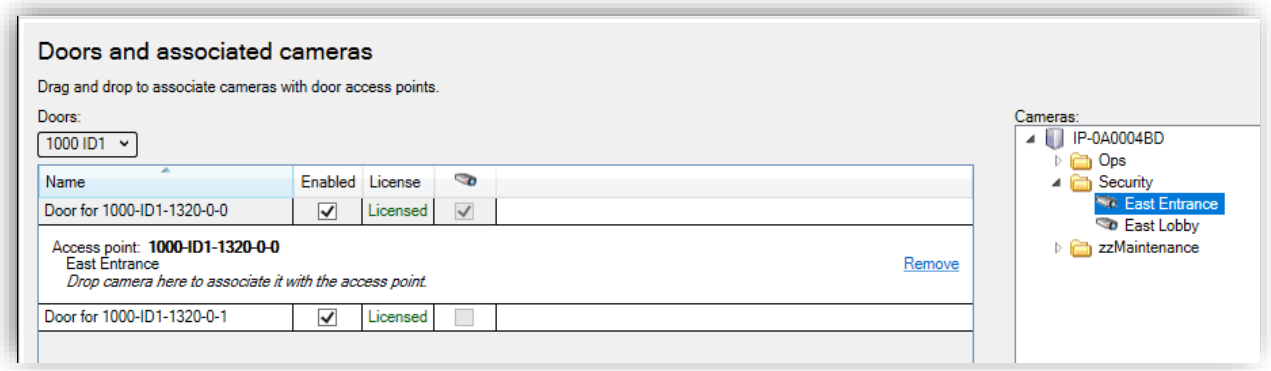
In the Doors and Associated Cameras menu of the XPA Instance it is possible to verify the status of all connected doors, and create, reassign, and remove the association between cameras and doors.

Doors require associated cameras to view live and recorded video - and listen to or play audio through any XProtect client application that supports visualization of doors.

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



Click on a door. Under it all associated cameras are listed. 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. Click the Remove link 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 greatly minimizes the number of individual alarms and rules that need to be programmed.

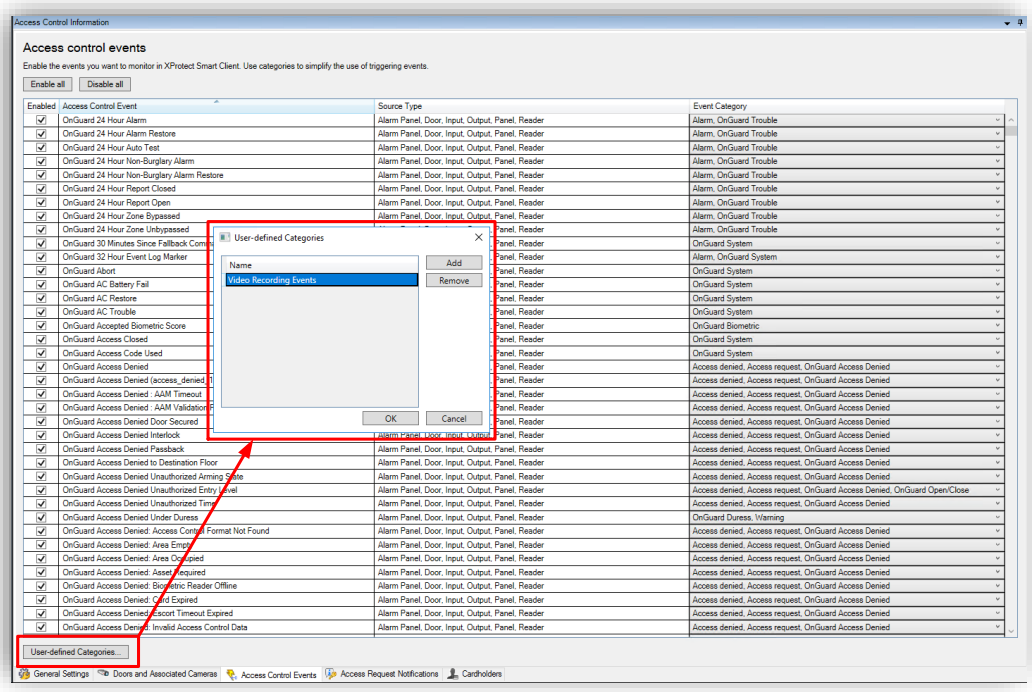
To generate XProtect alarms or rule-based actions triggered by any one of a group of individual OnGuard events, the events must be categorized. For example, the integration can be configured to start recording video from associated cameras based on any number of unique OnGuard hardware events: "Door Forced," "Denied, Badge Not in Panel," and "Access Denied Unauthorized Entry Level." Chosen events are placed in the same category, and then a rule is created to start recording based on the receipt within XPA of any event in that category.

The categories are:

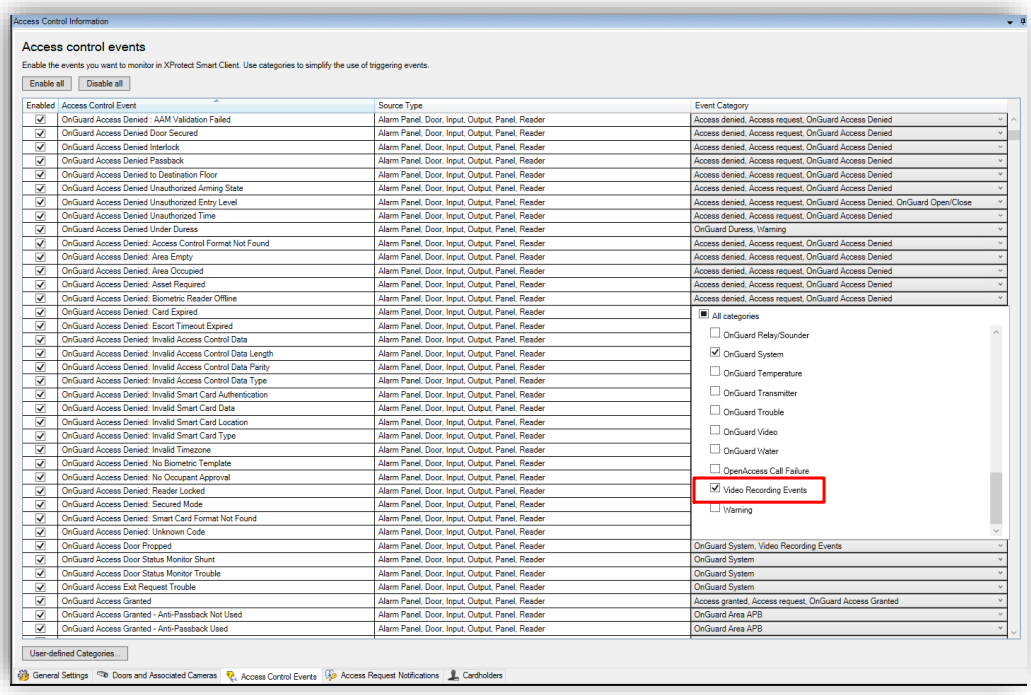
Default XPA Events	OnGuard Events	Custom Events
• Access Granted • Access Request • Access Denied • Alarm • Error • Warning	• OnGuard Access Denied • OnGuard Access Granted • OnGuard Area APB • OnGuard Asset • OnGuard Biometric • OnGuard Burglary • OnGuard C900 • OnGuard Digitize • OnGuard Duress	• User Defined Category...

	• 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	

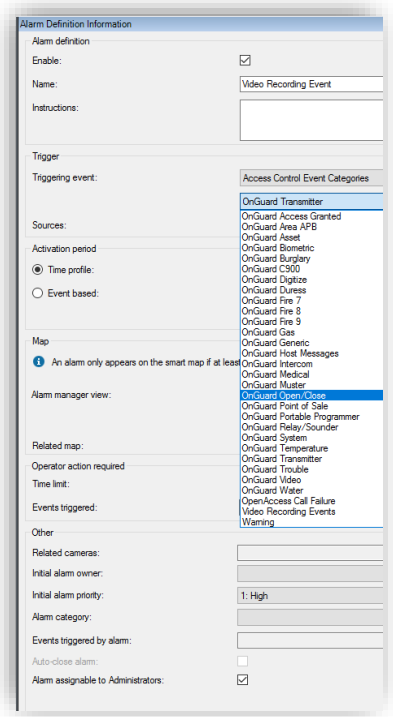
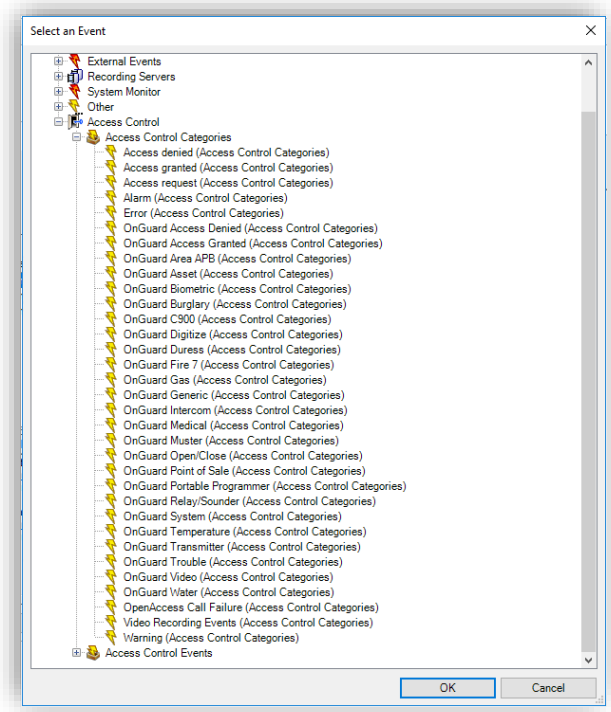
To create a User-defined Category, there is a User-defined Categories button on the bottom left corner of the Access control events menu. Click the User-defined Categories button to create your own custom event category.



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



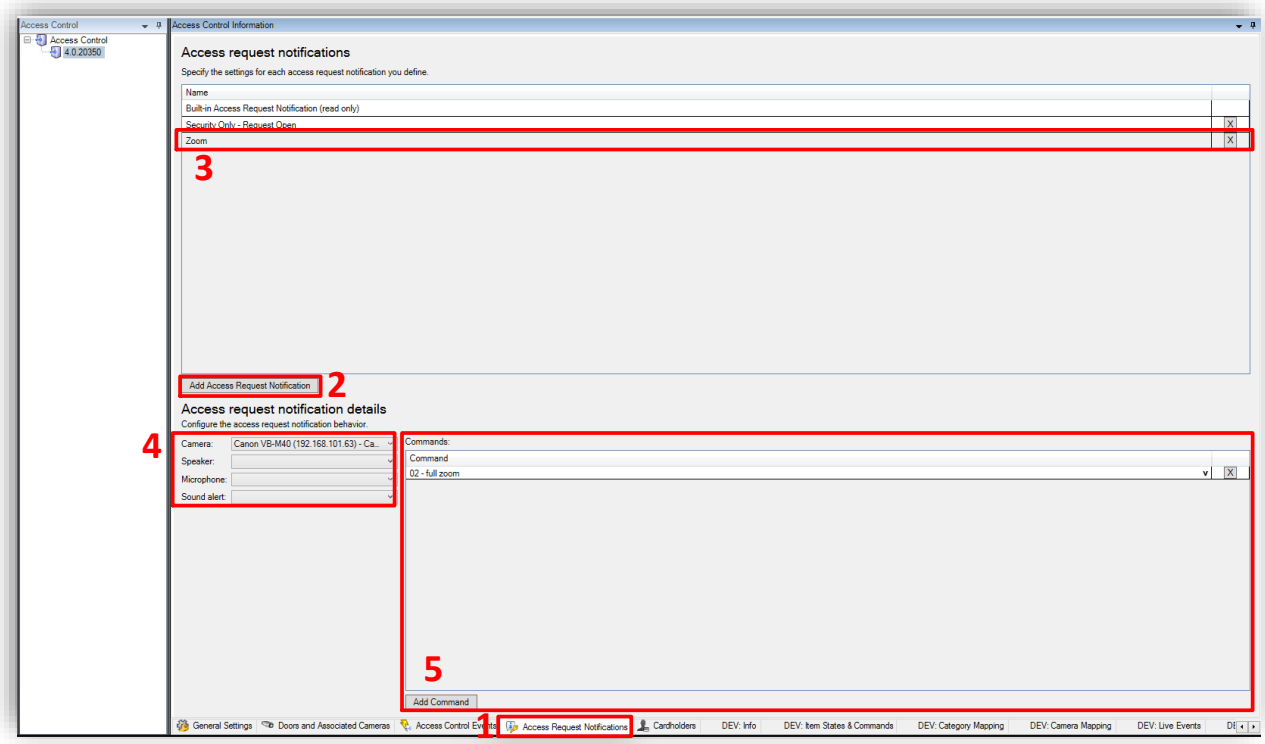
Alarms and Rules in XProtect are triggered using any category of event.

Alarm Access Control Categories Event list	Rule Access Control Categories Event list
	

Access Request Notifications

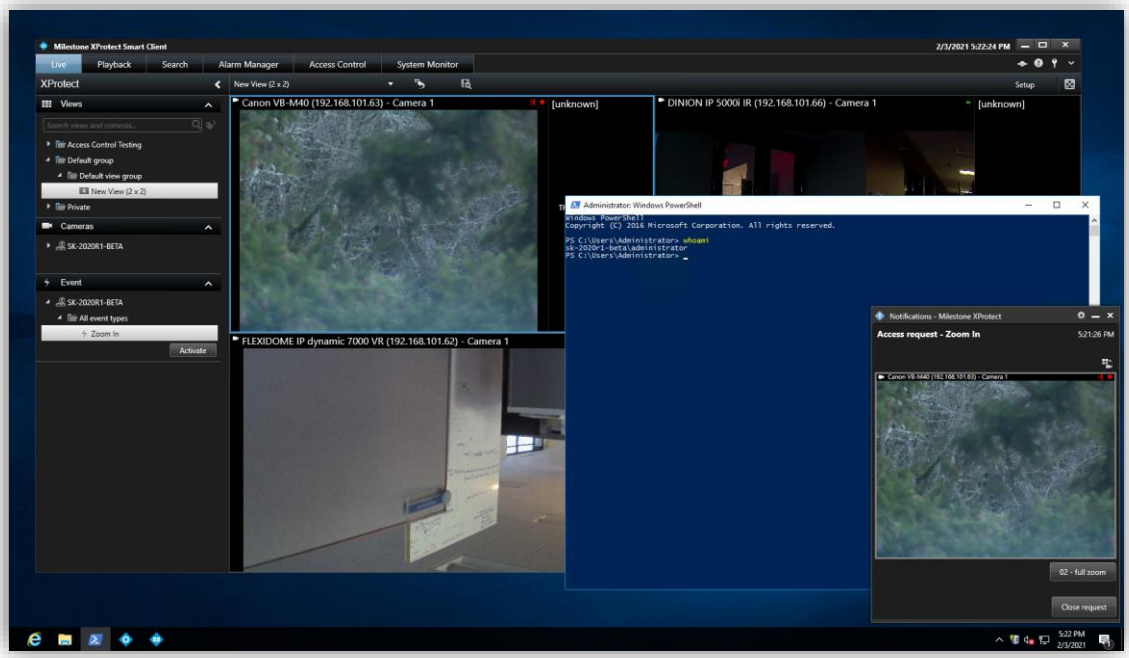
Access Request Notifications are pop-up notifications which appear in front of all other desktop applications for all users logged into the Smart Client with access to view XPA features and devices. These notifications can be customized in the Access Request Notifications menu. The XPA integration includes a Built-in Access Request Notification.

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.



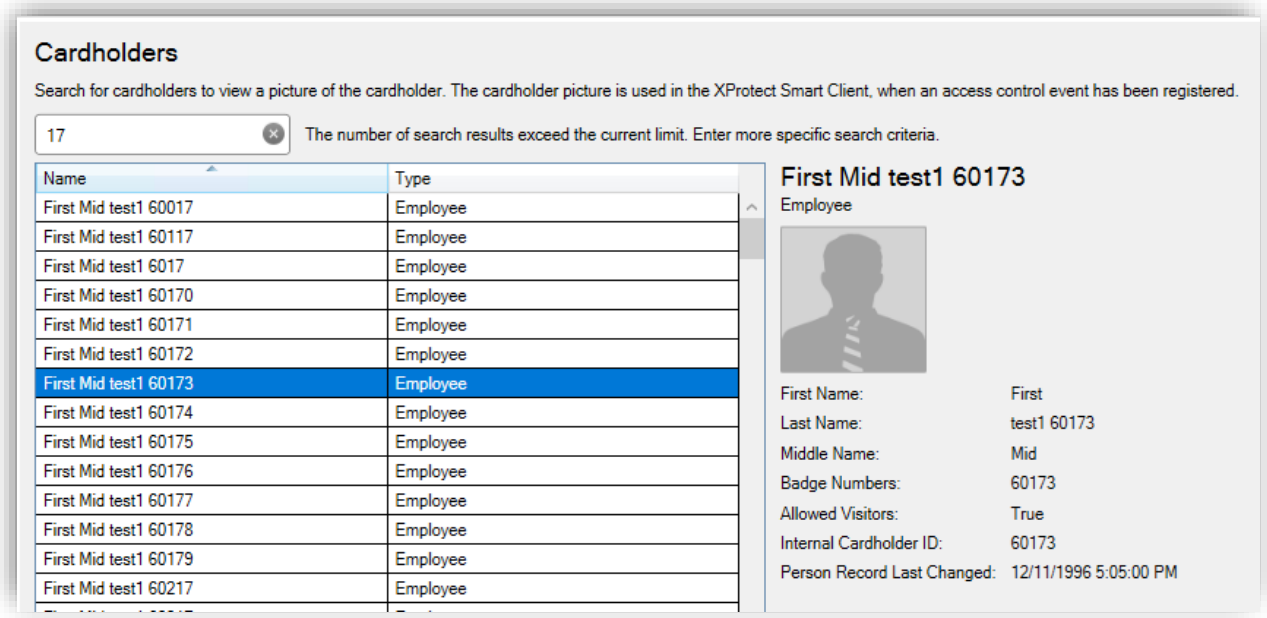
When the notification pops up on the desktop a sound will play if you choose to include a Sound alert. The Built-in Access Request Notification does not include a Sound alert.

Access Request Notifications can be used to trigger pop up notifications from within the XProtect rules system, and the notifications do not need to be connected to access control hardware devices.



Searching for Cardholders

All “active” cardholders in the OnGuard system are imported from the connected OnGuard server. “Active” cardholders have one or more badge(s) with a status of “active.” Search for cardholders in the Cardholders menu of the XPA 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, Badge numbers...etc., are controlled within the OnGuard database.

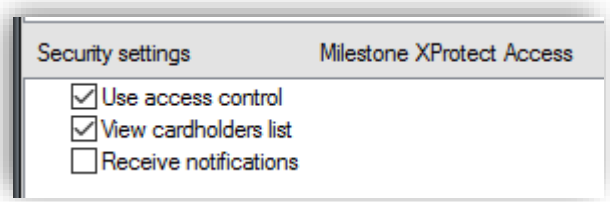
Client Profiles & Roles

Smart Client Profiles and User Roles in XProtect allow administrators to control the features available in the XProtect Smart Client.

Smart Client Profiles allow control over the visibility of access request notifications. Roles allow control over access control globally, visibility of the cardholder list, and access request notifications. For example, if a user cannot receive access request notifications it could be disabled in both the Smart Client Profile that user is assigned, or in their Role.

To manage Smart Client Profiles – open the Management Client, expand Client and select Smart Client Profiles. The Access Control menu contains the setting for notifications.

To manage Roles – open the Management Client, expand Security and select Roles. Select the role to manage and click on the Access Control menu to adjust the available settings.



Smart Client Features

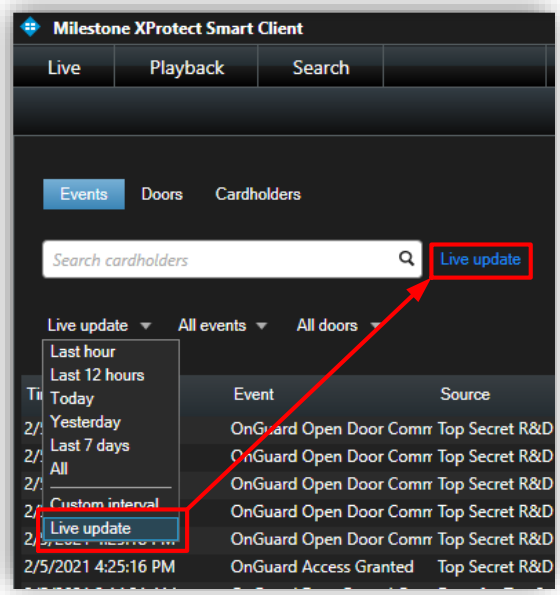
Access Control Workspace

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

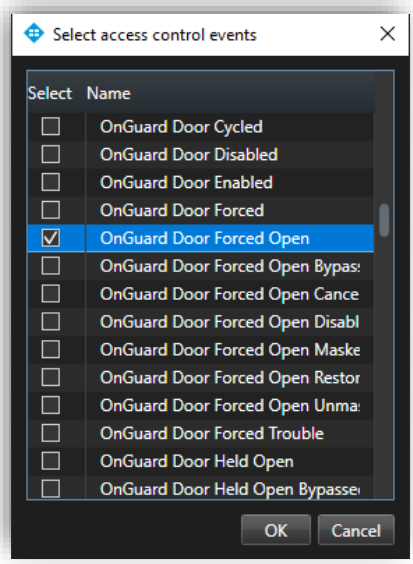
This workspace is used to search and filter Events, Doors and Cardholders.

Events:

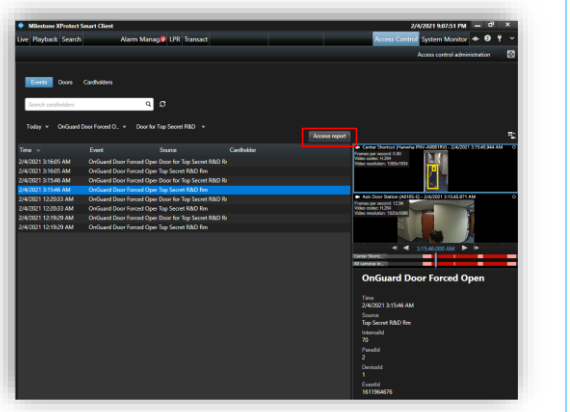
Choose a time range, including a custom time range, or live update. Choose the Live update time range to view a real-time display of access control events.

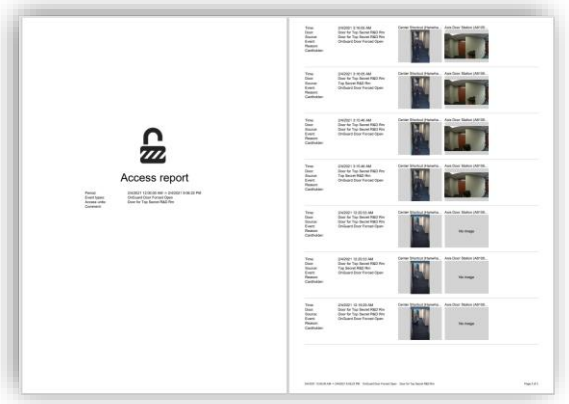


Filter for specific events including custom events and all integrated OnGuard events. Open the All events list and select the "Access control event..." option to open the Select access control events window. Choose a specific OnGuard event from this list.



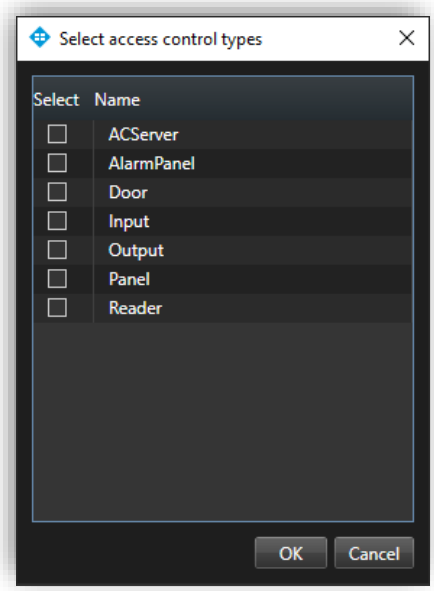
Filter for specific hardware devices. Click the Access report button to create a PDF file of the events in the current list. In the Access report window: name the report, choose a destination to save the report, include comments, and select the option to include snapshots.



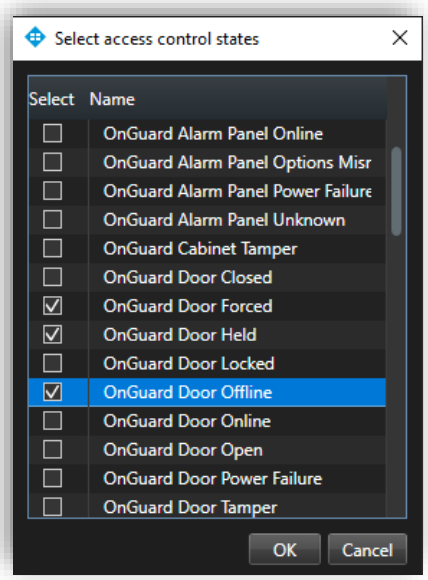


Doors:

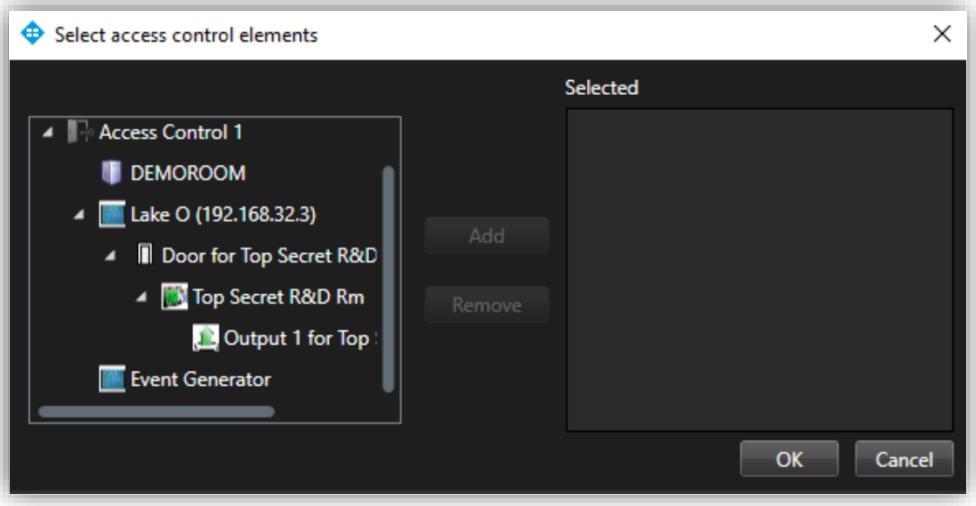
Open the Door list and select the type of access control hardware to display. Choose the “Access control type...,” option to open the “Select access control types” window. “Door” is the default option for this list, however, servers, panels, and any type of access control hardware in the system can be selected.



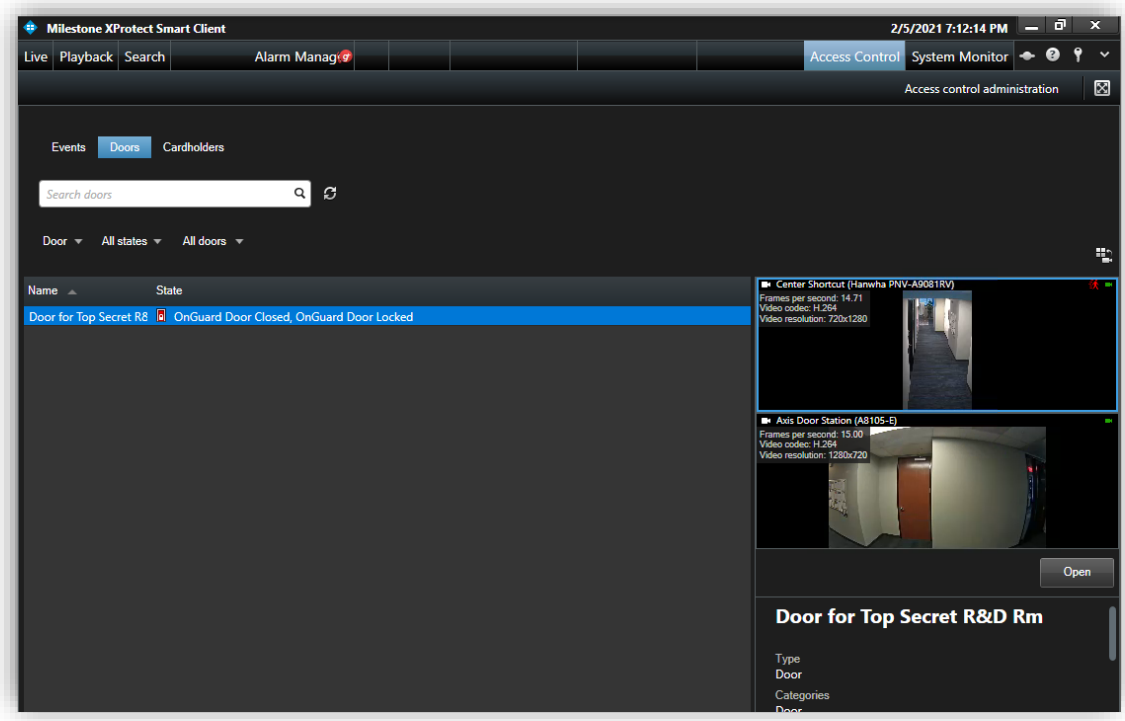
Open the All states list to filter hardware by status. Choose the “Access control state...,” option to open the Select access control states window and select from the list of all available OnGuard hardware states.



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. Expand the directory, find the hardware device(s), and add them to the selected list.

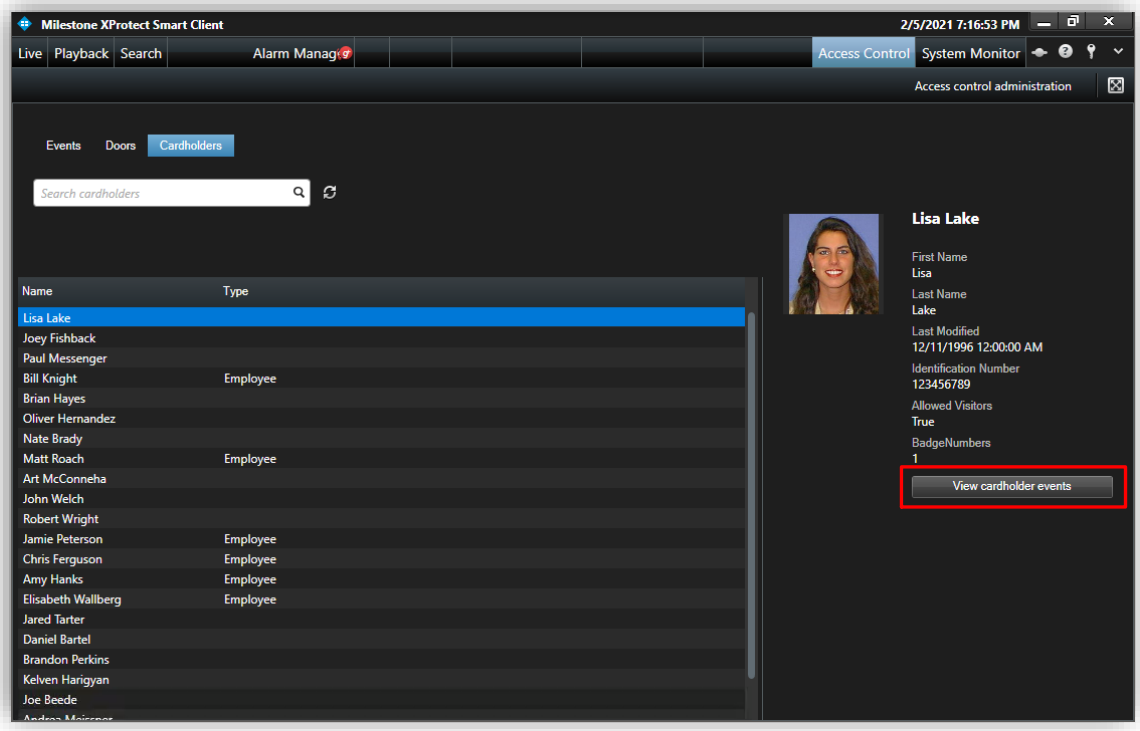


Select a Door in the list to see video from associated cameras, view door status information, and Command buttons available for that door.



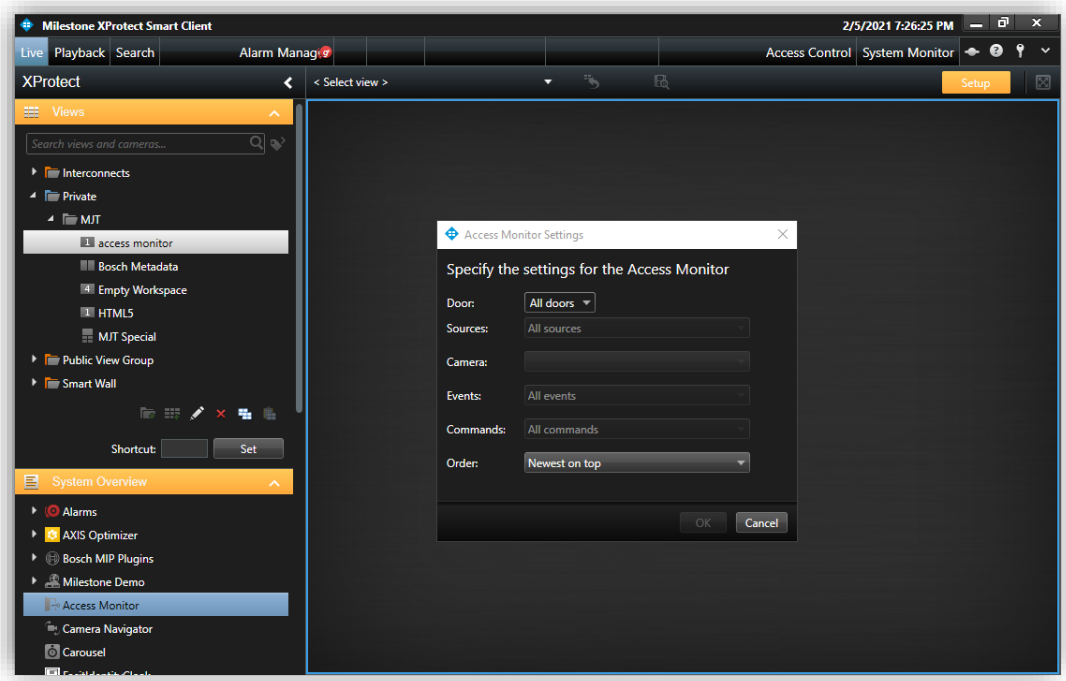
Cardholders:

By default, all cardholders in the system are displayed in the list. Filter for specific cardholders by typing into the search field. Select a cardholder to view their data. Click the View cardholder events button to switch to the Events list automatically filtered to display events only from the chosen cardholder.

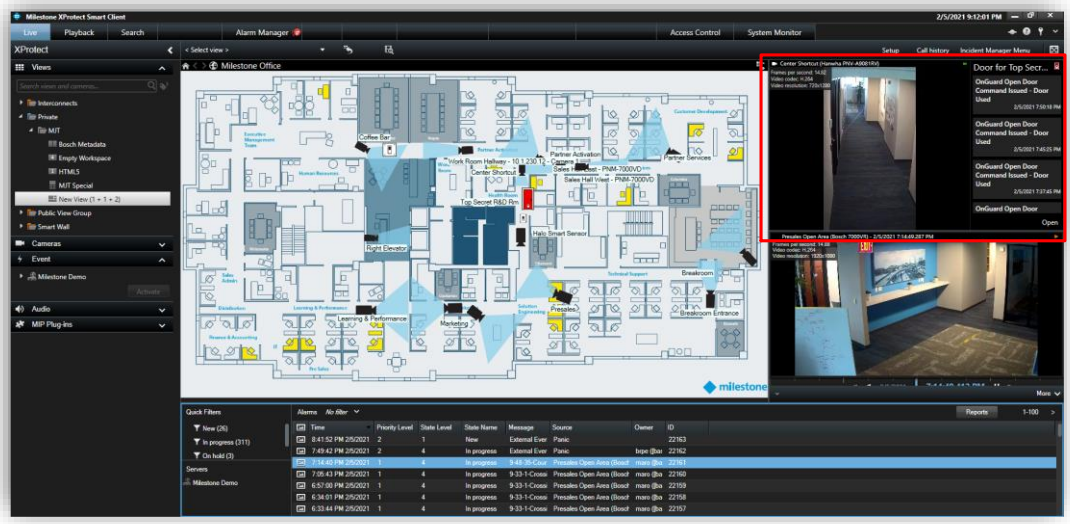


Access Monitor

The Access Monitor view item displays live status from doors and video from associated cameras in a single view pane in the Smart Client. Click Setup in the Smart Client and expand the System Overview panel menu. Select the Access Monitor view item and drag it into any available view pane:



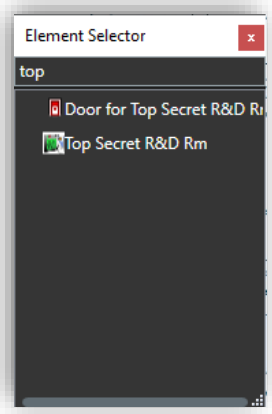
In the access monitor settings window open the lists to select the door, sources, cameras, events, commands, and the order in which new events appear in the access monitor. Once the door is selected, many of the other options will change, based upon the available cameras, events, and commands. The access monitor view item can be added to any available view pane and works in a view alongside all available view items.

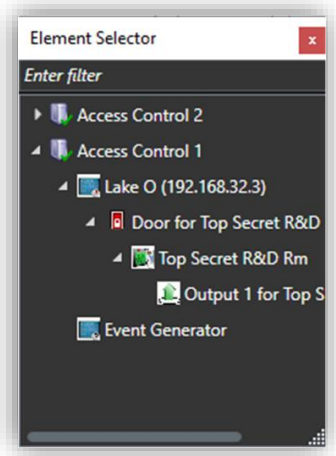


Maps

It is possible to place doors, readers, inputs, outputs, panels and OnGuard server(s) on an existing Smart Client Map. The map icons display hardware status as well as execute commands. With the Smart Client in setup mode a Tools window will appear in the view pane. From this window, select the Add access control icon:

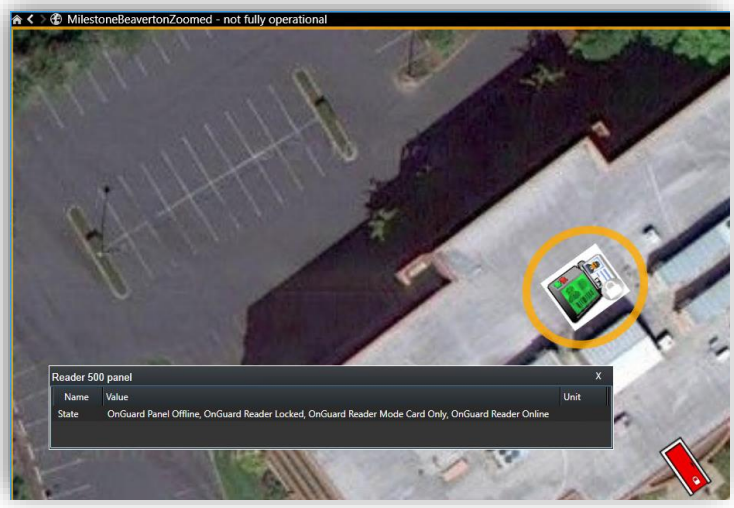
The Element selector window will appear. Type the name of a hardware device into the filter to quickly find a device or expand the servers and panels to find all available hardware icons in the system.





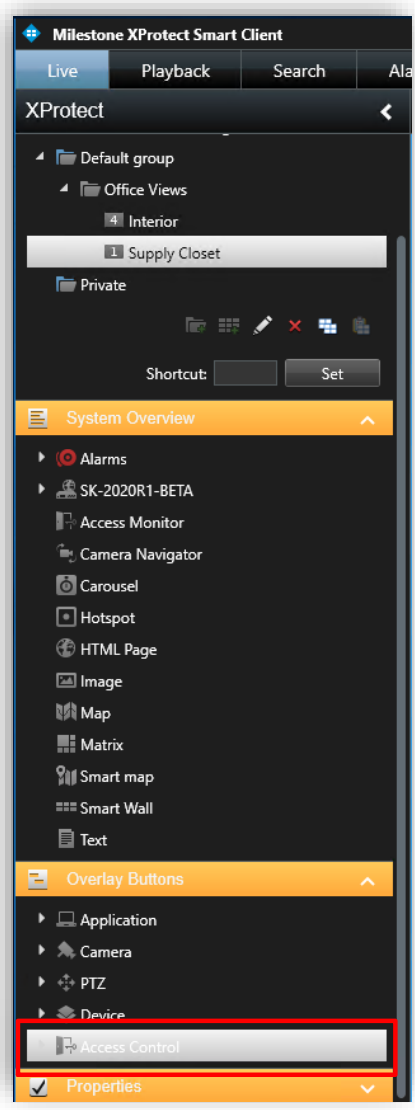
Drag the chosen icon onto the map. During normal operations, it is possible to right-click on any of these icons to execute the commands from the shortcut menu.

Right click the device icon and select Status Details from the shortcut menu to view more information.

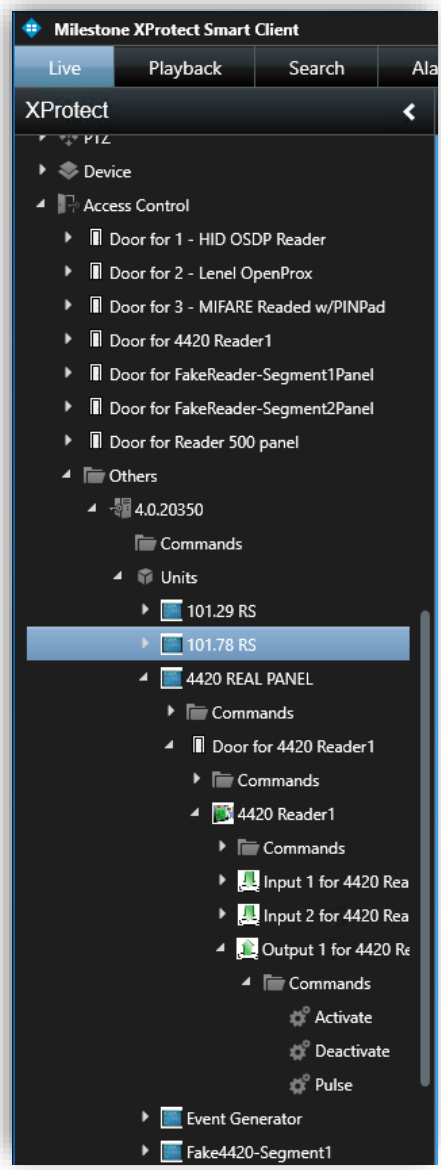


Overlay Buttons & Commands

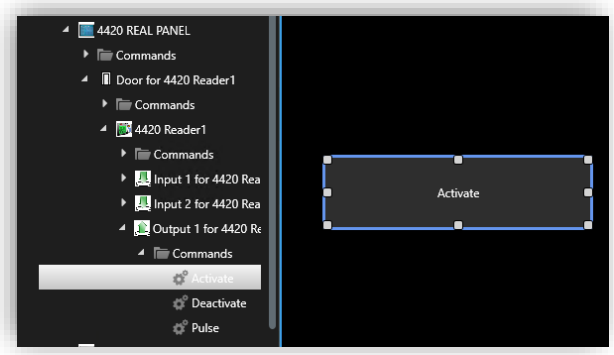
Overlay buttons are used to add manual buttons to video panes. Anything that can be triggered by a command can be added with an overlay button in the Smart Client. When the Smart Client is in setup mode, there is an Overlay Buttons panel on the left side of the client, select the Access Control icon.



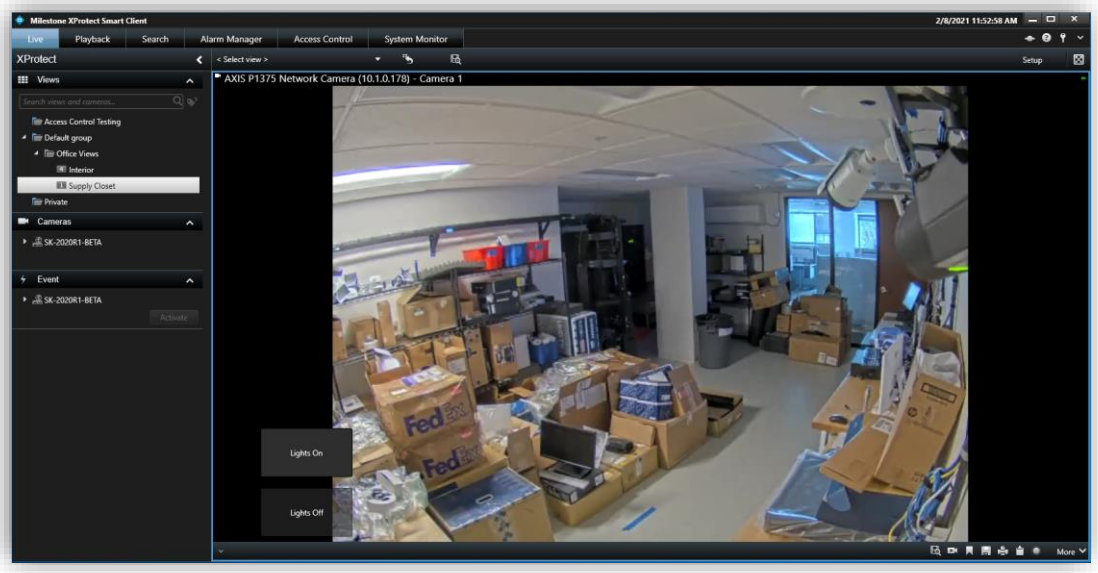
Expand the Access Control icon to find all the doors and readers, panels, and the connected inputs and outputs in the system.



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



The output commands include activate and deactivate. Once the commands are visible on a camera view pane they can be resized, moved around, and - with a right click - the name of the command can be edited.



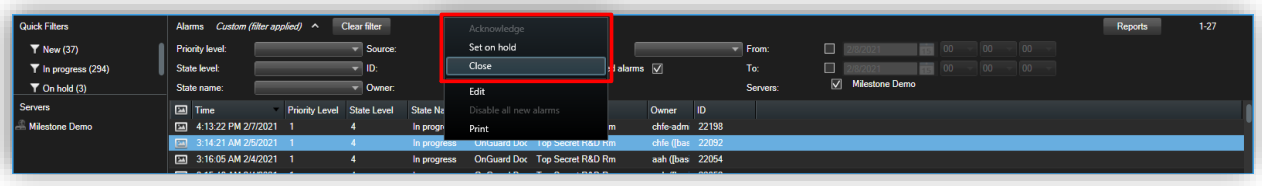
Alarm Acknowledgment

Alarm status between XProtect and OnGuard is shared. When alarms are closed in XProtect that state is shared with OnGuard. In the OnGuard system the same alarm will be acknowledged/closed. Alarm status is shared in the opposite direction as well – from OnGuard to XProtect.

Possible alarm states in XProtect and OnGuard are not identical. In XProtect alarms can be new, acknowledged, set on hold, or closed. In OnGuard alarms are either active or acknowledged. For the XPA OnGuard integration, acknowledged alarms in OnGuard are the same as closed alarms in XProtect. All other alarm states in XProtect are equivalent to active alarms in OnGuard.

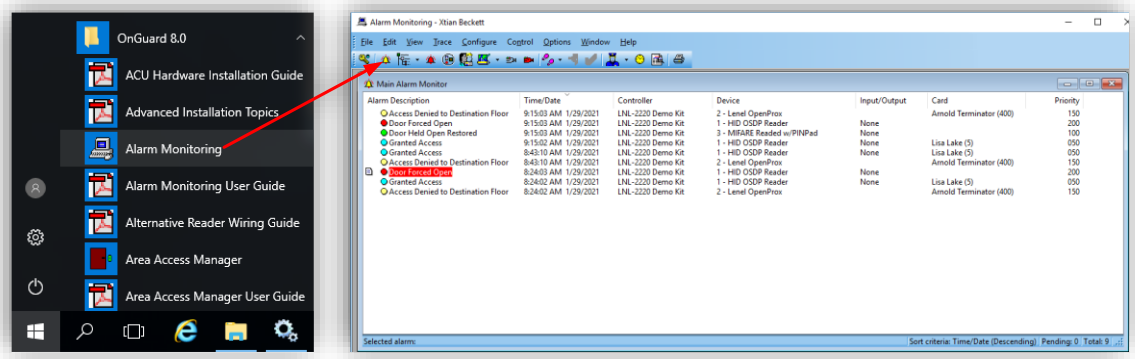
OnGuard Alarm Status	XProtect Alarm Status
• ACTIVE	• NEW • ACKNOWLEDGED > IN PROGRESS • ON HOLD
• ACKNOWLEDGED	• CLOSED

Alarm acknowledgment and other alarm status change operations are performed manually in the XProtect Smart Client. In the Alarm Manager, or any alarm list view item, right-click an alarm, and choose a new status from the shortcut menu. Close will close the event in XProtect and in OnGuard.

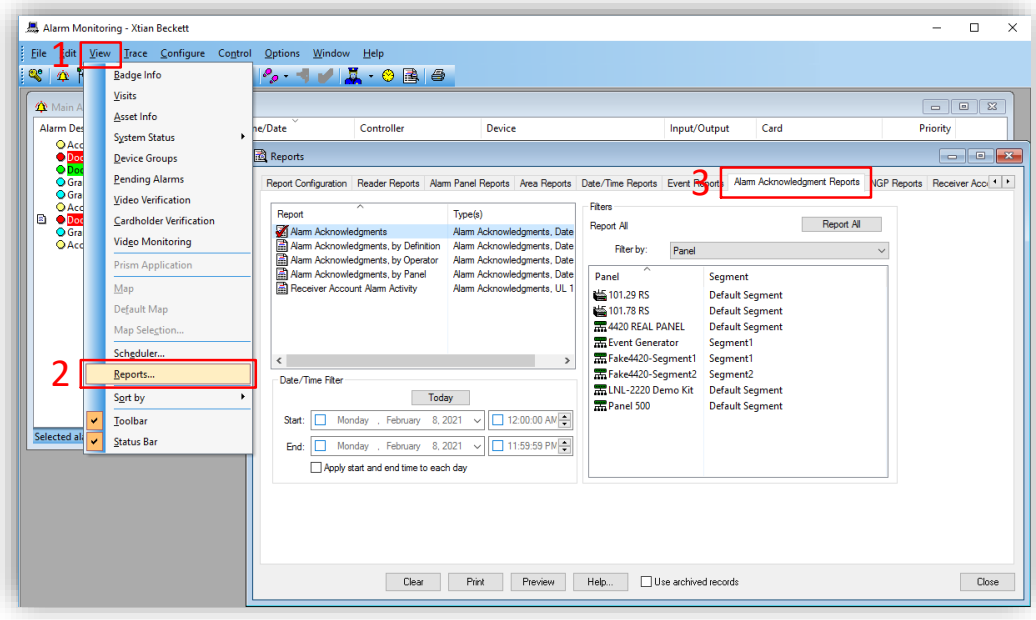


When alarms are acknowledged in OnGuard, the alarm is closed, and the associated alarm is also closed in XProtect. If the alarm is acknowledged within XProtect it will not change status in OnGuard. The status of the alarm in OnGuard will only change when the alarm is closed in XProtect.

Verify state changes of alarms in the OnGuard system in real time by opening the Alarm Monitoring application from the Start menu. If it is not automatically opened, click the View Alarms icon to open the Main Alarm Monitor window. Status of OnGuard alarms is displayed in this window in real time. Right click an alarm in this window to acknowledge the alarm.



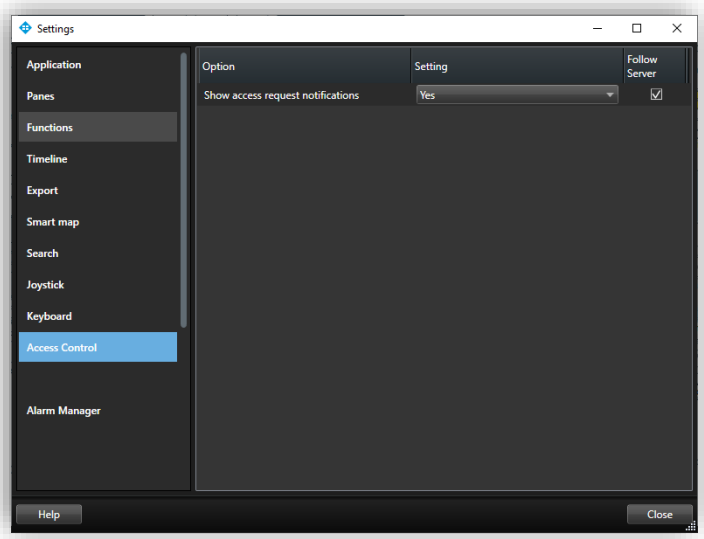
Verify closed alarms from the View > Reports window and the Alarm Acknowledgement Reports menu. Choose a time range and export a report of all acknowledged alarms in the OnGuard system.



Access Control Options

In the upper right corner of the Smart Client application is a down arrow icon.

Click on this icon and choose the settings option to enter the Smart Client settings window. Select the Access control menu in the Settings window. Choose to show or block access request notifications in the Smart Client.

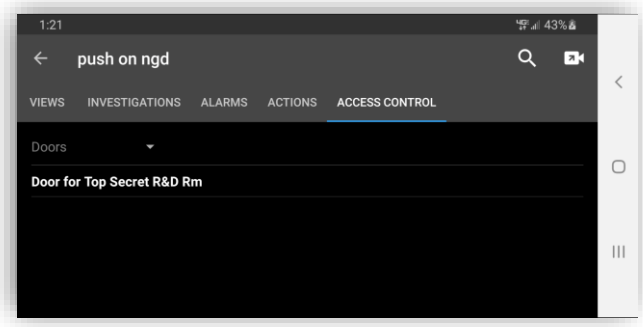


Mobile Client

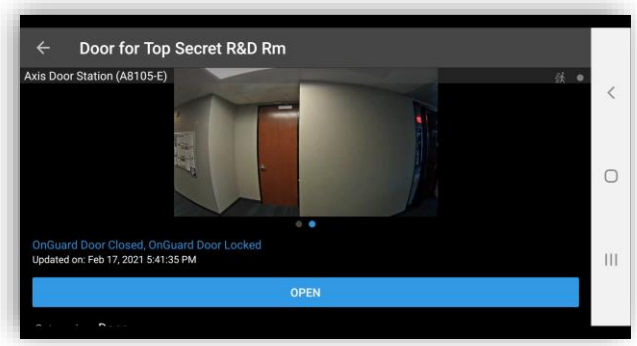
Milestone Mobile is a smartphone app that connects to your VMS system. The XProtect Access OnGuard Integration adds functionality to Milestone Mobile. Using Milestone Mobile it is possible to receive a push notification from the access control system, view live video related to the notification, and open the door – all remotely from a smartphone.

Access Control Tab in Milestone Mobile

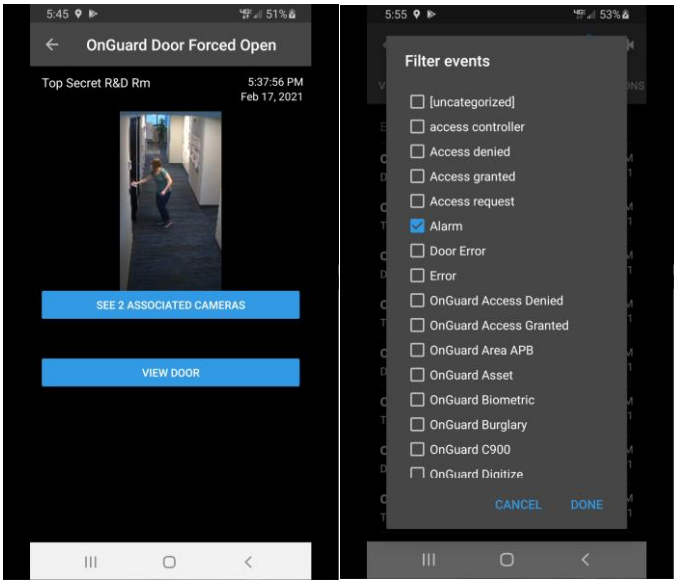
After logging into the VMS with Milestone Mobile the Views tab is presented by default. From this tab it is possible to select the Access Control tab. The Access Control tab shows the list of doors available.



Filter for specific doors or select a door to view cameras associated to that door or interact with commands available for the selected door. Swipe to switch between cameras when multiple cameras are associated to a door.



Switch between Doors, Events, and Access Requests. Select an event from the event list to view still images associated to the event and playback video related to the event. Filter the event list.



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

Logging

Debug logs are enabled on the Milestone Event Server plugin and the OnGuard ACM server application. The default log level is info, which is the least detailed level. The level of detail can be increased.

Log File Locations

Milestone

1) Go to the Milestone Event Server.
2) Open File Explorer. Select the View menu and enable Hidden items.
3) Log files in these locations are relevant:
   a) C:\ProgramData\VideoOS\ACMServerPlugin
   b) C:\ProgramData\Milestone\XProtect Event Server\logs

OnGuard

1) Go to the OnGuard server.
2) Open File Explorer. Select the View menu and enable Hidden items.
3) Log files in these locations are relevant:
   a) C:\ProgramData\VideoOS\ServiceHost\logs
   b) C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\logs
   c) C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServerPlugin\logs

Changing logging level

The log's level of detail can be changed by setting the logging level. The logging level can be set at any of the following values:

- Off
- Fatal
- Error
- Warn
- Info
- Debug
- Trace

"Off" writes no information to the file and "Trace" writes as much information as possible to file. The default setting is "Info." New log files are created each day. After 10 days the files are automatically deleted. Here is the procedure to change the log levels:

Milestone

1. Go to the Milestone Event Server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Open the following folder:
    a. C:\ProgramData\VideoOS\ACMServerPlugin
4. In each subfolder named with a globally unique identifier (GUID - something like "4c53f6e5-e951-1616-83f0-e44fb813e451") do the following:
    a. Find the file: "ACMServerPluginNLog.xml", open it with notepad.
    b. The second to last line in the file is like this "<logger name="*" minlevel="Info" writeTo="mainlog" />"
    c. Change the "Info" to "Debug" or "Trace," or any other log level and save the file.
    d. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.

OnGuard

1. Go to the OnGuard server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Open the following folder:
    a. C:\ProgramData\VideoOS\ServiceHost.
    b. Find the file: "ServiceHostNLog-4-0.xml" and open it with notepad.
    c. Near the bottom of the file, find the lines that begin with:
        i. <logger name="OnGuardAcmServerPlugin.Managers.EventManager"
        ii. <logger name="OnGuardAcmServerPlugin.Managers.StateManager"
        iii. <logger name="OnGuardAcmServerPlugin.BackwardCompatibility.Backward-CompatibilityManager"
        iv. <logger name="OnGuardAcmServerPlugin.*"
        v. <logger name="VideoOS.OnGuard.Client.*"
    d. Change the "minlevel" attribute values in those lines from their current values to "Debug" or "Trace," or any other log level.
    e. Near the bottom, find this line in the file:
        i. <logger name="*" minlevel="Info" writeTo="mainlog" />
    f. Change the "minlevel" attribute values in that line from the current value to "Debug" or "Trace," or any other log level and save the file.
    g. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.
4. Open the following folder:
    a. C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService
    b. Find the file: "VideoOSACMServerASMScannerNLog.xml" open it with notepad.
    c. Near the bottom, find this line in the file: "<logger name="*" minlevel="Info" writeTo="mainlog" />"
    d. Change the "Info" to "Debug" or "Trace," or any other log level in that line and save the file.

e. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.

Troubleshooting Guide

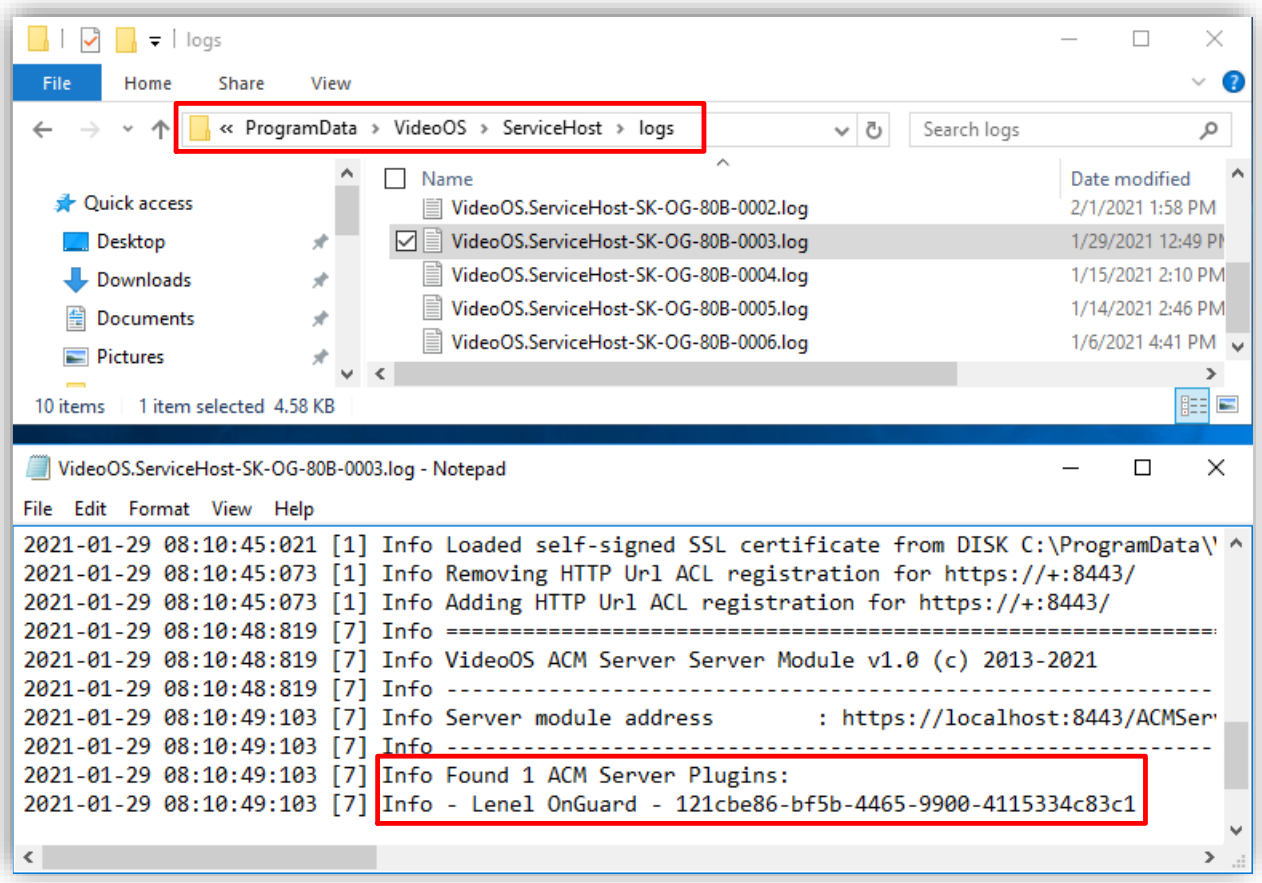
ACM Server: OnGuard Plugin Post-Install Verification

Verify the OnGuard Plugin (located on the Milestone Event Server server) successfully installed by checking in the logs below. These logs are located on the OnGuard server. The log location is:

C:\ProgramData\VideoOS\ServiceHost\logs

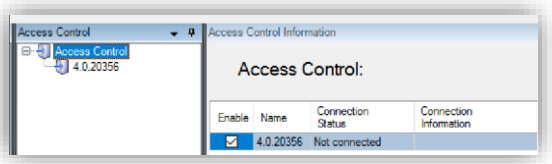
Open the VideoOS.ServiceHost-LocalhostPCName.log file – the LocalhostPCName section of the file name is the PC name of the OnGuard Server. Enable Hidden items in the View menu of File Explorer if the ProgramData folder is not visible. Verify that the following entries are in the Log file:

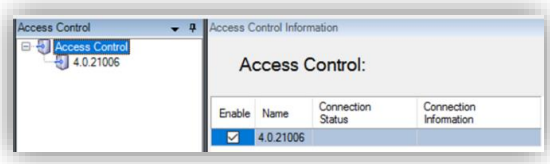
Info Found 1 ACM Server Plugins:
Info – Lenel OnGuard - **GUID**-****-****-****-************



Connection Status displays “Not connected” or is empty.

OnGuard version 4.0 access control instance added into XProtect displays a Connection Status in the Access Control Information window as "Not connected" or no information is displayed.





This is an indication that a non-critical error has happened with the ACMServer. The process of retrieving the current state of the system failed. Verify that the other functions of the integration are still working by clicking the Doors and Associated Cameras menu or any other active menu for this instance. If functionality is still working in these menus, proceed to verify that Smart Client functionality: access control monitors, map icon status, and access control workplace search are still available.

Cardholder search data fields are missing

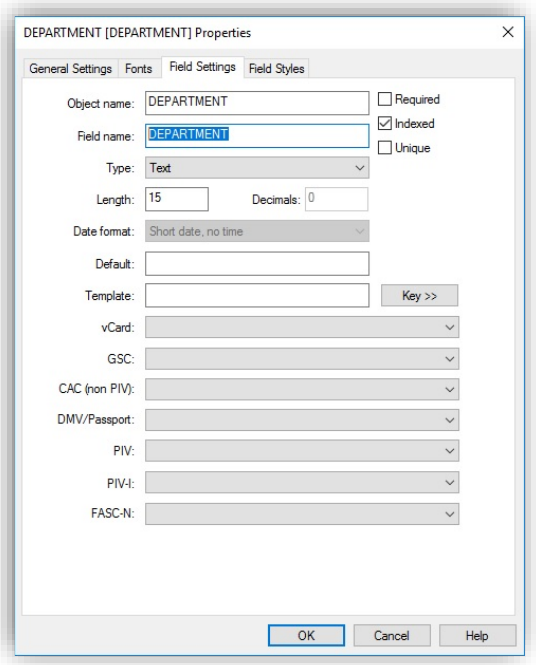
The OnGuard XPA Integration uses a default list of cardholder data fields when searching for cardholders. A .json file is created automatically when the first search is performed. This file is named "PluginSettings.json" and it is located on the OnGuard server or the host of the ACM Server application. The file location should be:

- C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardACMServerPlugin\PluginSettings.json

The default list of cardholder data fields contains the following data types:

.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

The list in this .json file can be modified to add new data fields or to remove existing data fields. If the list, in the .json file is left empty, then the complete range of searchable fields available with OnGuard will be used. To edit the list of data fields the name of the fields must match the "field name" values as displayed in the OnGuard FormsDesigner application:



The default .json file should look like this:

```
{
  “Version”: “1.0”,
  “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”
    }
  }
}
```

An empty .JSON file will look like this:

```
{
  “Version”: “1.0”,
  “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”: {}
  }
}
```

After editing and saving the .json file, changes will take effect after the next restart of the ACM Server application. Follow this process to use a non-default or full list of searchable fields:

1. Complete the first cardholder search.
2. .json file is created with default list.
3. Edit the .json file to meet the new requirements.
4. Restart the ACM Server application.

NOTE: If the .json file is deleted, it will be recreated with the default search fields the next time the ACM Server is restarted and a new search is performed. It is recommended to edit the file instead of deleting it, if the full list of searchable fields is required.

OnGuard loses communication with access control hardware

Communication can be lost for the following reasons:

1) Firewall blocking traffic
2) The OnGuard LS Communication Server service is not running or needs to be restarted.
3) The OnGuard LS Web Service service is not running or needs to be restarted.

Not receiving cardholder or badge changes

If cardholder or badge changes are not reflected in either the Milestone Management or Smart Clients, ensure that software events are enabled in OnGuard.

ACM integration flooding OnGuard user transaction report

Milestone's XProtect system regularly 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 many transactions from the OnGuard ACM integration under the SSO user in the report. It is 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., will not support custom reports.
- Contact the OnGuard Custom Solutions group and have them create/customize the reports.

OnGuard ACM instance not displayed in the XProtect Management Client

If XProtect is unable to communicate with the OnGuard ACM instance, the instance will not 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 Milestone Event Server

On the OnGuard Server:

3. Stop the Milestone ACM Service
4. Ensure required OnGuard services are running.
   a. LS Event Context Provider
   b. LS Message Broker
   c. LS OpenAccess
   d. LS Web Event Bridge
   e. LS Web Service.
5. Start the Milestone ACM Service

On the Milestone Server:

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

If the instance still is not 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 shortly after it starts, which can cause OpenAccess to crash. The Milestone ACM Server will attempt 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 concerning a fix for this issue, please contact support for information regarding this bug 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 no detected in the Milestone ACM Server integration.

For questions and information concerning a fix for this issue, please contact support for information regarding this bug 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 do not send events through OpenAccess to the Milestone ACM Server integration.

For questions and information concerning a fix for this issue, please contact support for information regarding this bug 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.

Known issues:

- DO NOT run the Milestone.ACMServer.msi on the OnGuard server and choose the “Remove” option to uninstall the software. Doing so will put the system into an inoperable state. The only supported method for uninstalling this software is to use the Programs and Features menu in Windows.
- This ACM integration has only been tested when running the OnGuard and Milestone systems on Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

- OnGuard doesn't model doors; they work only with readers. But Milestone ACM requires doors to be modelled. Therefore, the OnGuard plugin creates virtual doors based on reader properties (i.e. panel id, panel address, reader number, etc). Currently, the virtual door names are based on the first reader that has a non-empty display name. So if that reader is named "reader 1", that's what the door will be named. This may not be intuitive when viewed in the XProtect Management or Smart Client applications' hardware hierarchy.
- When creating a new ACM instance on the Access Control tab in the XProtect Management Client, especially when creating the first instance, it may take 1 or 2 clicks of the Next button in the wizard before configuration is successfully fetched from the OnGuard system.
- The XPA Instance (MIPPlugin) in the Management Client can fail to load after the Event Server starts or is restarted if the ACM Server on the OnGuard Server is not started or not yet ready. Symptoms of this issue include:
    - Existing XPA Instance disappears from Management Client.
    - Creation of new XPA Instance is not allowed.
    - NullReferenceException log entries appear in the Event Server log file.

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 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 is a stand-alone company in the Canon Group.

milestone