Milestone XProtect Access

OnGuard User Manual

Prepared by:

Custom Development Americas

milestone

Table of Content

Copyright, Trademarks & Disclaimers 5
Copyright 5
Trademarks 5
Disclaimer 5
Version Notes 6
Version Compatibility 7
Matrix (Updated Jul 23, 2020) 7
XProtect Version details 7
OnGuard Version details 7
Hardware Support 7
Scalability 8
OnGuard Tested Setup (July-Sep 2020) 8
General Description 9
Introduction 9
Solution overview 9
Prerequisites 10
Time Synchronization 10
SQL Server: Configure OnGuard SQL for remote connections 10
.NET Framework: Installation on OnGuard Server machine 10
Milestone XProtect®: License Options 10
Milestone XProtect®: Event Server machine DNS / Name resolution 10
Milestone XProtect®: Smart Client Profiles 10
OnGuard: License Options – PLEASE CONSULT CARRIER FOR LICENSING 11
OnGuard: Mandatory Windows Services 11
OnGuard: Generate software events settings 12
OnGuard: Create Single Sign-On (SSO) Directory 13
OnGuard: Create Single Sign-On (SSO) User 14
Planning your Installation 16
Single System Scenario: The default case for OpenAccess / DataConduIT 17
Multiple Single Systems Scenario: Scaling the default case for OpenAccess / DataConduIT 18
Milestone XProtect® Federation with OnGuard Enterprise 19
Alternative deployment options for OpenAccess ONLY 20
Single system – ACM Server and OnGuard Server on separate machines (OpenAccess ONLY) 21

milestone

Milestone XProtect®: Federated with Single Large Segmented OnGuard (OpenAccess ONLY) 21
Milestone XProtect®: Clustered with Single Clustered OnGuard (OpenAccess ONLY) 22
Installation 23
ACM Server Installation 24
ACM Server Credentials 25
ACM Server: OnGuard Plugin Installation 26
ACM Server: OnGuard Plugin Post-Installation 27
ACM Server: XProtect ACM MIP Plugin 28
MIP Plugin Upgrades 29
OnGuard Configuration 30
Configure to run as OnGuard Single-Sign-On Account 30
Reducing Permissions 33
XProtect ACM MIP Plugin Configuration 34
ACM Server Wizard 34
Installing an ACM Server 34
Uninstalling an ACM Server 39
XProtect Management Client Configuration 40
XProtect Management Client 40
Properties 42
Reducing Permissions 47
Personalized Login 48
Common Actions 53
Editing OnGuard Event Types 53
Searching for cardholders 54
Defining alarms based on OnGuard events 56
Defining rules based on OnGuard events 61
XProtect® Smart Client Maps 64
XProtect® Access Monitor tiles 65
Alarm Acknowledgment 66
Fetching OnGuard event types 68
Defining cardholder properties to display in Milestone XProtect 68
Feature Differences Between Connection Modes 70
Alarm Acknowledgement 70
User Privileges 70
Events 70
Logging 71
Gathering the logs 71
Changing logging level 71
Troubleshooting Guide 72
OnGuard loses communication with the access control hardware 72
Failure of the ACM plugin to communicate with Window Management Interface (WMI) 72
Milestone Event Server MIP Plugin cannot communicate with the ACM Server (DataConduIT only) 73

milestone

Debug log shows SqlAccess.connect() failed 73
Failure to connect to SQL Server 73
Not receiving card holder or badge changes 74
Optimizing Event Processing Performance 74
Refreshing cardholders 75
WMI related errors 76
OnGuard OpenAccess connectivity 76
XProtect® Smart Client not showing alarm panels or their inputs/outputs 76
OnGuard ACM integration flooding user transaction report 77
OnGuard ACM instance is not displayed in the XProtect® Management Client 77
LS OpenAccess service automatically stops seconds after starting 77
I/Os connected to OSDP readers are no longer detected 78
LS OpenAccess fails to send any events when running in an Enterprise configuration 78
All other support issues 78
Known issues 78

Copyright, Trademarks & Disclaimers

Copyright

© 2020 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 document 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 reserve the right to make adjustments without prior notification. All names of people and organizations used in this document's examples 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 3*rd_party_software_terms_and_conditions.txt* located in your Milestone surveillance system installation folder.

Version Notes

Version	Notes
3.4.x.x	Last Version compatible with DataConduIT
3.5.x.x	This version is NOT compatible with DataConduIT

Version Compatibility

Matrix (Updated Jul 23, 2020)

Here is the compatibility matrix between OnGuard and Milestone XProtect.

OnGuard	XP 2017 R1-R3	XP 2018 R1-R3	XP 2019 R1-R3	XP 2020 R1-R2	XP 2020 R3
7.4 Before Dec 2020	S	S	S	S	S
7.4 After Dec 2020	U*	U*	U*	U*	U*
7.5	S	S	S	S	S
7.6	S	S	S	T	S
8.0	S	S	S	T	S

*OnGuard 7.4 is end-of-life and no longer supported or maintained after Dec 2020

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

XProtect Version details

Version	Version Information
XProtect 2017 R3 XProtect 2018 R1-R3 XProtect 2019 R1-R3 XProtect 2020 R1-R3	These versions are fully supported*

*XProtect Free Editions of Go, Essentials and Essentials+ are NOT supported

OnGuard Version details

Version	Minimum update / patch level	Version Information
OnGuard 7.4	7.4.457.0 and up	These versions are fully supported until Dec 2020
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	8.0.379.0 and up	This version is fully supported

Hardware Support

The following OnGuard panels have been tested and are known to be supported.

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

Scalability

The scale testing section depicts the latest test setup run at the Lenel certification labs and expresses the scale that can be expected of the integration

OnGuard Tested Setup (July-Sep 2020)

Type of Device	Count
Panel	120
Door	1024
Reader	1028
IOModule	14
Input	2074
Output	2055
Card Holders	44540

Eventing	Events/sec
OpenAccess	7
DataConduIT	N/A

General Description

Introduction

This document describes specifics to the XProtect Access (XPA) integration between Milestone XProtect and the OnGuard access control (AC) system. This integration supports the following standard XProtect Access (XPA) features:

- Retrieve configuration from the OnGuard AC system, e.g. doors and event types
- Receive AC event streams and state changes from the OnGuard system
- Get/Search cardholder information with picture association
- Create alarms in alarm manager based on AC events.
- Alarm state synchronization between XProtect (2017 R3 or greater) and OnGuard when the alarm is acknowledged in XProtect. Alarm acknowledgment synchronization when the alarm is acknowledged in OnGuard is implemented for the OpenAccess connection mode only.
- Association of access control events to cameras for simultaneous display of events and video
- Select and categorize the events the user wants to view from the OnGuard system
- Trigger rules or actions based on access events – e.g. start recording, go to PTZ preset, display access request, send camera to matrix and system actions such as activate output or trigger manual event. With XProtect Corporate and Expert this functionality is extended to full use of the event as a triggering mechanism for the rules system.

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.msi)
3. The "OnGuard ACM Server Plugin" that runs on the OnGuard server (Milestone.ACMServer.OnGuard.msi)

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.

SQL Server: Configure OnGuard SQL for remote connections

These instructions are here to help setup a SQL server instance to enable remote connections so that the OnGuard integration can connect to the database. They are not meant to replace the knowledge of a trained SQL Server administrator, only to provide a way to enable remote connections on SQL Server. The following assumes that SQL Server is using its default ports.

1. Make sure that the SQL Server Browser service is started on the server.
    a. Use the Windows Services UI to start the Browser service if it's not running.
2. Make sure that you have configured the firewall on the server instance of SQL Server to open ports for SQL Server and the SQL Server Browser port
    a. In Windows Firewall with Advanced Security, create two new inbound rules:
        i. Enable incoming port UDP on port 1434
        ii. Enable incoming port TCP on port 1433
3. Use the SQL Server Surface Area Configuration tool to enable SQL Server to accept remote connections over the TCP or named pipes protocols
    a. In SQL Server Configuration Manager:
        i. Enable TCP/IP protocol for port 1433
4. Restart the SQL Server database server.

.NET Framework: Installation on OnGuard Server machine

.NET Framework 4.5 must be installed on the OnGuard server machine (dotnetfx45_full_x86_x64.exe). This is mostly for older OS editions, anything above Windows 8 and Windows 2012 Server 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 Options

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.

Milestone XProtect®: Event Server machine DNS / Name resolution

The machine running the Milestone XProtect Event Server must have network name resolution such that it can resolve the computer name of the OnGuard Server machine (e.g. DNS, manual host file entry, etc). The OnGuard Server machine must also be able to resolve the Milestone machine.

Milestone XProtect®: 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 in either DataConduIT or OpenAccess connection modes the following license options must be enabled in the OnGuard license:

Type of Connection	OnGuard License Options Needed
DataConduIT	Maximum Number of DataConduIT Clients (SWG-1140) must be >= 1
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 later, 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 3.5 or later, the system must be licensed for OpenAccess and OpenAccess specific properties mentioned in the Properties section must be configured before upgrading.

OnGuard: Mandatory Windows Services

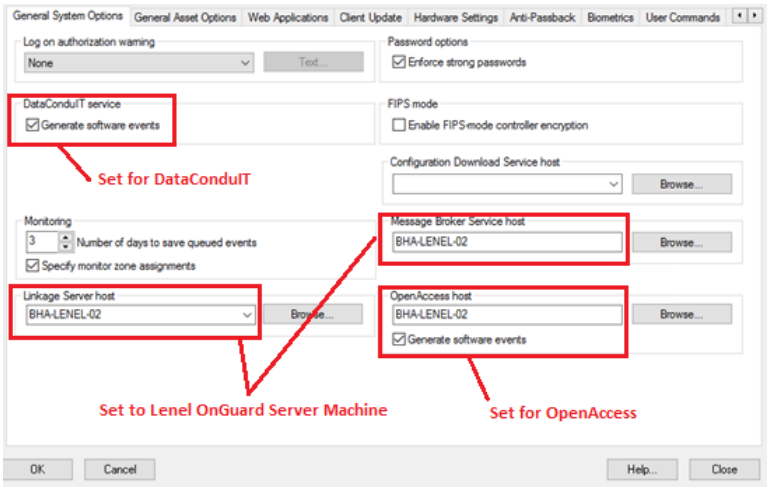
The following Windows services must be running on the OnGuard machine:

OnGuard Windows Service Name	Description
LS Communication Server	Required for the hardware to communicate with the OnGuard system
LS Linkage Server	Required for event handling
For DataConduIT	
LS DataConduIT Service	Required for our integration to use the OnGuard DataConduIT API
For OpenAccess	
LS Event Context Provider	Required to receive events from the OnGuard system
LS OpenAccess	Required to interface the OnGuard system web service-based API Open-Access (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)

OnGuard: Generate software events settings

Under Administration, System Options:

1. To use a DataConduIT connection, check the DataConduIT Service and Generate Software Events checkbox.
2. For OnGuard versions greater than or equal to 7.4 using OpenAccess, check the OpenAccess Host and Generate Software Events checkbox.
3. Set the Linkage Server Host to the OnGuard server's machine name.
4. Set the Message Broker Service Host to the OnGuard server's machine name.

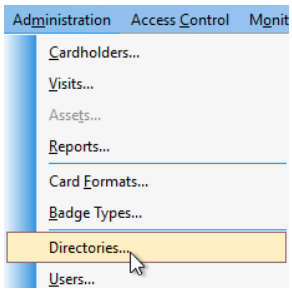


OnGuard: Create Single Sign-On (SSO) Directory

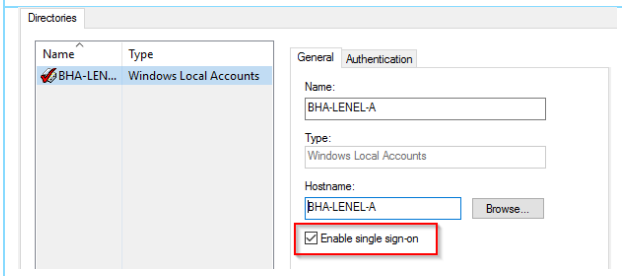
These instructions are not meant to replace the knowledge of a trained Lenel system administrator. They are here to enable the basic setup of an authentication directory and SSO user so that the integration can connect to the OnGuard system.

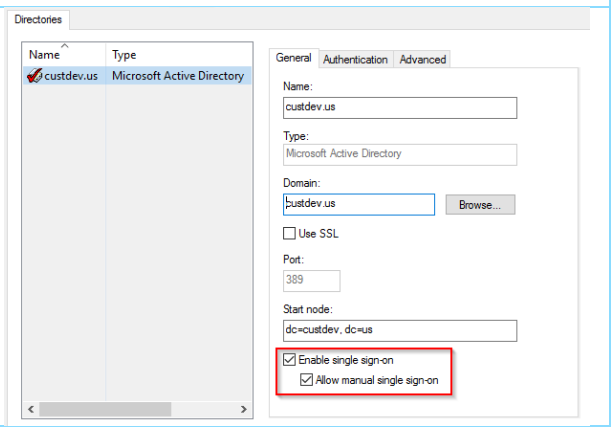
For a Lenel OnGuard Enterprise system, you can only create directories on the master

Using the OnGuard System Administration app: Select Administration -> Directories from the application menu



DataConduIT	OpenAccess
For **DataConduIT** support, the single sign-on account MUST be a "Windows Local Account".	For **OpenAccess** support, the single sign-on account **MUST** "Allow manual signal sign-on" as shown below.





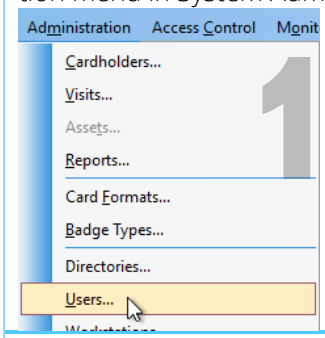
If you are creating a Directory of a type other than "Windows Local Accounts" (e.g. LDAP, Active Directory), ensure that the SSO user is a member of the Local Administrators group.

If you are using OpenAccess on Lenel OnGuard 7.4 Update 1 or lower, ensure that the SSO account is a windows local account.

OnGuard: Create Single Sign-On (SSO) User

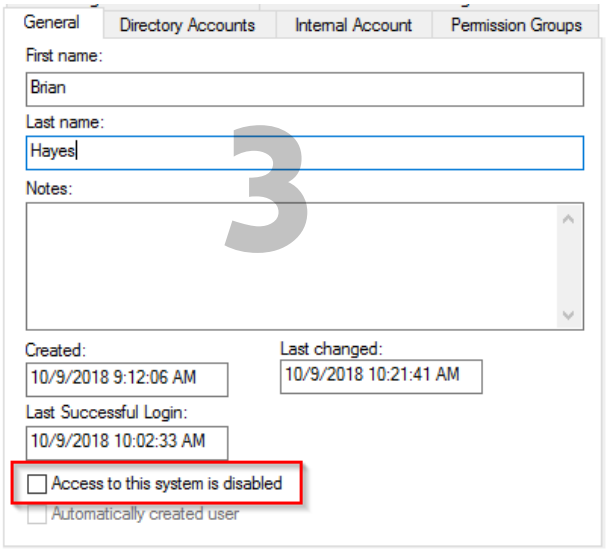
These instructions are not meant to replace the knowledge of a trained Lenel system administrator. They are here to enable the basic setup of an authentication directory and SSO user so that the integration can connect to the OnGuard system.

Select Administration -> Users from the application menu in System Administration

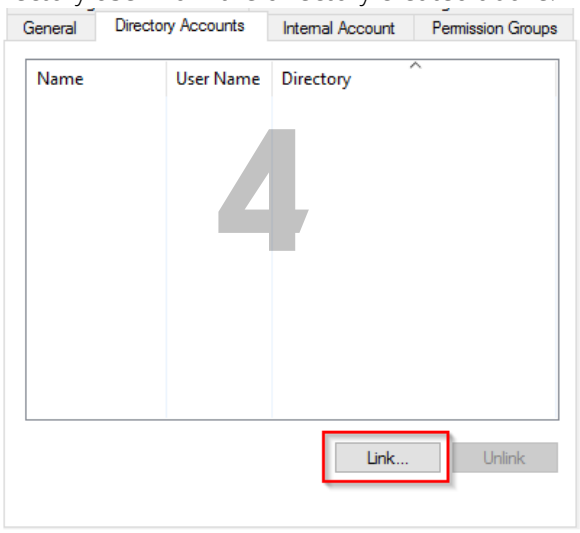


Add a new user.

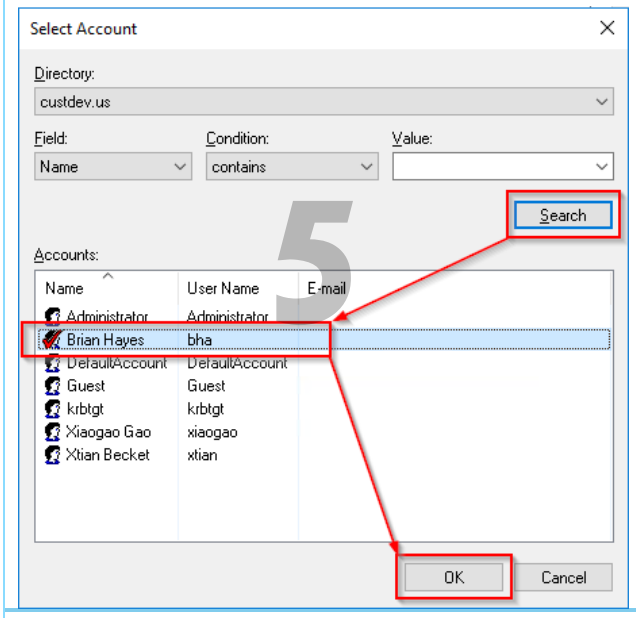
General tab -- Be sure that "Access to this system is disabled" is NOT checked.



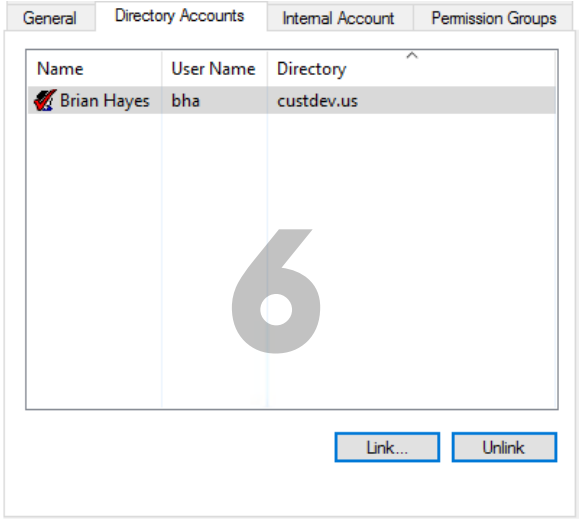
Directory Accounts tab -- Link the user to the directory user from the directory created above.



In the Select Account dialog, Select Directory from drop-down, click Search, select a Windows user in Accounts then click OK.

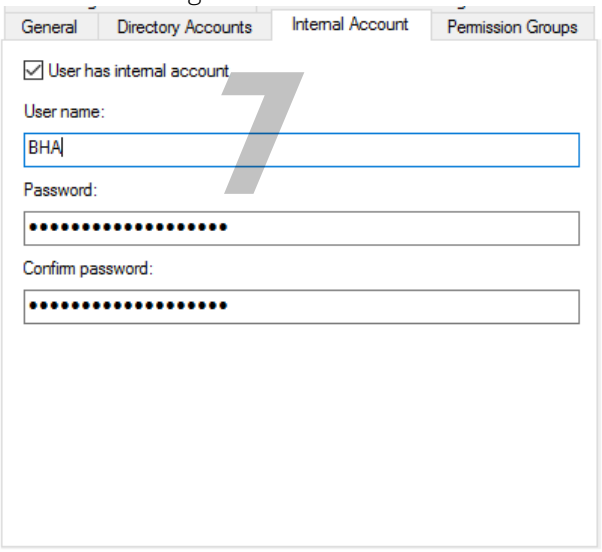


Once selected the OnGuard user account is linked to the corresponding Directory account



Internal Account tab

- Make sure that the "User has internal account" checkbox is checked.
- Enter login credentials.



Permission Group tab

Assign the following permission groups:

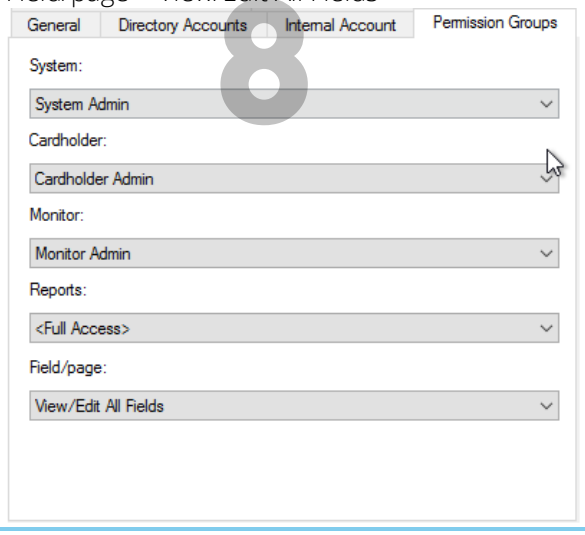
System = System Admin

Cardholder = Cardholder Admin

Monitor = Monitor Admin

Reports = Full Access

Field/page = View/Edit All Fields

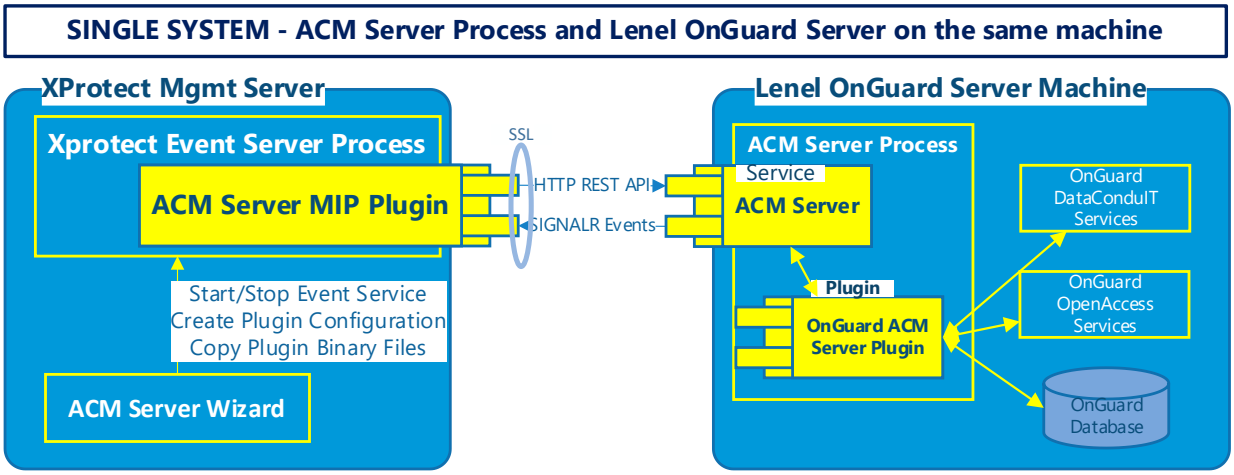


Planning your Installation

There are many options and different ways of integrating the XProtect VMS with the OnGuard Access Control System. This section is meant to be a guide to help you figure out which deployment options you should use depending on your use case. In all cases below care should be taken to respect the scale numbers on every XPA connection. See the scalability section here for limits of the integration on a per XPA connection basis.

Installation Scenario	Use case
Single System DataConduIT or OpenAccess	You have a single XProtect system (one event server per system) and a single OnGuard system (one OnGuard database per system)
Multiple Single Systems DataConduIT or OpenAccess	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 DataConduIT or OpenAccess	You have an existing OnGuard Enterprise system that needs pairing (you have to use XProtect Federated Architecture to pair OnGuard Enterprise). You have a federated XProtect system and an OnGuard Enterprise system that need pairing. The customer needs centralized configuration and alarms.
Alternative Configurations	
Single system – ACM Server and OnGuard Server on separate machines OpenAccess ONLY	This configuration is part of the alternate configurations where there is a need to run the ACM Server on a different machine than the OnGuard Server. This configuration is only valid in OpenAccess mode.
XProtect Federated with Segmented OnGuard OpenAccess ONLY	You have a single large OnGuard system that is segmented and the customer would want to see different segments of the system associated to a different XProtect system
XProtect Clustered with OnGuard clustered OpenAccess ONLY	You have a XProtect clustered environment connecting to an OnGuard clustered environment

Single System Scenario: The default case for OpenAccess / DataConduIT

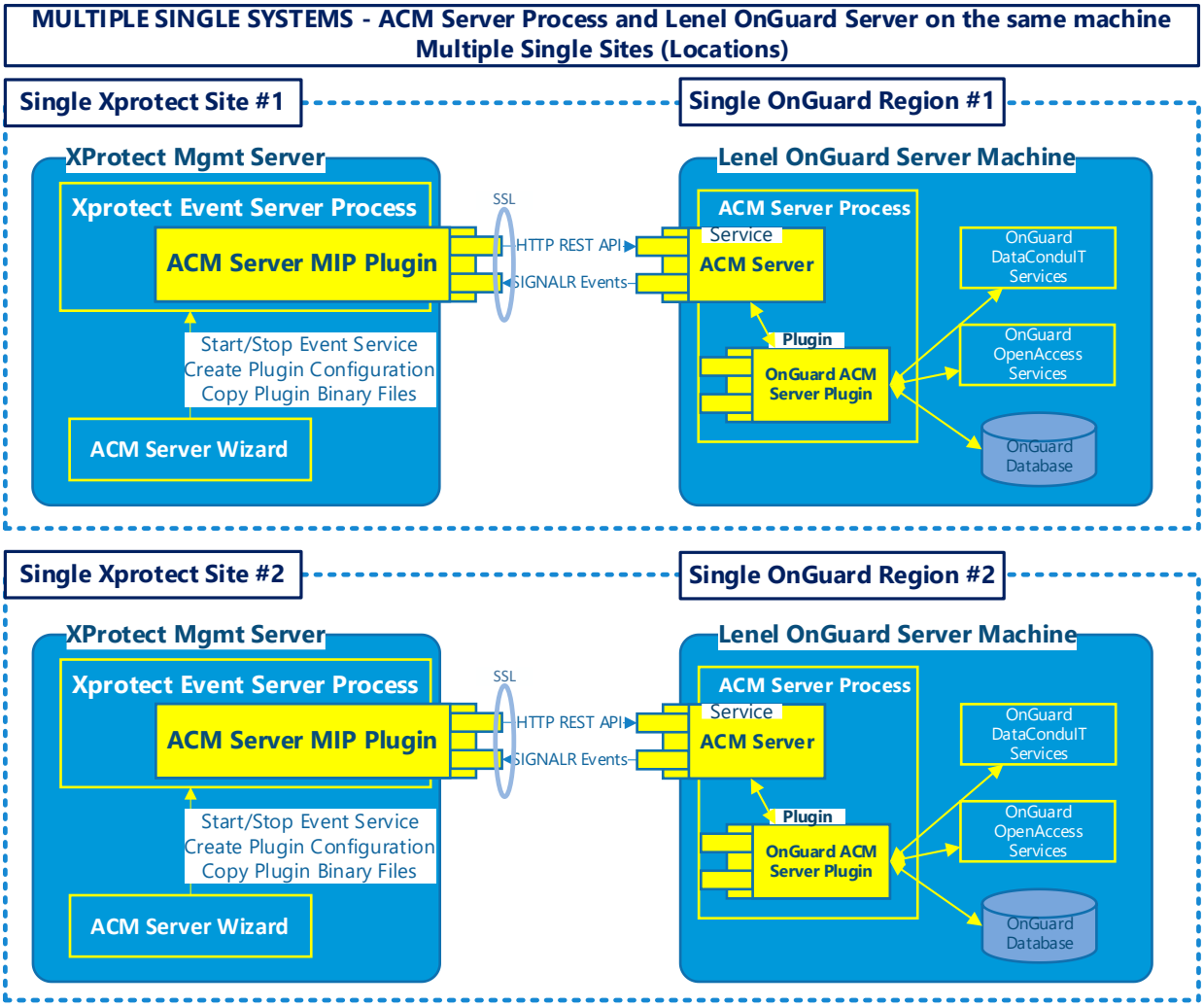


For most scenarios, this is the recommended installation scenario

- 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 / DataConduit / OpenAccess Services.

Multiple Single Systems Scenario: Scaling the default case for OpenAccess / DataConduIT

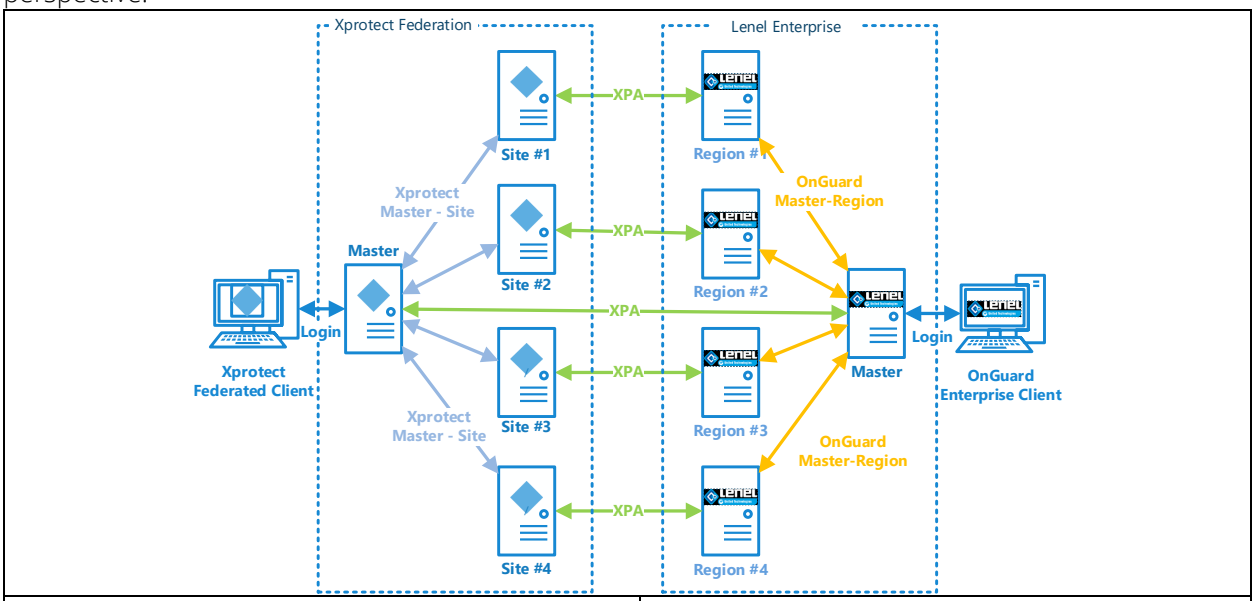
Increasing the scale in the default scenario means adding more Lenel OnGuard systems and XProtect systems in a 1:1 ratio. The Lenel and XProtect systems are independent of each other keeping the ACM Server process on the Lenel OnGuard machine. The customer is NOT interested in centralized configuration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



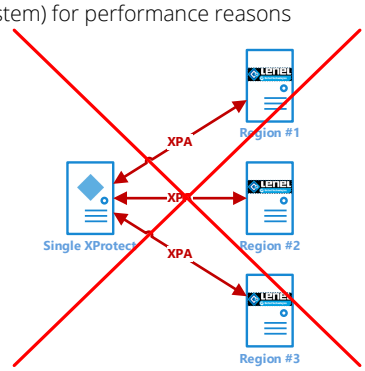
Site #1 and Site #2 are independent of each other and are not communicating with each other or commonly managed. The same is true for both the XProtect and the OnGuard systems in this scenario.

Milestone XProtect® Federation with OnGuard Enterprise

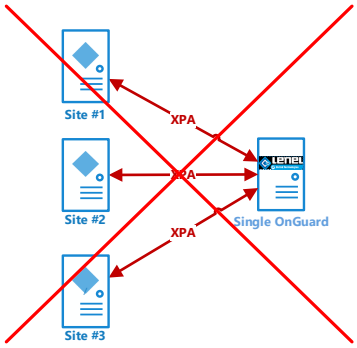
This scenario has multiple uses, and will most probably be the most used scenario in large scale deployments. This scenario should be the default when the customer already has an Enterprise deployment of OnGuard and wants to introduce an XProtect counterpart. It should also be used when the customer wants centralized alarm and configuration management from the XProtect/OnGuard perspective.



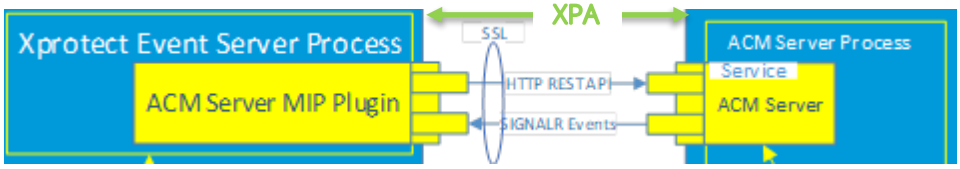
We DO NOT support one single XProtect Site to connect to multiple OnGuard Regions for performance and scale reasons. We do not recommend running more than one XProtect Access integration per event server (whether it be OnGuard or other AC system) for performance reasons



We DO NOT support multiple XProtect Sites to connect to a single OnGuard region WHEN AND ONLY WHEN the ACM Server is on the same machine as the OnGuard Server



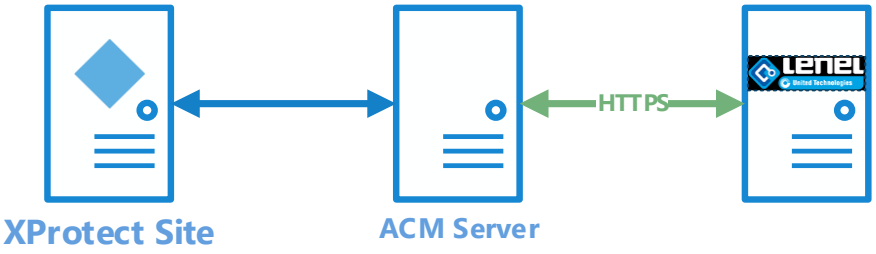
Each green XPA lines represents the HTTP/SignalR connection between the Event Server process in XProtect and the ACM server living on the OnGuard Server machine (there are some scenarios where ACM server may not live on the same OnGuard server, see Alternate Configurations for details)



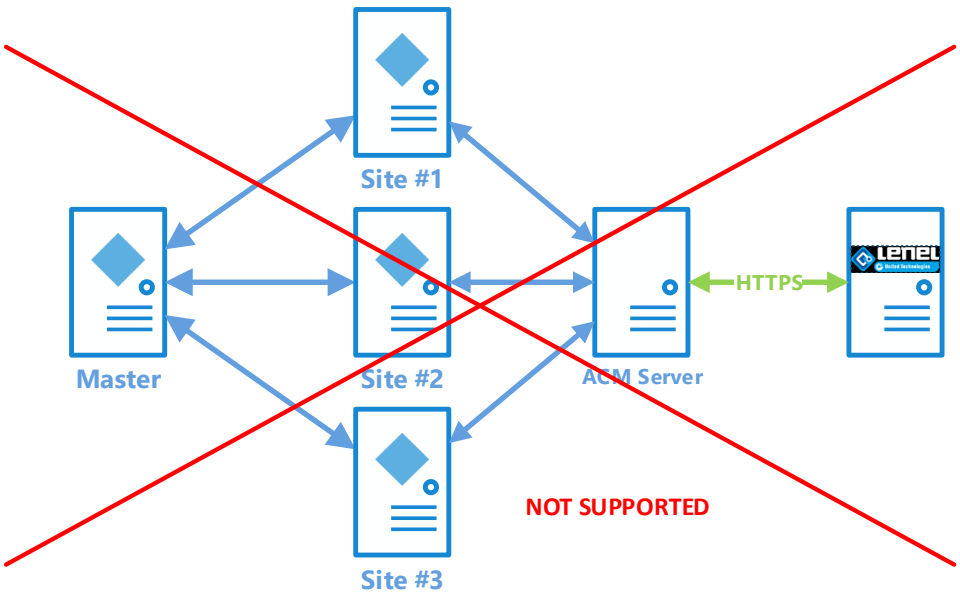
Alternative deployment options for OpenAccess ONLY

For configurations that use the OpenAccess connection mode, it is possible to have the "integration" ACM server site on a different machine than the XProtect machine and the OnGuard server machine. These alternate scenarios allow among other things to support OnGuard segmentation of hardware and events to multiple XProtect sites, OnGuard clustering support and potentially other enterprise scenarios.

You cannot use this alternative installation configuration when using the DataConduIT Access Type.

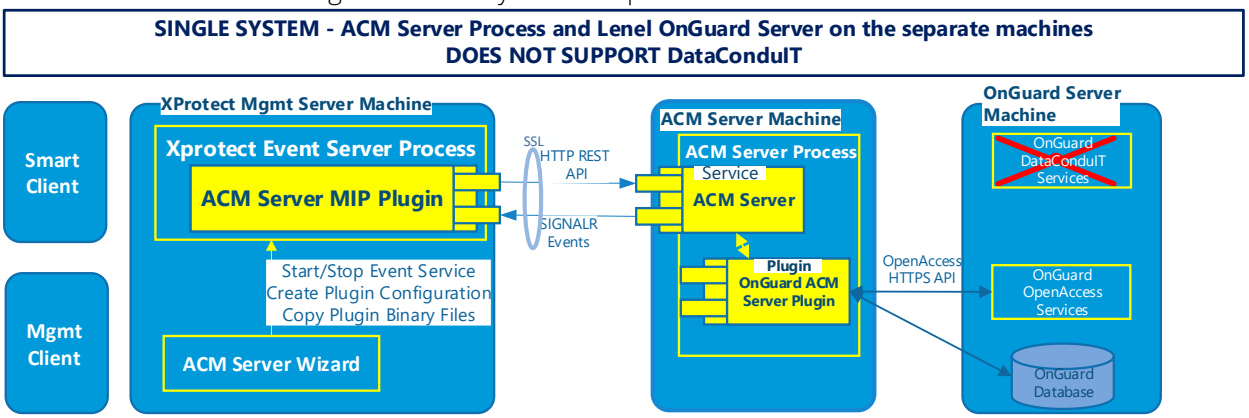


For design, scaling and performance reasons, we do not support connecting multiple XProtect sites to the same ACM Server instance.



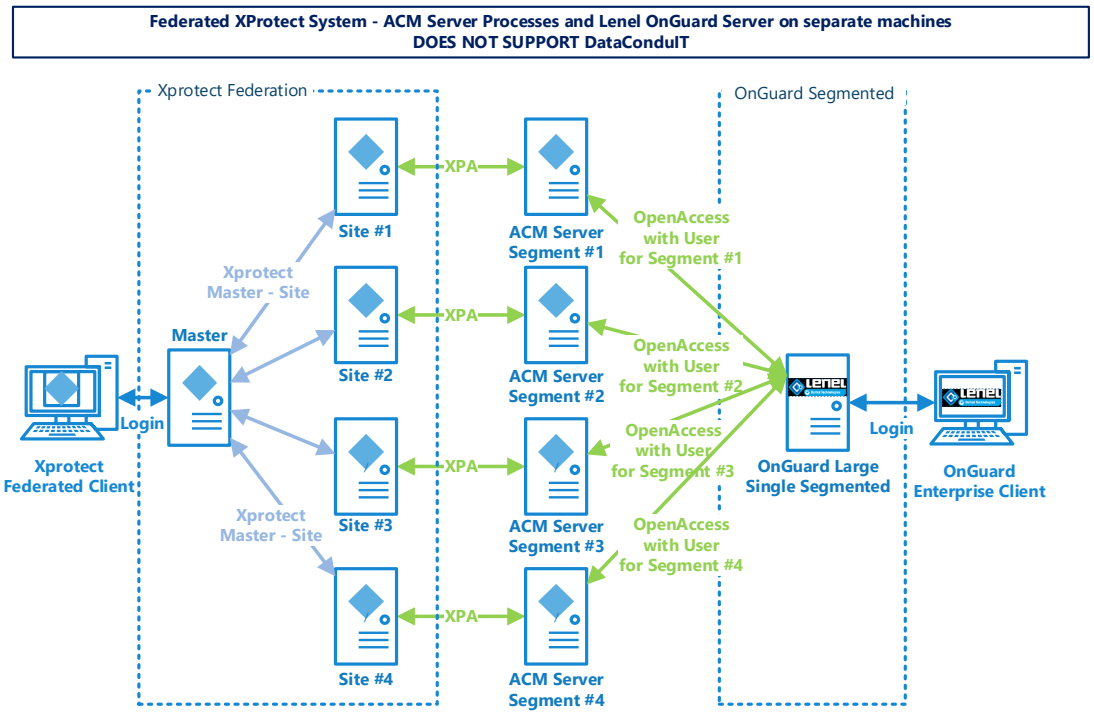
Single system – ACM Server and OnGuard Server on separate machines (OpenAccess ONLY)

This configuration is used where there is a need to run the ACM Server on a different machine than the OnGuard Server. This configuration is only valid in OpenAccess mode.



Milestone XProtect®: Federated with Single Large Segmented OnGuard (OpenAccess ONLY)

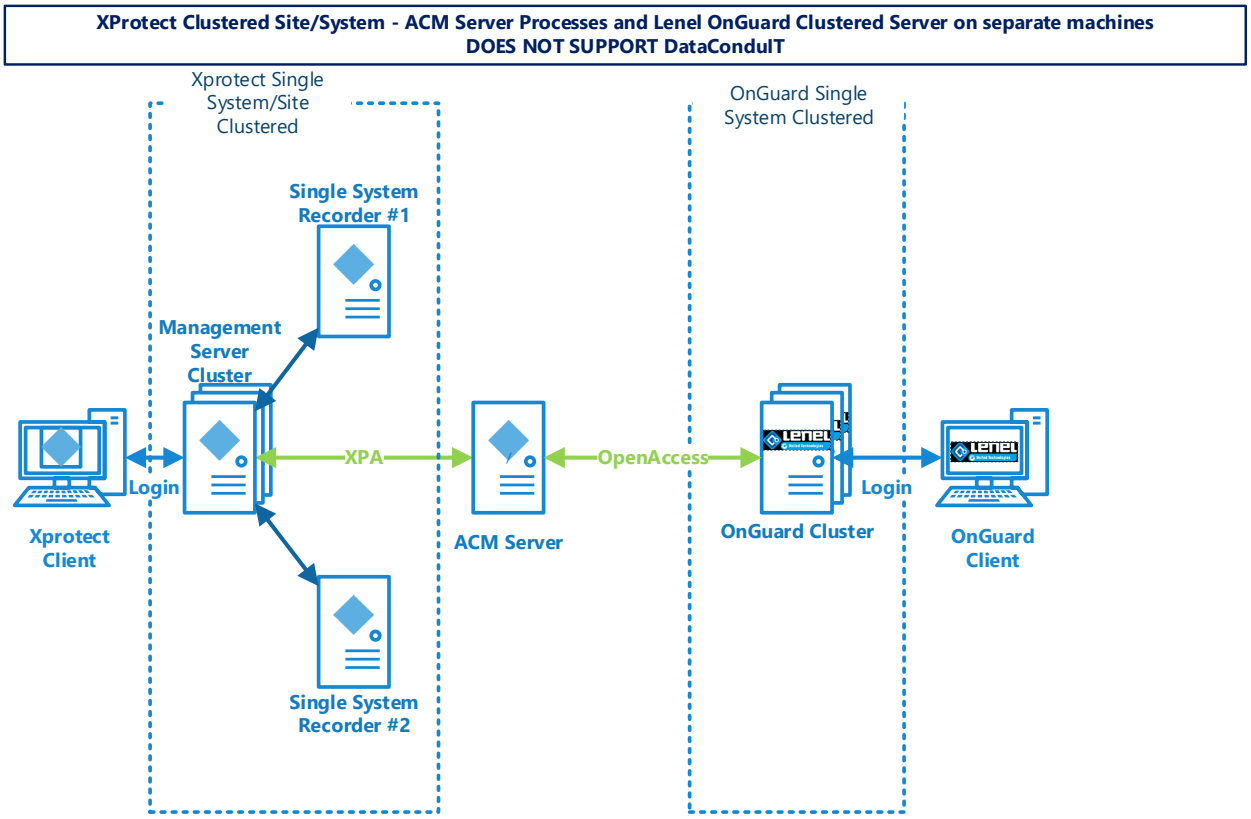
With a Federated Milestone XProtect installation, each XProtect site must be connected to their own ACM Server instance. In the case where one large OnGuard system is used, it isn't always practical to have all the doors on one XProtect system when you need to assign certain cameras on a specific system to a door on a different one. This scenario could be used for those reasons. The ACM Server(s) has to be configured to run on a machine separate from the OnGuard server, like so:



Of note, each OpenAccess connection to the segmented system, uses a different user in OnGuard configured to only see the segment relevant to the corresponding XProtect system.

Milestone XProtect®: Clustered with Single Clustered OnGuard (OpenAccess ONLY)

When clusters come into play, ACM Server has to be removed from both the XProtect and OnGuard server machines. This is what a scenario like this would look like if both software were clustered:

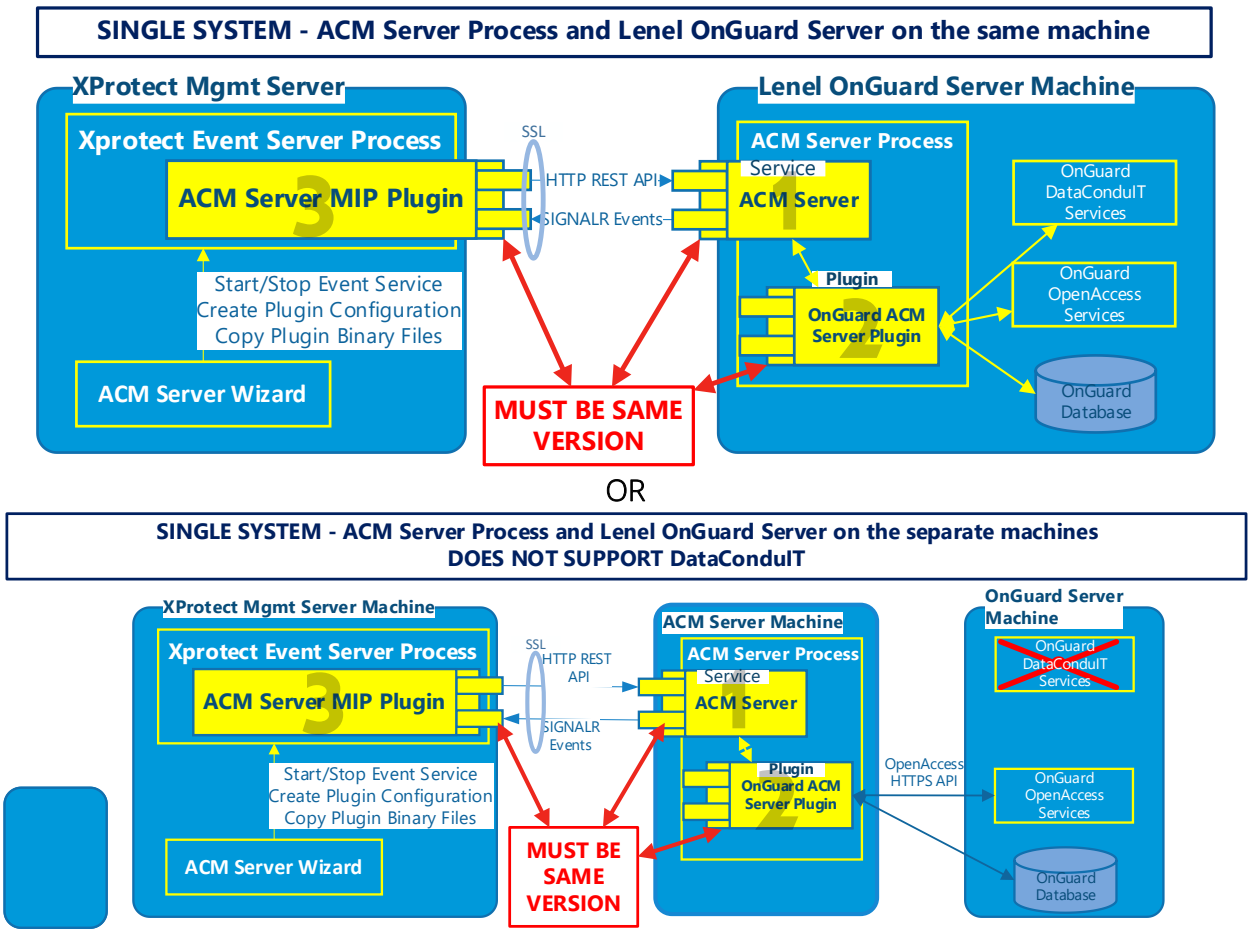


Installation

The installation package consists of three independent installers:

1. Milestone.ACMServer.msi: Installer for the ACM Server
   - Installed on the OnGuard server machine(DataConduIT) or its own machine (OpenAccess ONLY)
2. Milestone.ACMServer.OnGuard.msi: Installer for the OnGuard ACM Server plugin
   - Installed on the OnGuard server machine (DataConduIT), after the ACMServer. On its own machine (OpenAccess ONLY) on the same machine as 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

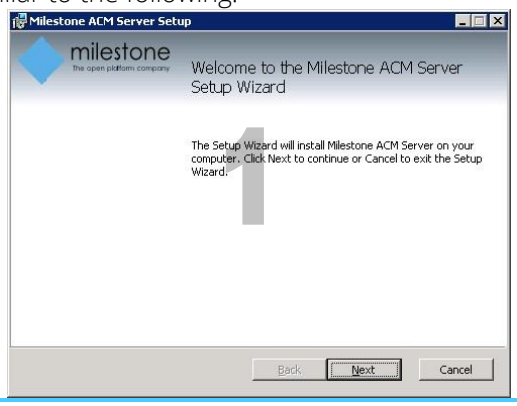
Please install them in the order specified above, following completion of the prerequisites section. See the Alternative Installation Configuration for an alternative configuration available for OpenAccess installations.



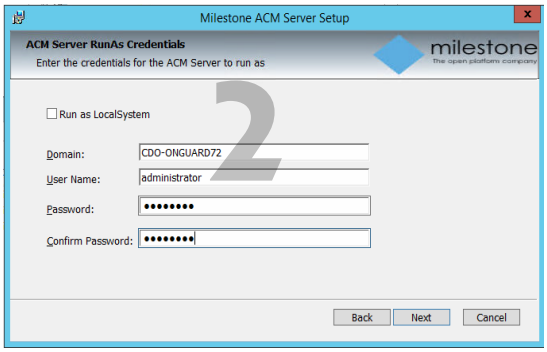
It is mandatory that the *same version* of the OnGuard ACM integration be installed on both the XProtect and OnGuard machines.

ACM Server Installation

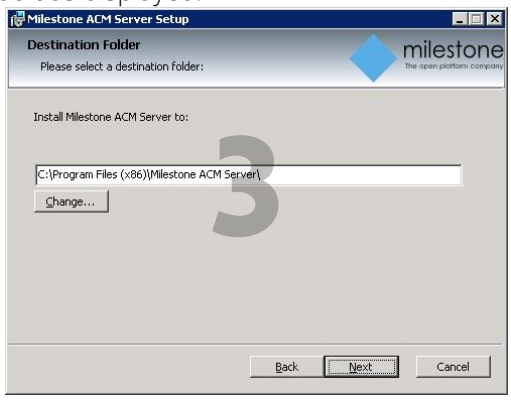
Double-click to install, you should see a screen similar to the following:



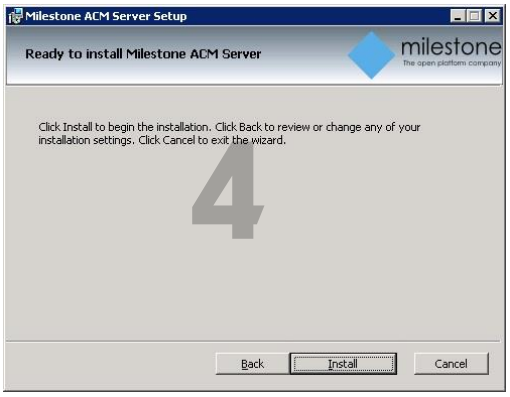
If using DataConduIT, you must enter the SSO credentials that will be used for the DataConduIT connection to OnGuard.



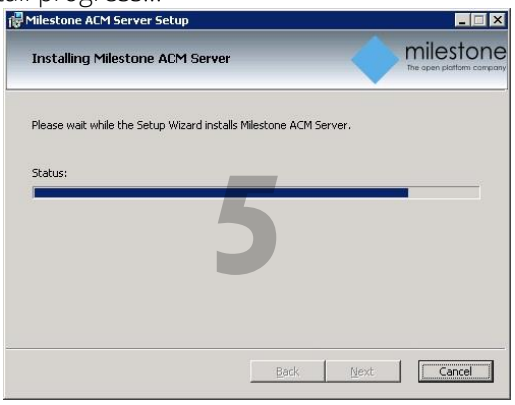
Press next and you will now be able to select the installation path, it is recommended to use the default as displayed:



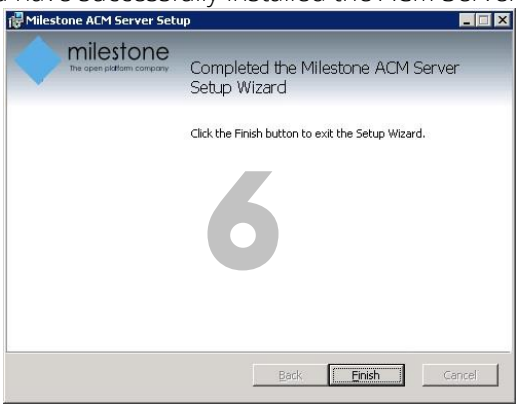
Press next and you are now ready to install, if you are satisfied with the selected options, press install to continue:



Install progress...



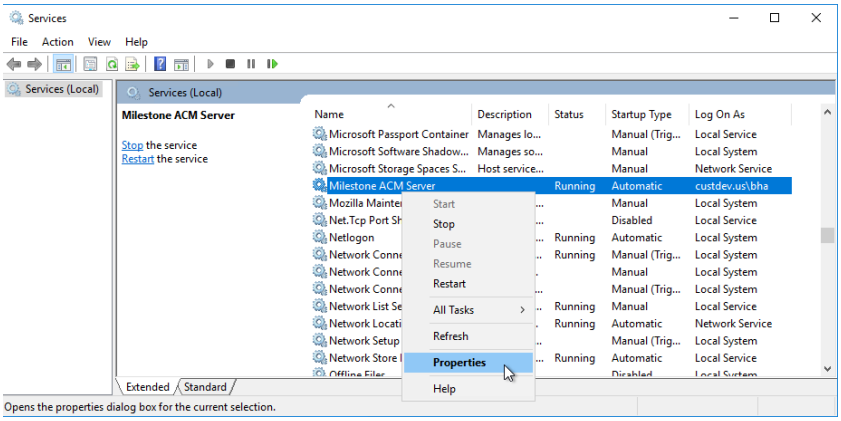
You have successfully installed the ACM Server:



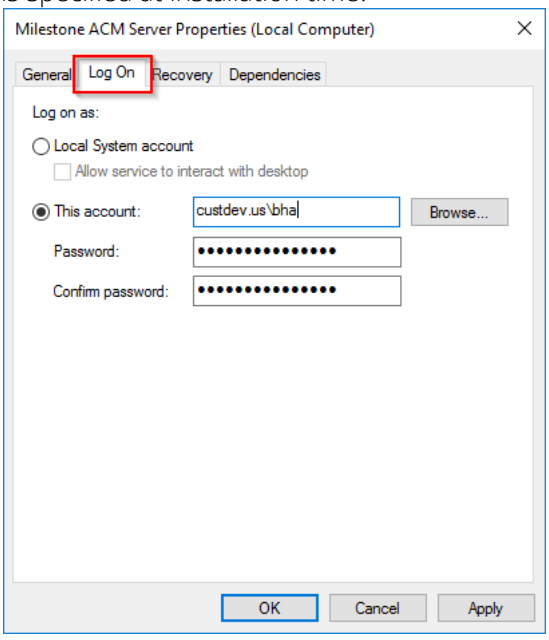
ACM Server Credentials

If you need to verify and/or modify the credentials the ACM Server service will be running as for DataConduIT connections do the following:

1- Open Windows Services, right-click properties on the Milestone ACM Server entry

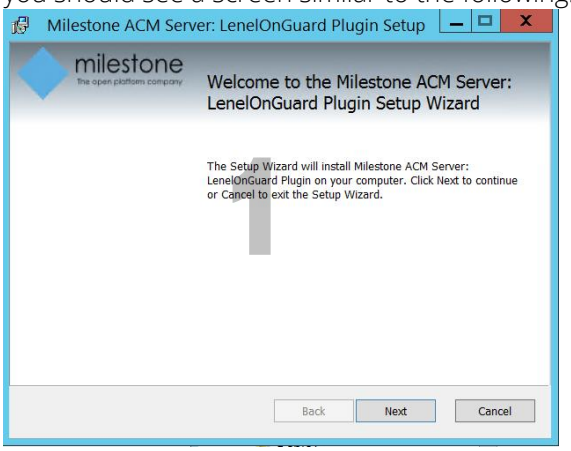


2- Go to Log On tab, select "This account", and enter/change the SSO credentials that will be used for the DataConduIT connection to OnGuard. You should only need to do this in case you need to modify the credentials specified at installation time.



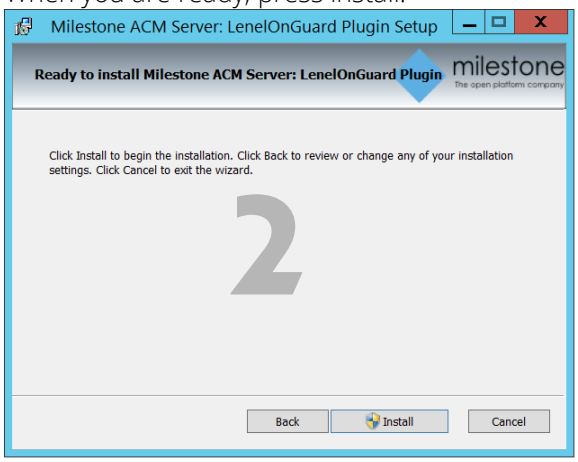
ACM Server: OnGuard Plugin Installation

Copy the "Milestone.ACMServer.OnGuard.msi" file to a temporay folder and double-click to install, you should see a screen similar to the following:

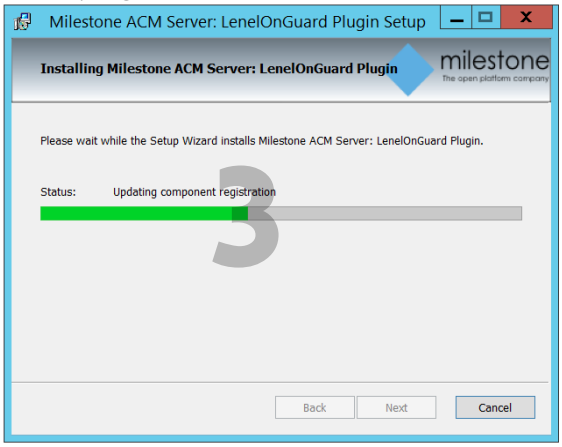


The OnGuard plugin automatically detects the presence of both the OnGuard server and the pre-installed ACM Server. If either is missing it will refuse to install.

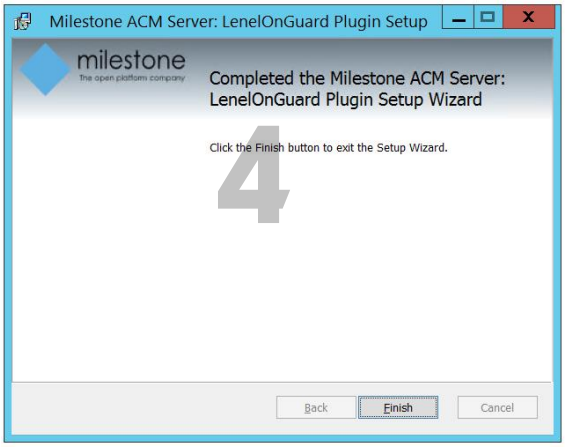
There are no configurable options in this installer. When you are ready, press install.



Install progress...

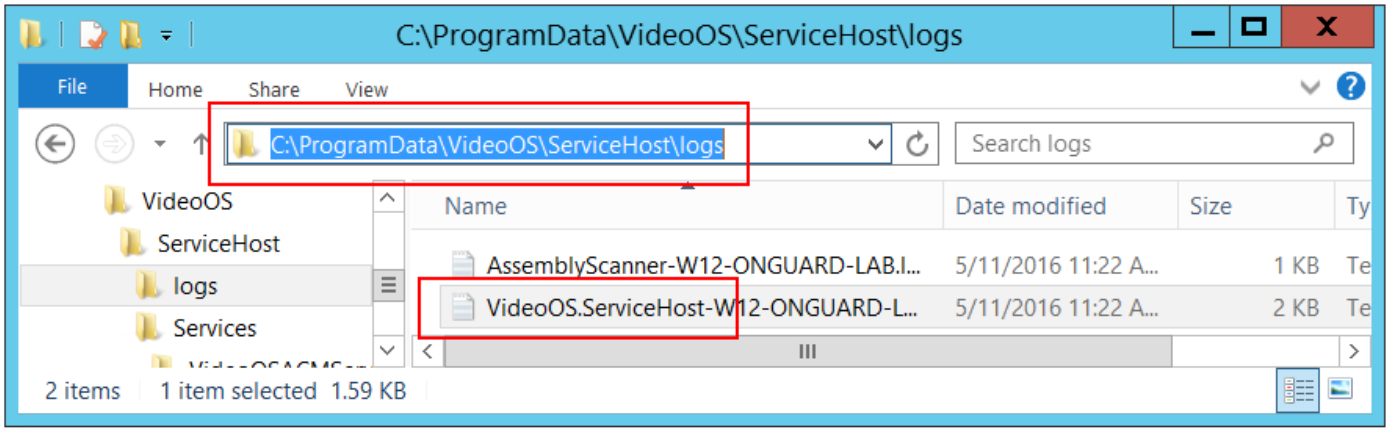


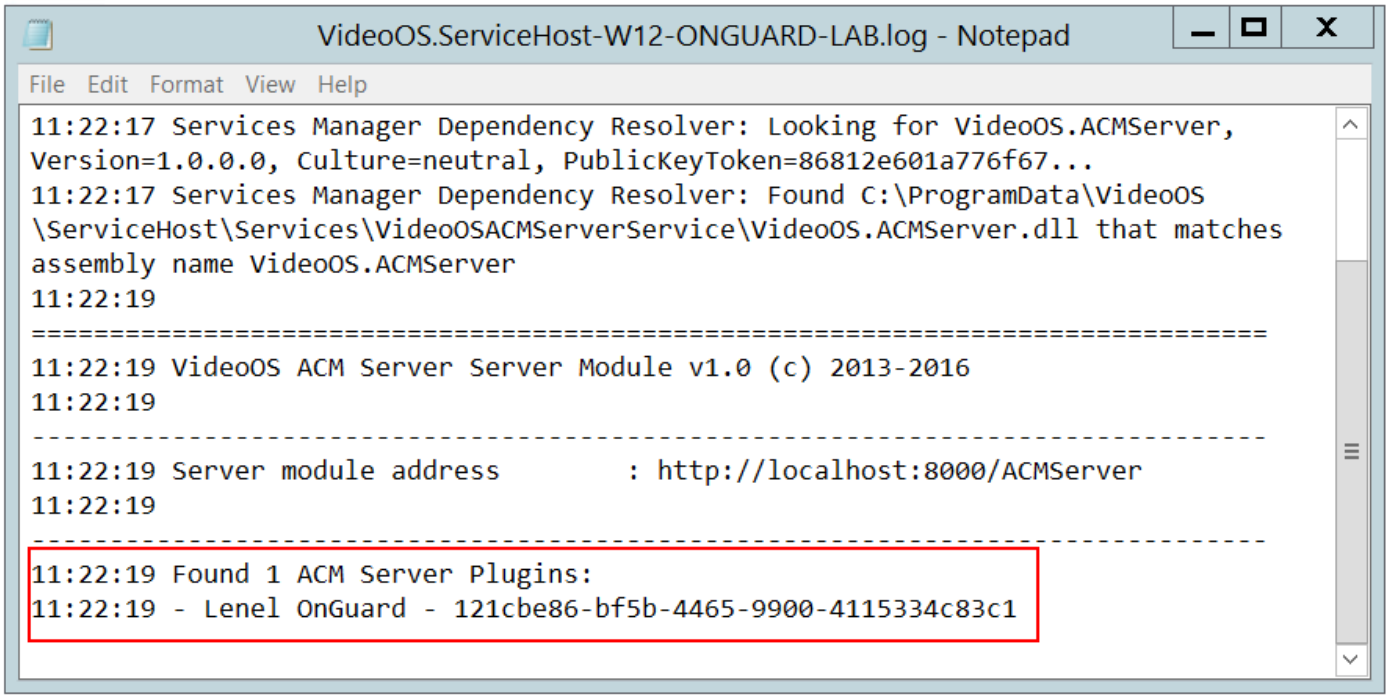
You have successfully installed the Milestone ACM Server OnGuard Plugin



ACM Server: OnGuard Plugin Post-Installation

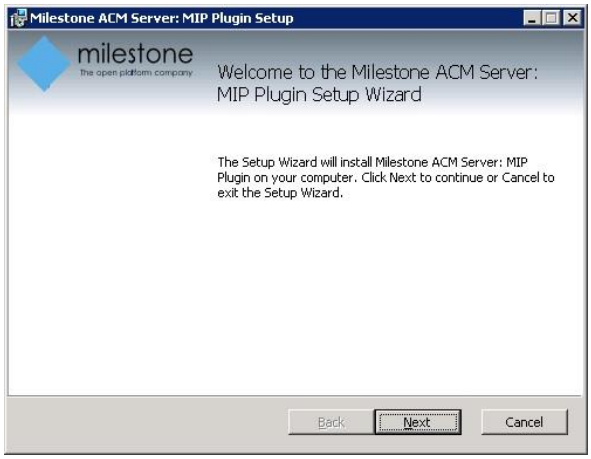
You can verify that the OnGuard Plugin is installed and loaded from the logs below:



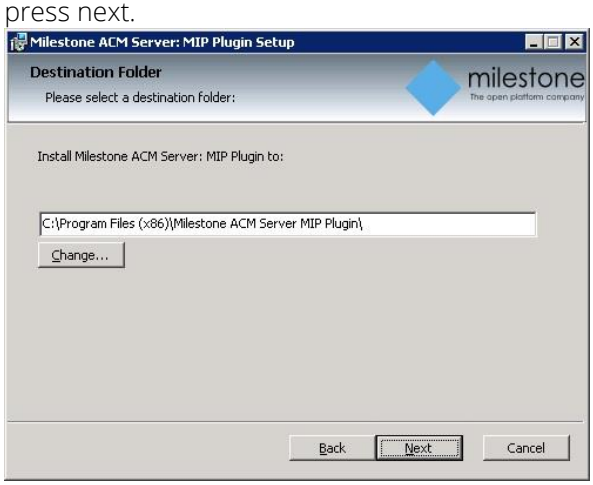


ACM Server: XProtect ACM MIP Plugin

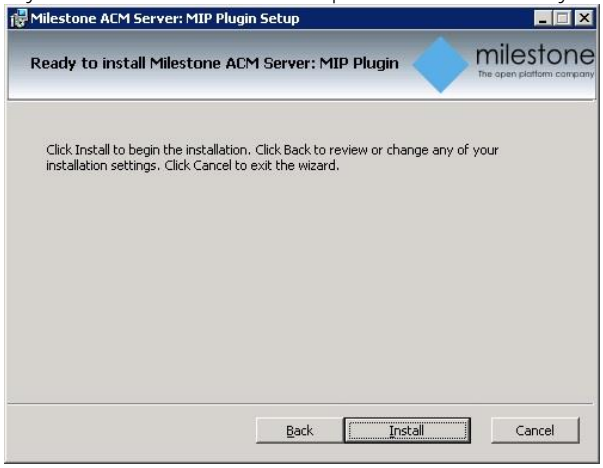
Copy the "Milestone.ACMServer.MipPlugin.msi" file to a temporay folder on the server where the XProtect Event Server is installed (in a typical deployment, this is the XProtect Management Server) and double-click to install. You should see a screen similar to the following:



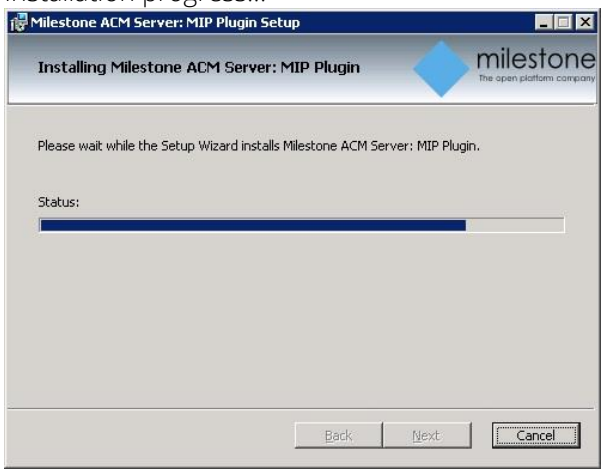
The installer will detect the presence of the XProtect Event Server on the machine and will refuse to install if it cannot be found. It is recommended to leave the default install path as displayed below and press next.



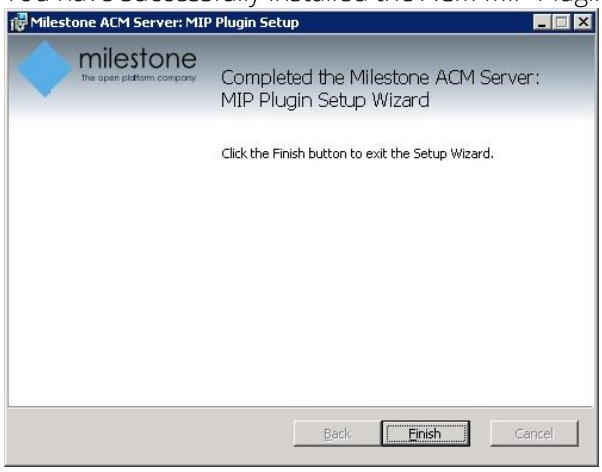
If you are satisfied with the path selection and you are ready to install press "Install"



Installation progress...

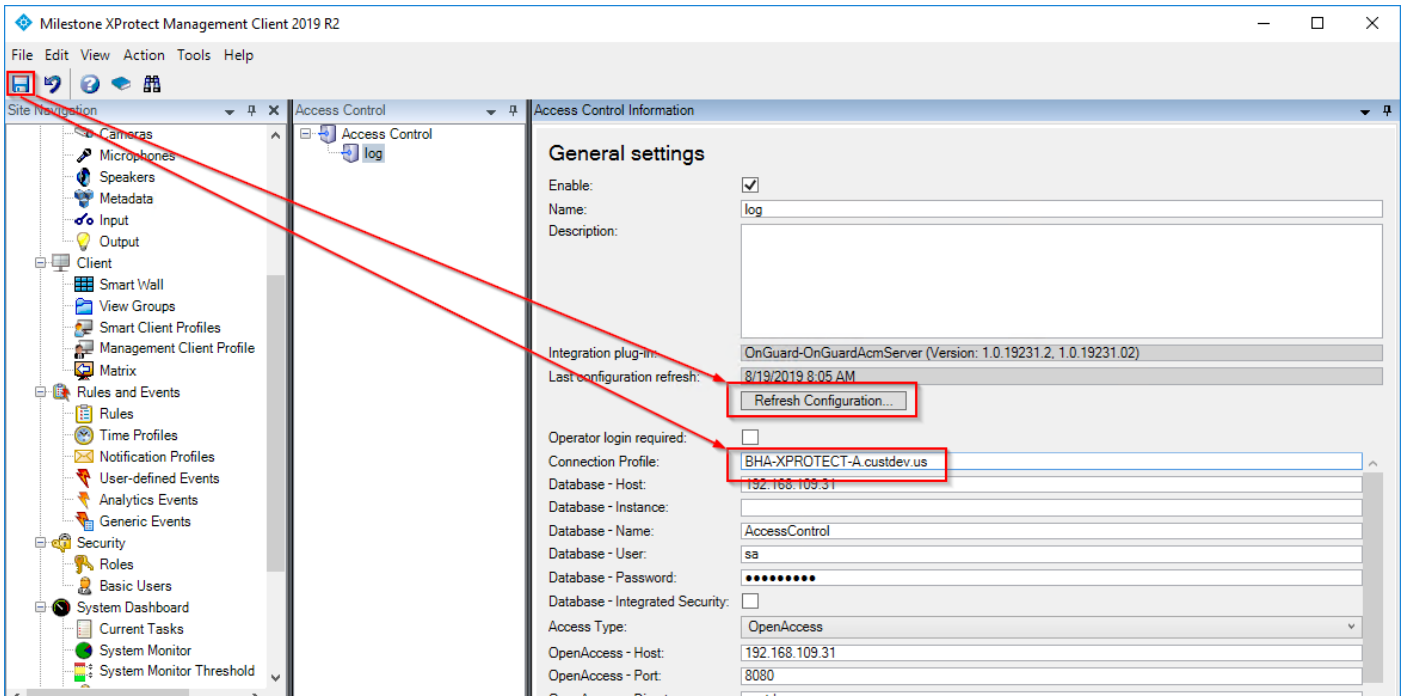


You have successfully installed the ACM MIP Plugin for ACM Server



MIP Plugin Upgrades

- IMPORTANT – Always upgrade *both* the ACM Server and OnGuard ACM plugin on the OnGuard machine *before* upgrading the MIP Plugin. We distribute all the installers with every new OnGuard ACM release.
- 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 will result in the following negative side-effects:

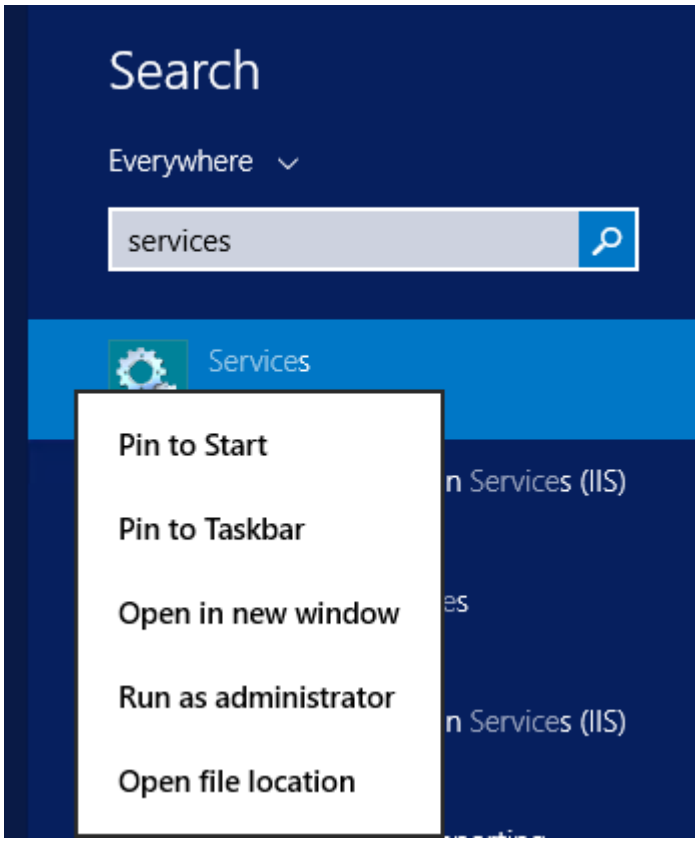
- Smart Client event history will be lost.
- Rules based off events and configured OnGuard hardware will no longer function. Rules based off the default access control event categories will not be affected and will continue to function.
- Custom event category assignments will be lost. The custom category will still exist; the user will just have to re-assign the category to events in the Management Client.

OnGuard Configuration

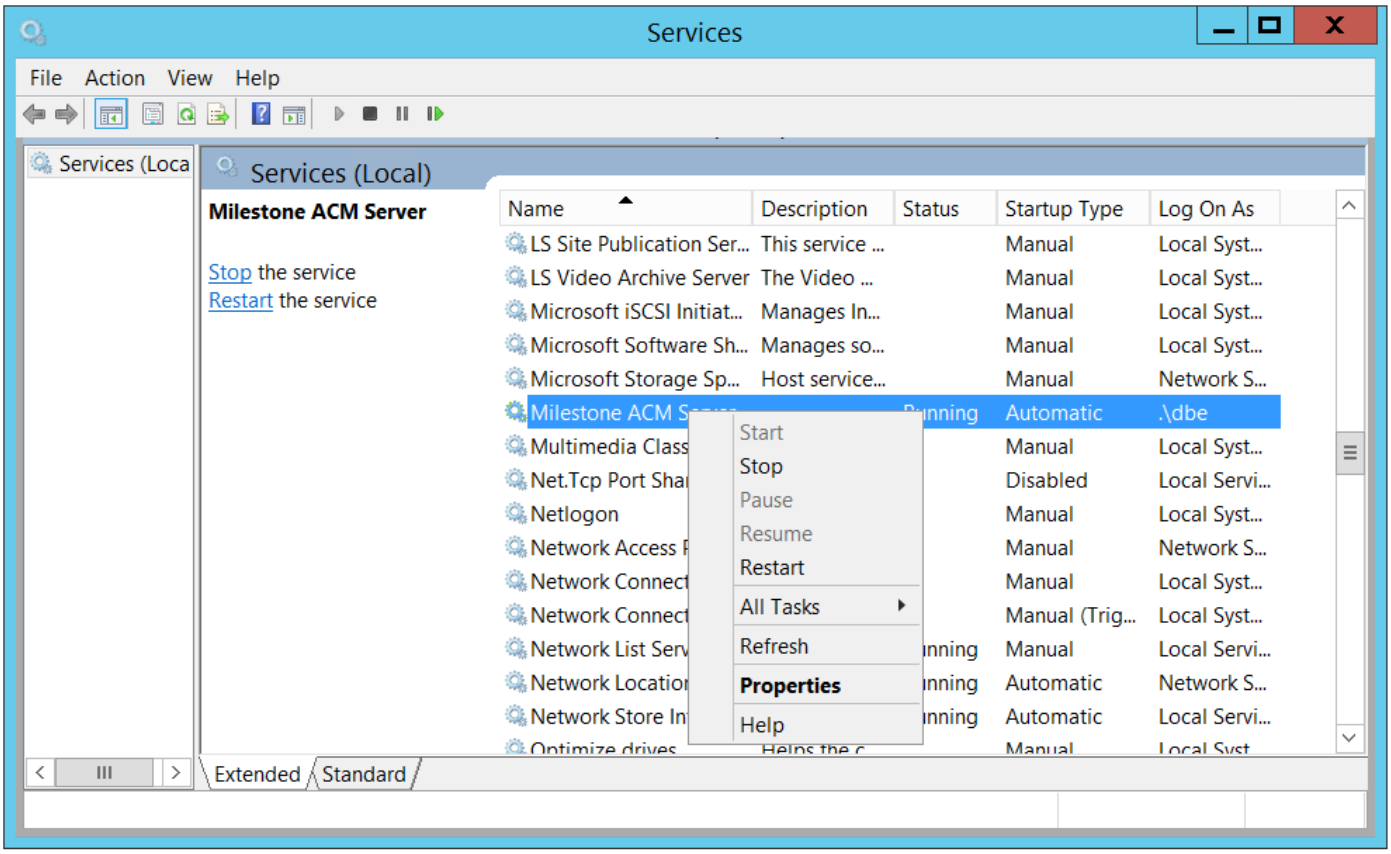
Configure to run as OnGuard Single-Sign-On Account

The OnGuard Plugin installer has already configured the ACM Server to run as the single sign-on account. You only need to do the following if you need to change the ACM Server's credentials.

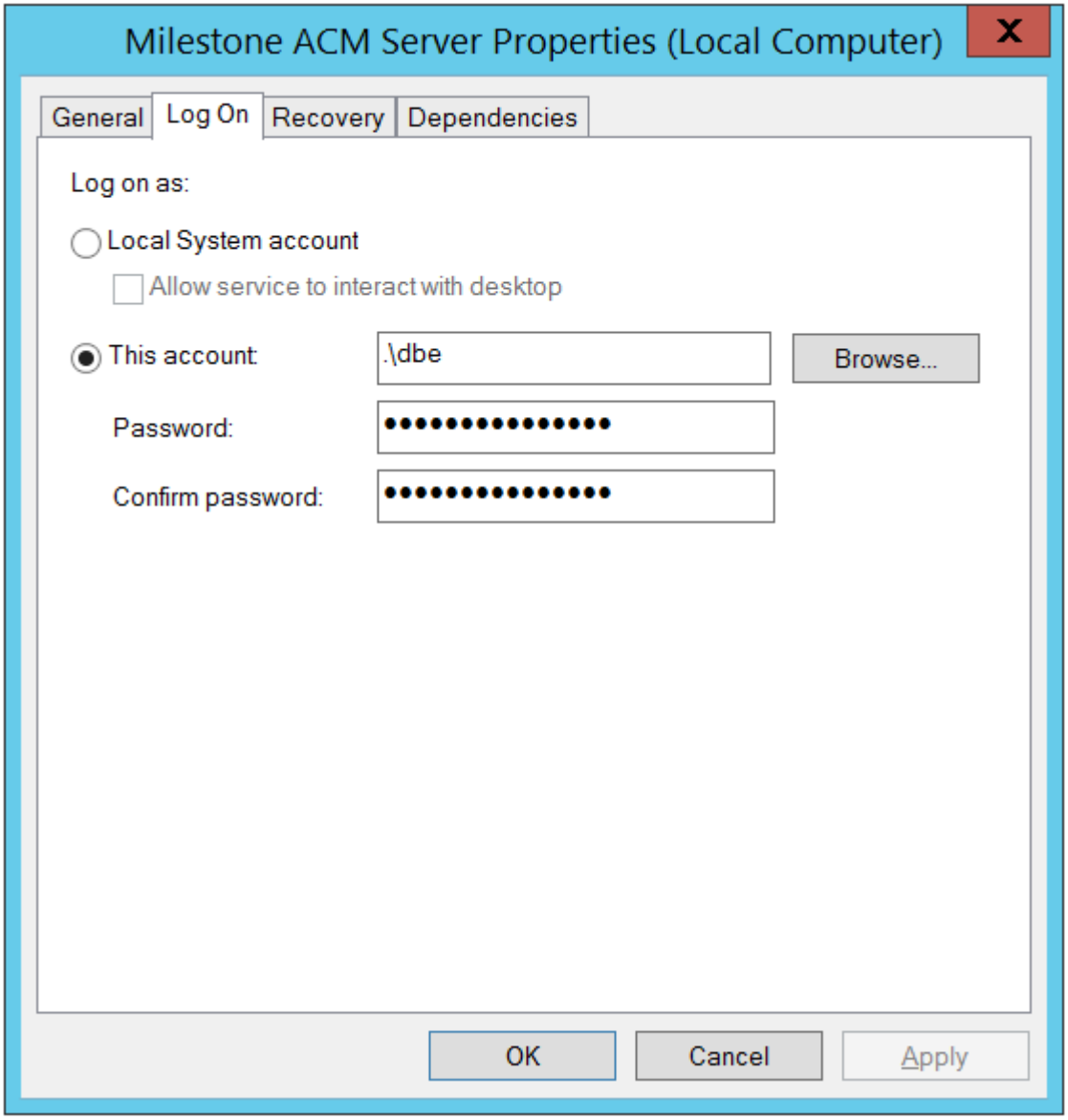
On the OnGuard server machine, click the Windows Start menu and type "services". Right click Services and select "Run as administrator".



Right-click the Milestone ACM Server service and select Properties:



Click the "Log On" tab, select "This account", and enter the credentials of an admin user on the local machine. Note that this admin user ***must*** be linked to a OnGuard Directory that is configured for single sign-on (see above for configuring single sign-on).



IMPORTANT: Restart the Milestone ACM Server service.

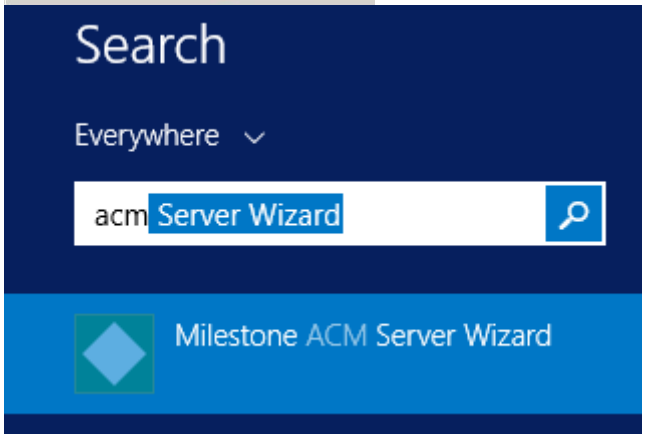
Reducing Permissions

It is not recommended to reduce the OnGuard Sql Server database permissions of the single sign-on user since we don't know exactly what the minimum permission set is. If you want to reduce the single sign-on user permissions, contact OnGuard Support.

XProtect ACM MIP Plugin Configuration

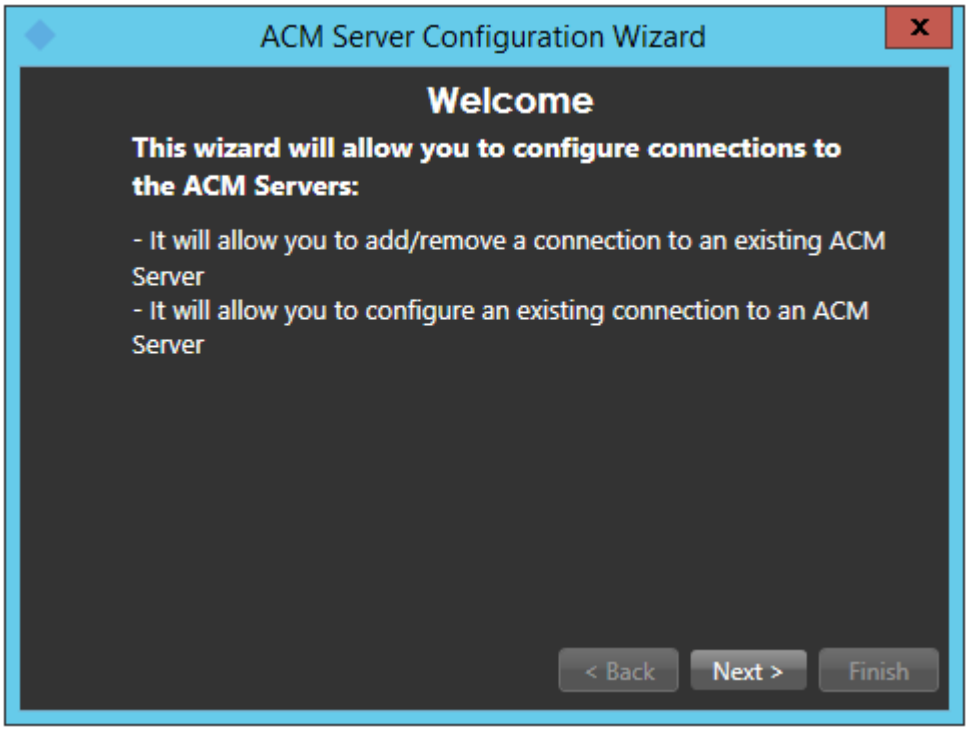
ACM Server Wizard

Once all three installers have been setup (see Installation section), it is now time to configure and install the ACM MIP Plugin in the XProtect Event Server. This configuration and deployment is handled by a wizard tool that was installed with the XProtect ACM MIP Plugin package. In the start menu you will find the following:

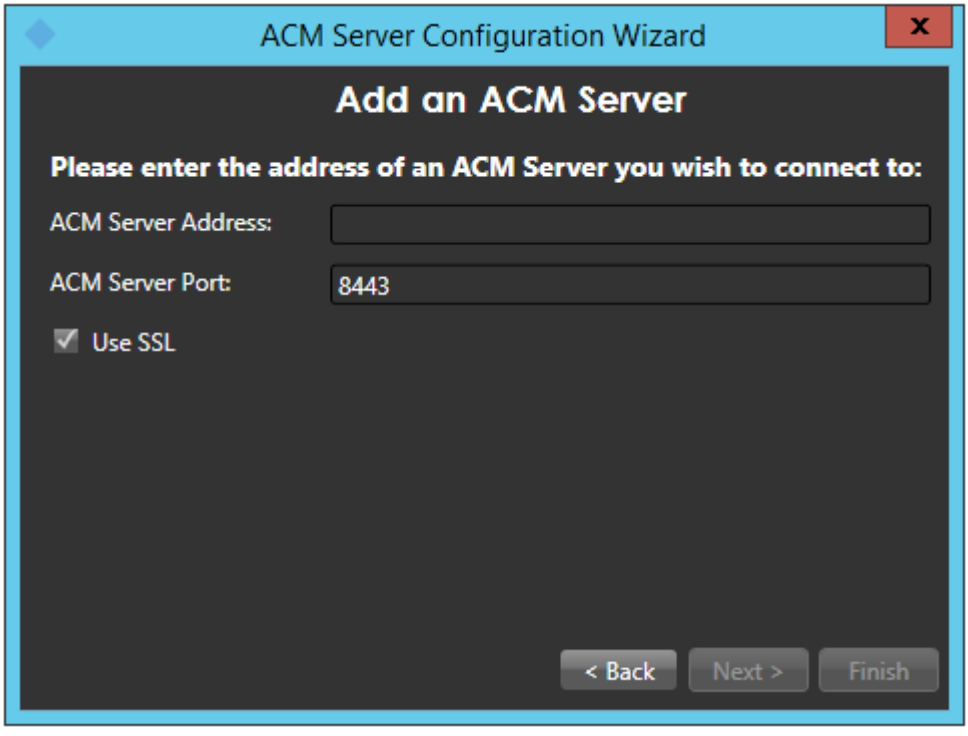


Installing an ACM Server

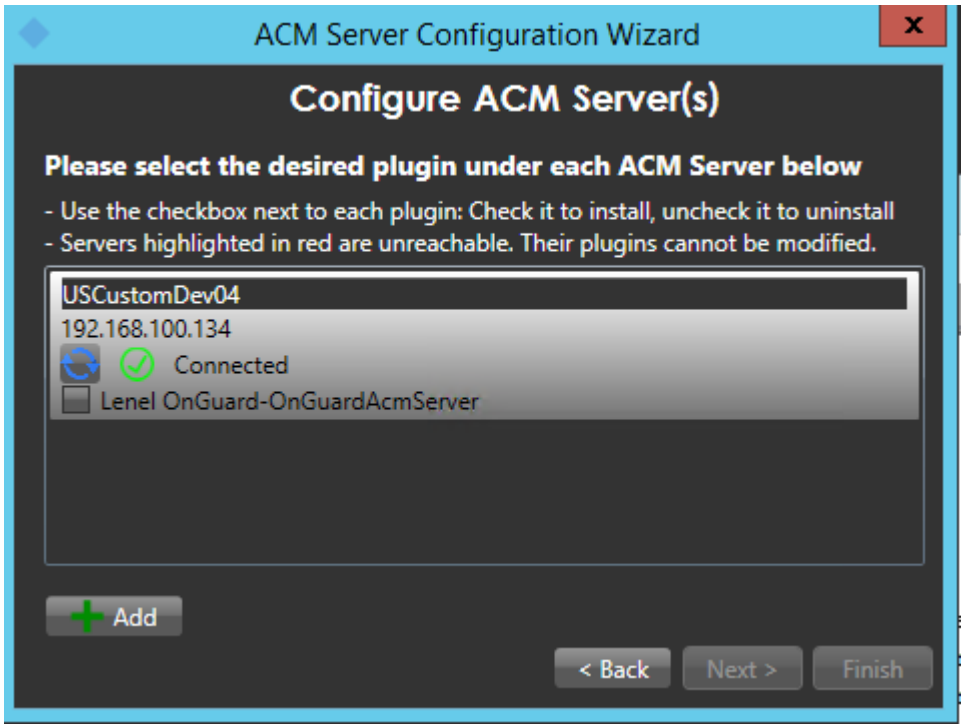
Once you start the wizard application you will see the following:



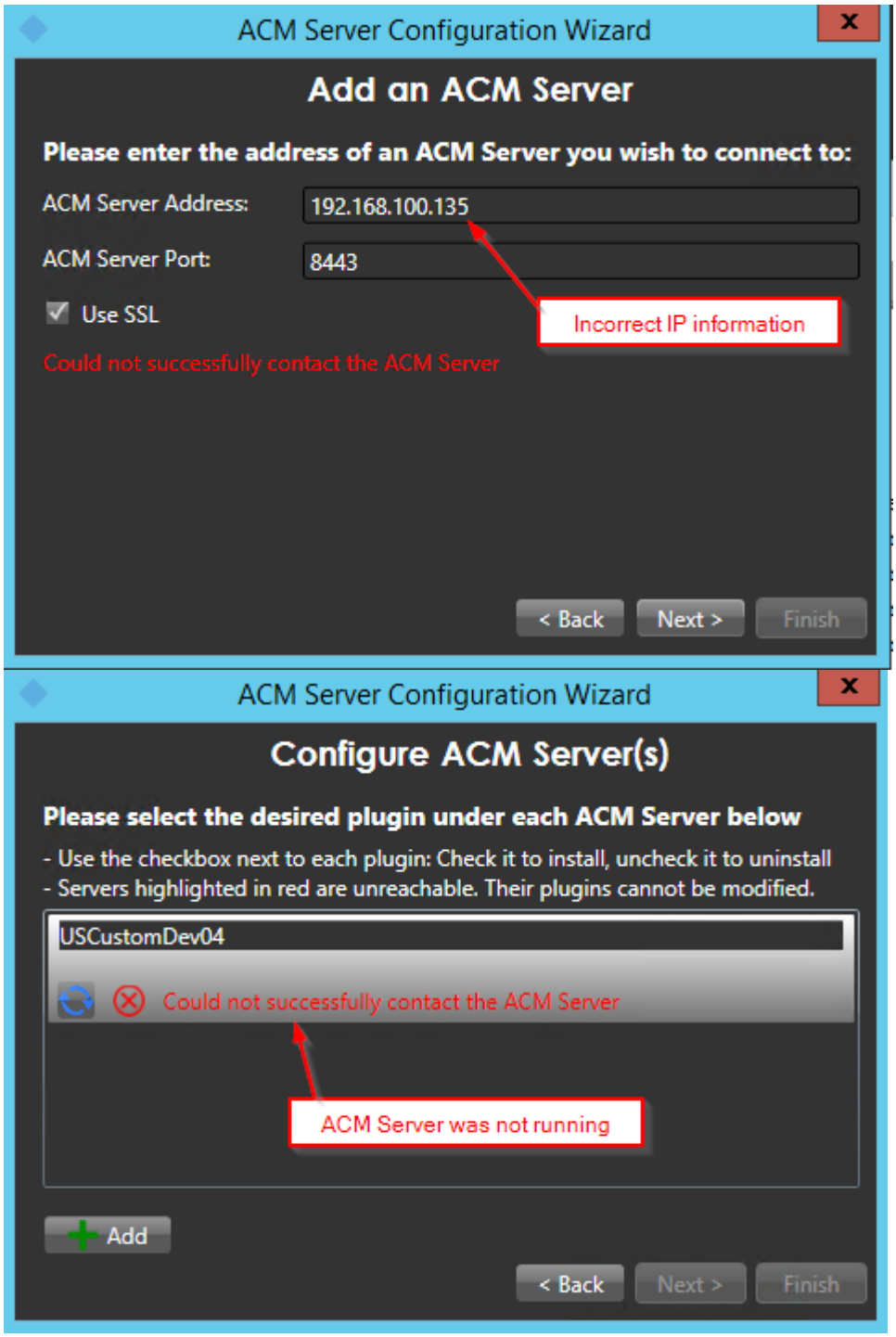
Once you click next, you will have to provide the IP Address / Machine name of the OnGuard server on which the ACM Server package was installed. If you have an integration server that you installed ACM Server on (described in Alternative Installation Configuration), use the IP Address or Machine name of the integration server instead.



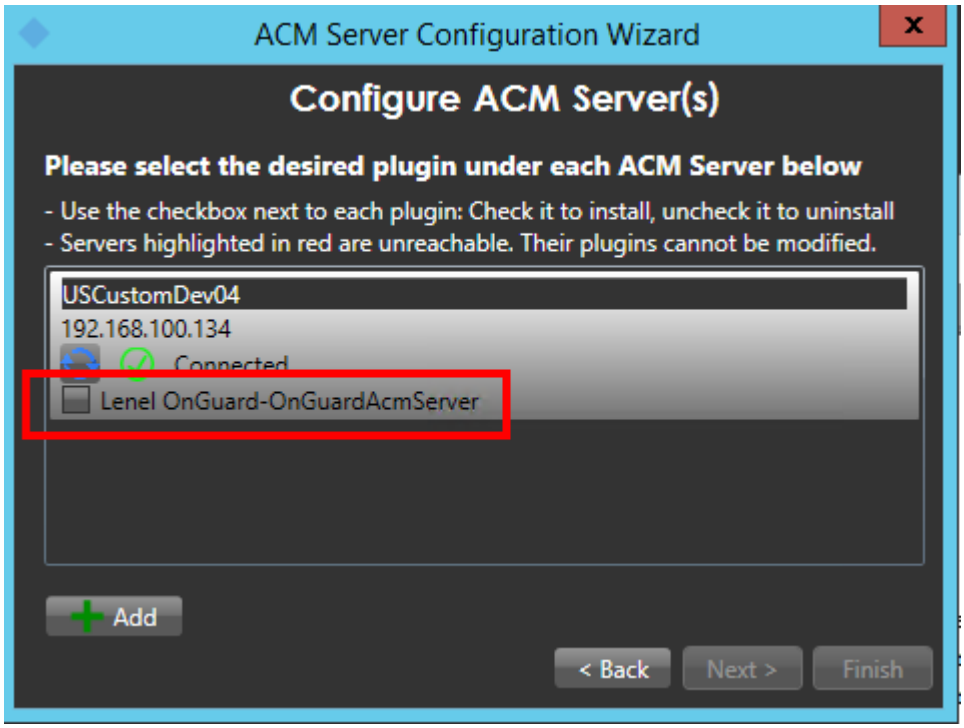
After you have provided the server name/ip address and pressed next, you should get the following screen after the software has validated that there is an ACM Server present at that address. The green checkmark means that it has successfully connected to the provided server name, the red x means that it failed to connect to the provided server. The wizard will not allow you to proceed without a valid connection to the server.



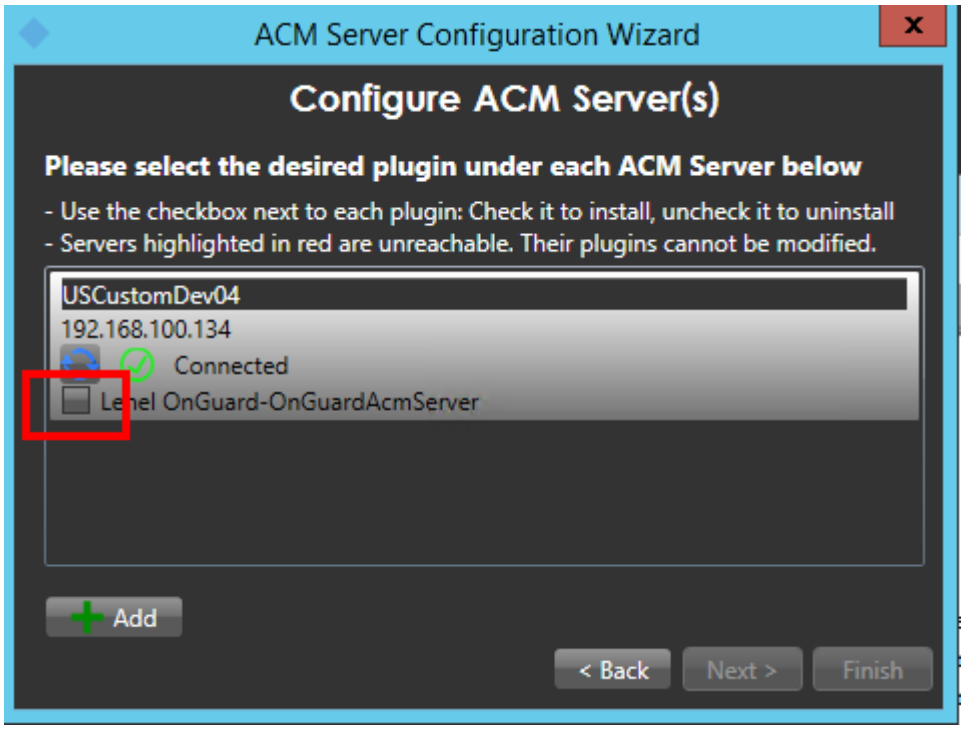
Note that the most common causes of the wizard not being able to connect to the provided server is that 1) you entered the wrong IP information, or 2) the ACM Server is not running with sufficient administrative privileges.



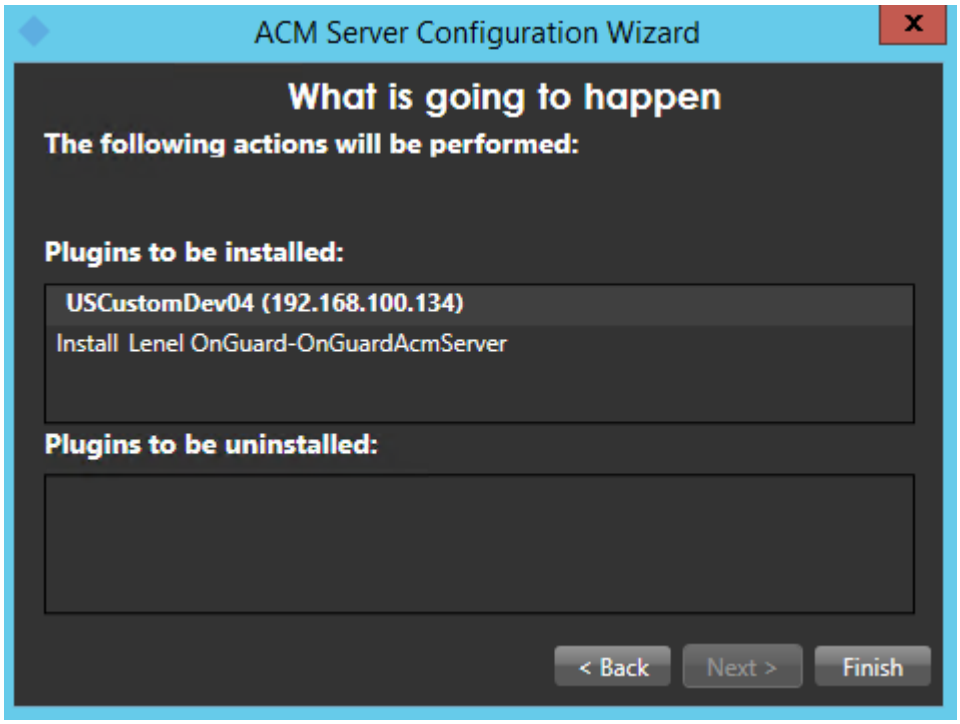
Once you have a successful connection, notice that there is a list of checkboxes under the server heading that represents all detected ACM server plugins installed on that machine. In this case we are looking for OnGuard.



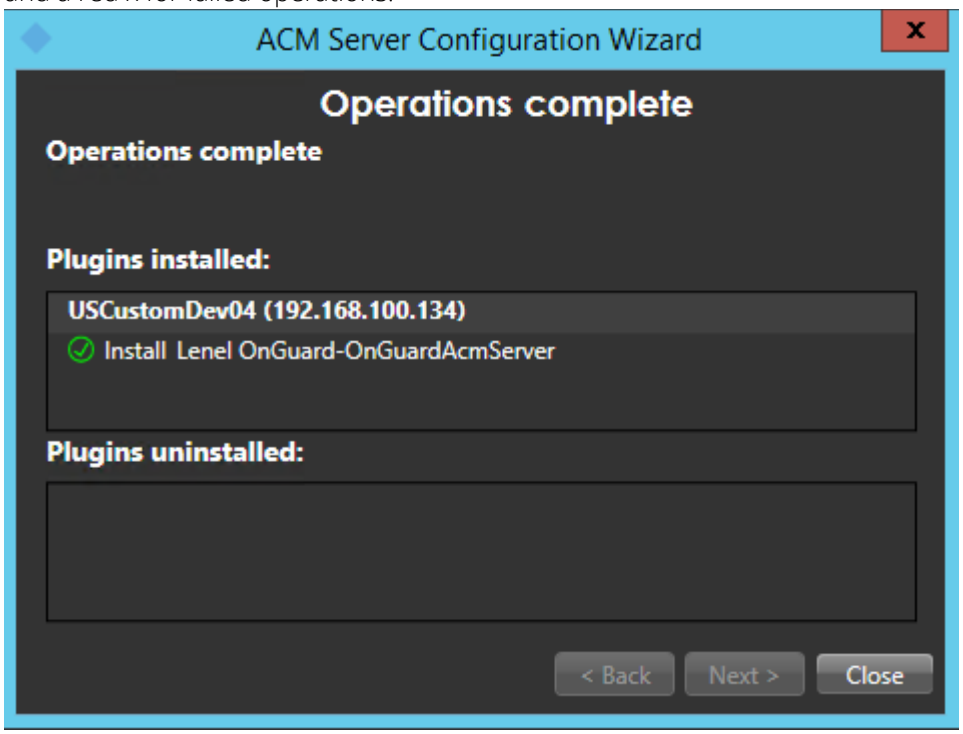
Check the box marked below and press next to install a MIP plugin on this host to connect to the OnGuard server identified.



This screen will confirm what actions are going to happen. Once you are ready to install, press finish.



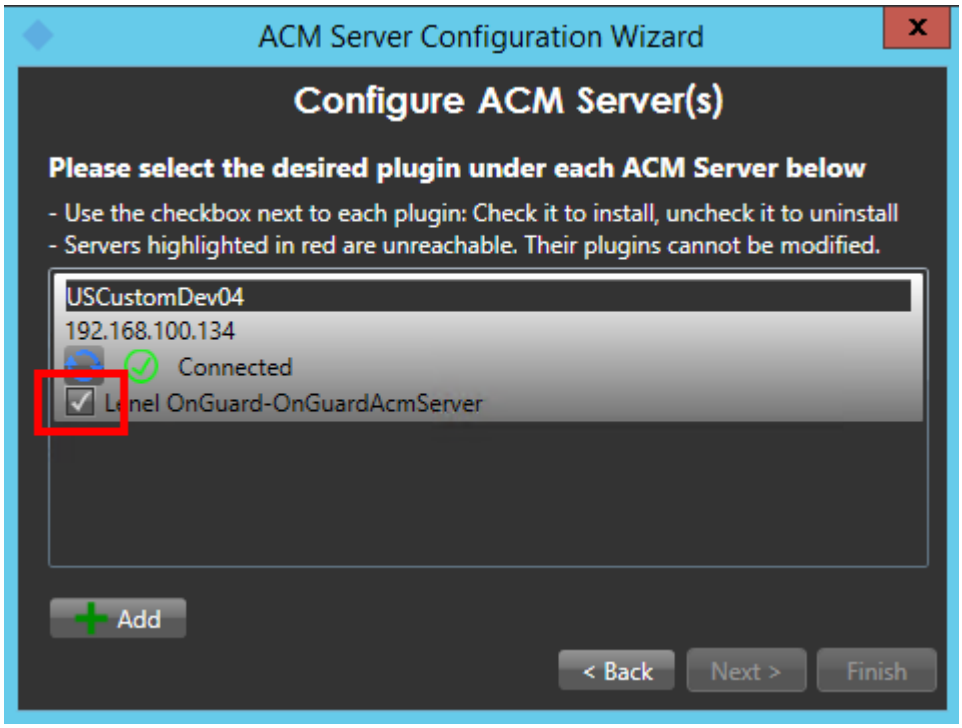
Once the operations are completed, the wizard will display a green checkmark for successful operations and a red x for failed operations.



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

Uninstalling an ACM Server

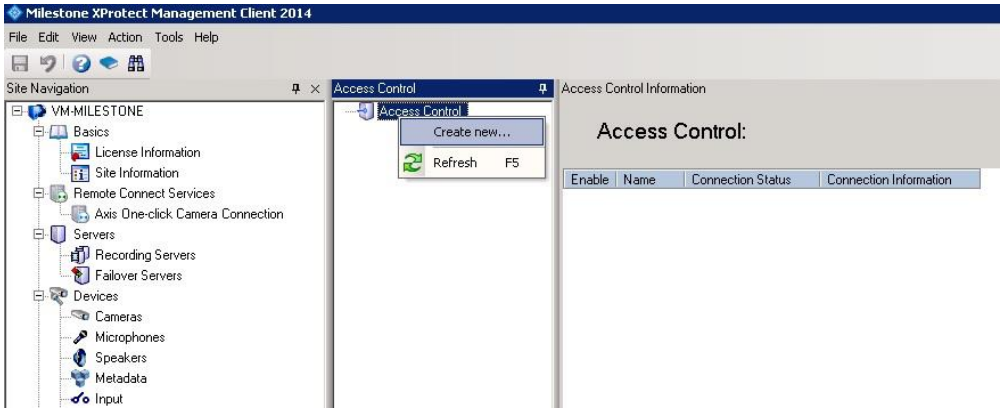
To uninstall an ACM Server, simply uncheck the box shown below, click Next, and click Finish.



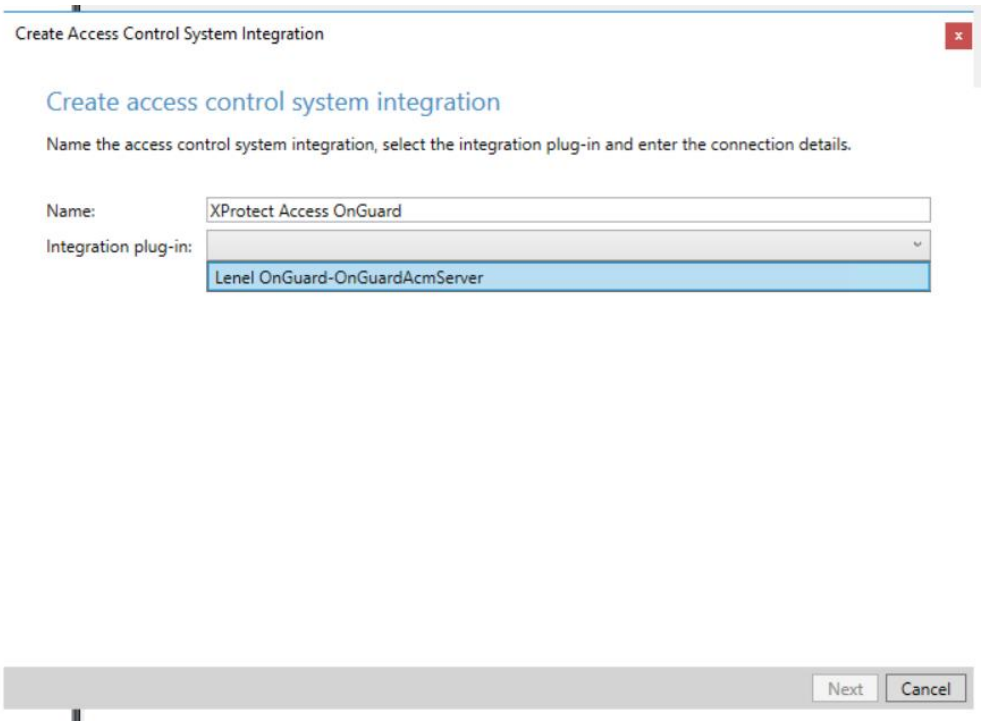
XProtect Management Client Configuration

XProtect Management Client

Once the MIP ACM Plugin is installed and configured on the XProtect Management Server, the Access Control instance can be created in Management Client by right-clicking on the Access Control Root Node.

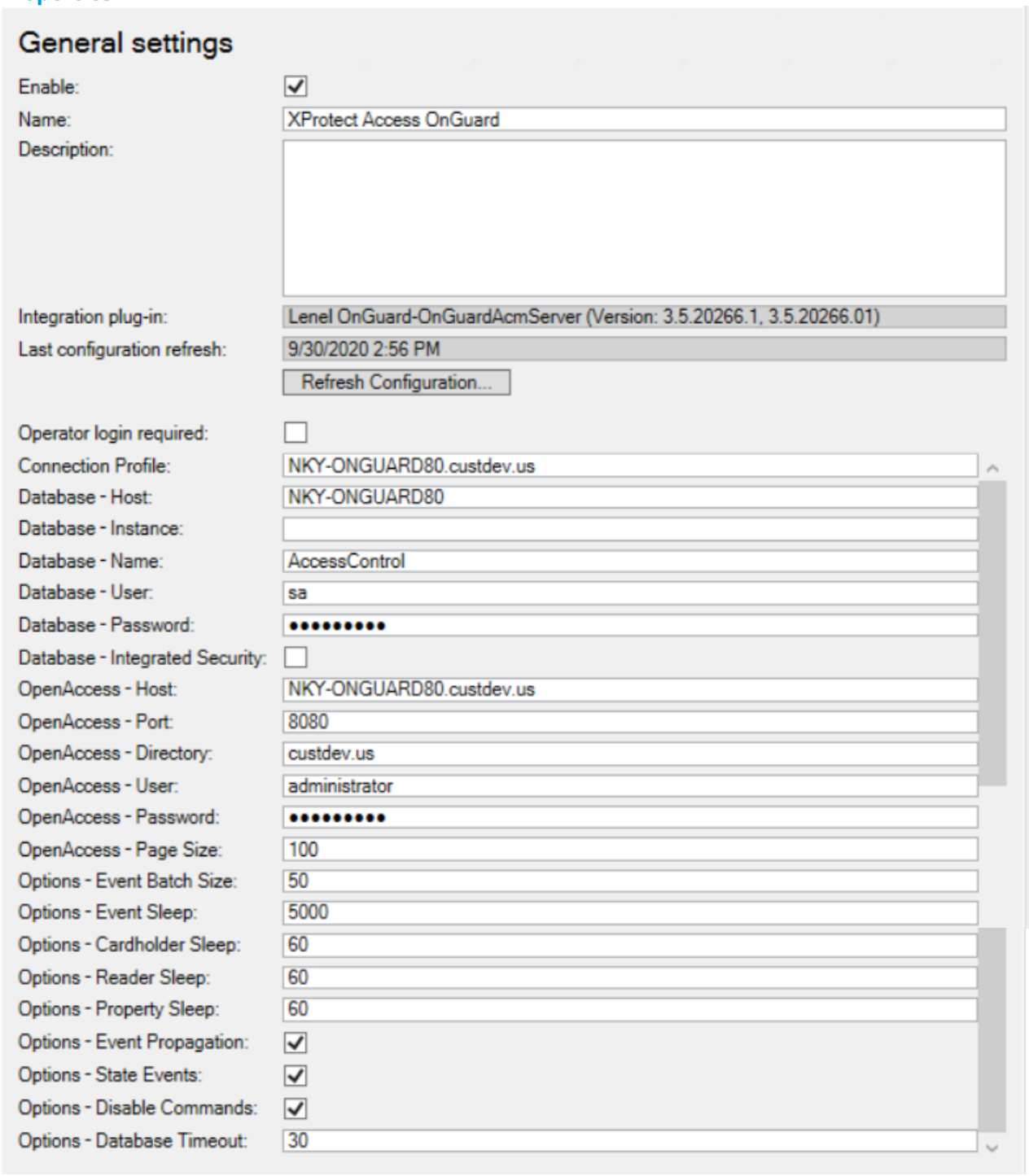


This will pop up a wizard to step you through the access control instance creation process. Type a name for the instance of the plugin you wish to create and select from the drop-down box the integration plug-in. Note that you will find a plugin named Lenel-OnGuardAcmServer-{ServerName} where {ServerName} is the name of the machine where OnGuard and ACM Server are installed.



After selecting the plugin, you will have to provide credentials and parameters to configure the connection to the OnGuard database server, optimize particular settings, etc.
Some of these settings only apply depending on your type of access, DataConduIT or OpenAccess. However, all the properties used for all versions of OnGuard are shown in the Management Client wizard.

Properties



Below, the properties are listed by access type.

All Access Types

Connection Profile

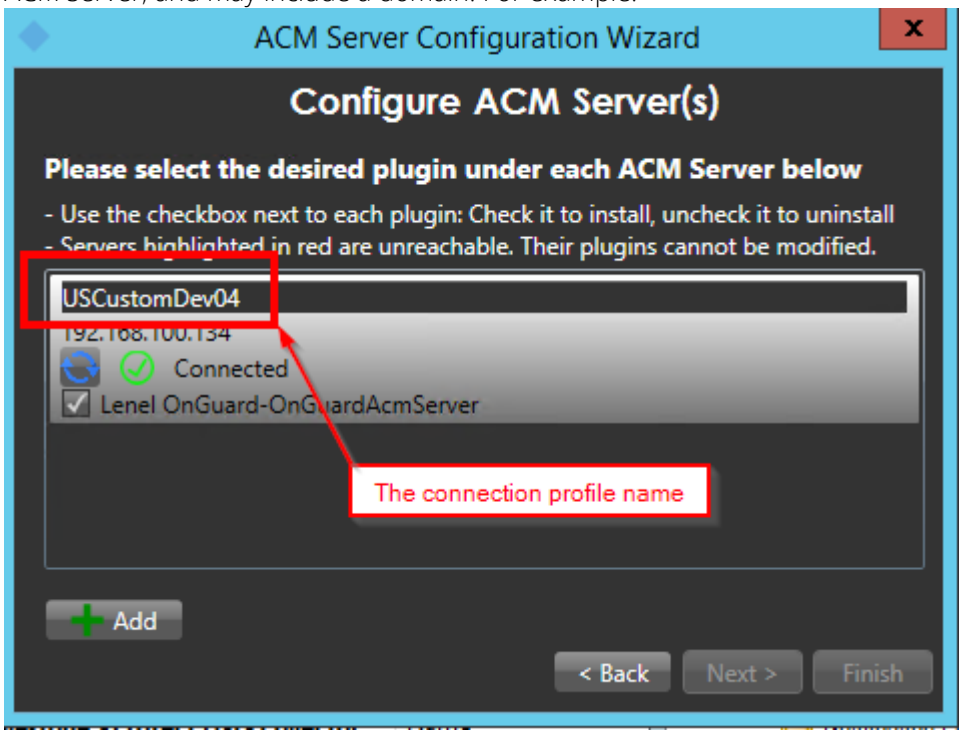
Database - Host

Database - Instance

Database - Name

Database - User
Database - Password
Database – Integrated Security
Options – Cardholder Sleep
Options – Reader Sleep
Options – Property Sleep
Options – Event Propogation
Options – State Events
Options – Disable Commands
DataConduIT only
Options – Event Batch Size
Options – Event Sleep
Options – Database Timeout
OpenAccess only
OpenAccess - Host
OpenAccess - Port
OpenAccess - Directory
OpenAccess - User
OpenAccess - Password
OpenAccess – Page Size

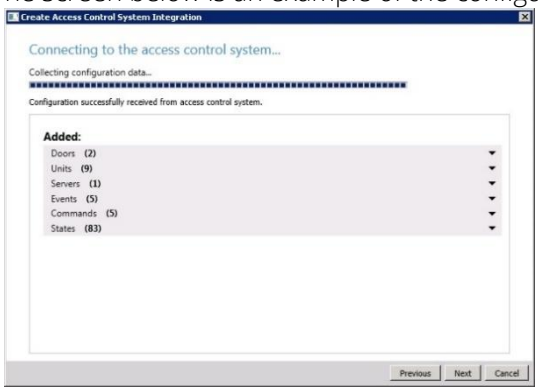
Property Details
Connection Profile – Should be set to the same as was shown in the ACM Wizard when you added the ACM server, and may include a domain. For example:

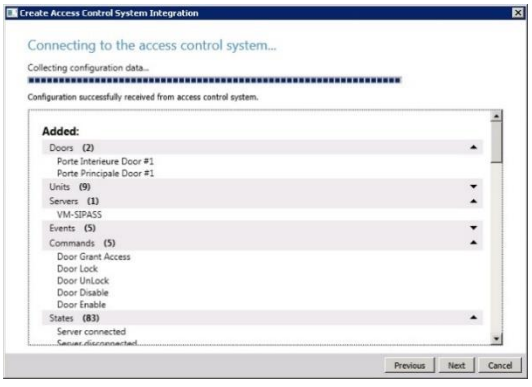


Database - Host – Name of the computer hosting the OnGuard SQL Server instance
Database - Instance – Name of the SQL Server instance hosting the OnGuard Access Control database. Leave blank to connect to the default SQL Server instance.
Database - Name – Name of the OnGuard Access Control database.
Database - User – User name to login to the OnGuard Access Control database.
Database - Password – Password to login to the OnGuard Access Control database.
Database – Integrated Security – Flag indicating if the OnGuard Access Control database uses integrated security. If false, the database user name and password is required.
Options – Cardholder Sleep – Defines how long the OnGuard plugin will sleep (in minutes) between fetching card holders from OnGuard. Legitimate values are greater than zero. This is here as a safety to ensure that card holders are kept up-to-date even if card holder modification events from OnGuard are not received or missed.
Options – Reader Sleep – Defines how long the OnGuard plugin will sleep (in minutes) between fetching door and reader information from OnGuard. Legitimate values are greater than zero. OnGuard doesn't provide notification of certain reader attribute changes (e.g. extended strike time) so this polling provides a way to force the system to refresh reader information.
Options – Property Sleep – As hardware events are received from OnGuard, this property defines the time to wait before updating a device's live properties (e.g. reader mode, device hardware status) (in seconds) again. Legitimate values are greater than or equal to zero. This property allows tradeoffs to improve OnGuard event processing speed. For every hardware event received from OnGuard, the OnGuard ACM integration generates related state change events. These state change events are very slow to process compared to the raw hardware events; this delay is caused by having to update the devices' live properties. The smaller you set LivePropertyUpdateInterval, the more "real time" will be those live property values; however, the cost is more cpu usage and slower state change processing. The higher you set LivePropertyUpdateInterval, state change processing will be faster due to using the currently cached values of the live properties; the cost is that state change events may be sent to MIP that contain "stale" live property values.
Options – Event Propogation – If checked, then applicable events will be propagated to child hardware. For example, a panel offline event would end up triggering offline events for all the panel's child hardware (e.g. readers, alarm panels, inputs, outputs, etc). If not checked, event propagation is not done. Note that certain functionality is dependent on event propagation. For example, if event propagation is disabled, a Smart Client reader map icon may not display the correct state when its panel is toggled between online and offline because we rely on receiving reader online/offline events to keep that up-to-date.
Options – State Events – If unchecked, then state change processing (including propagated state changes) is disabled. If checked, state change processing is performed and the DoEventPropagation setting is respected. This property can be disabled to maximize raw OnGuard event processing speed. Note that unchecking this property will prevent XProtect Smart Client map icons from showing the current device state.
Options – Disable Commands – This is a setting to enhance security. If checked (the default), then no commands will be executed. The commands will still be visible in XProtect Smart Client maps and in the Dev tabs of the XProtect Management Client; however, they will be silently ignored if a user attempts to execute them. If unchecked, commands will execute as normal.

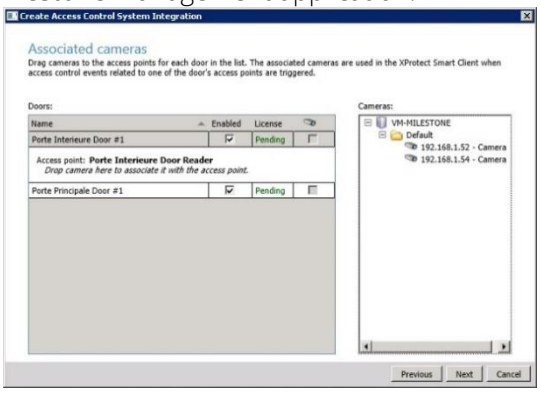
Options – Event Batch Size – Defines the maximum number of events to process per batch. This is an approximate number; the actual number could be less than or slightly more than this number due to several factors – less events available, more events with the same filter criteria, etc.
Options – Event Sleep - Defines how long the event processor subsystem will sleep (in milliseconds) between batches of events. Legitimate values are greater than zero. The subsystem does not sleep when it finishes a batch of events if there is another batch of events ready to process. The actual loop and event processing time may vary while the plugin is caching or while the system is under heavy load.
Options – Database Timeout – Events are fetched from OnGuard using a direct SQL query. Internally, there is a timeout for how long to wait to get the results of the query. This default timeout is 30 seconds. When querying for events from an OnGuard table containing many (i.e. millions) of rows, the query can easily take longer than 30 seconds. In that case, the query will fail, events won't get processed, and errors will be written to the debug log. To prevent failures in this situation, increase the event command timeout (e.g. 240 seconds). Legitimate values are greater than or equal to 30 seconds. Changing this property value has NO impact on the actual time it takes to perform the query; it only is an attempt to prevent premature timeouts. It is ***always*** better to keep the number of rows in the OnGuard EVENTS table to a reasonable amount. OnGuard provides the capability to archive events; contact OnGuard Support for help setting that up.
OpenAccess - Host – Name of the machine hosting the OnGuard OpenAccess service.
OpenAccess - Port – The port the OnGuard OpenAccess service is listening on.
OpenAccess – Page Size – The OnGuard OpenAccess service limits the number of instances returned for a given query. For example, multiple queries are required if the number of OnGuard card holders is greater than the page size. Legitimate values are greater than or equal to 20 and less than or equal to 100. Performance is better with a larger page size.
OpenAccess - User – The name of an OnGuard administrative user to use to log into the OnGuard OpenAccess web service. This user should have access to all hardware, cardholders, etc in the system.
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.

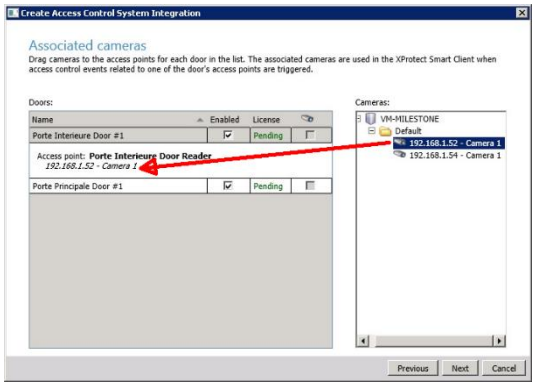
The wizard will now fetch the configuration of the OnGuard AC system into Milestone.
The screen below is an example of the configuration found on the server:



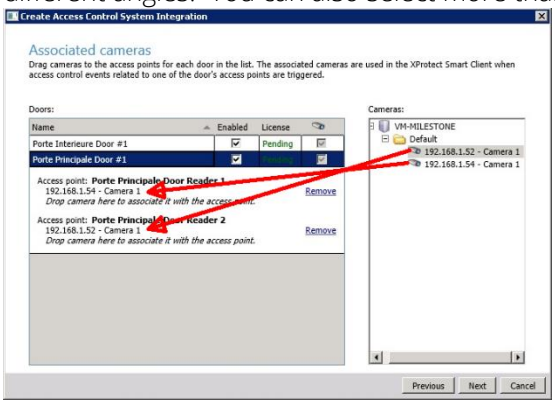


On this screen an association has to be created between each access point of a door and cameras in the Milestone system. This is done so that the system will know which cameras to display on door alarms. For each access point of each door drag a camera from the right tree and place it under the desired access point to create the association. Note that this can also be configured later in the Milestone Management application.

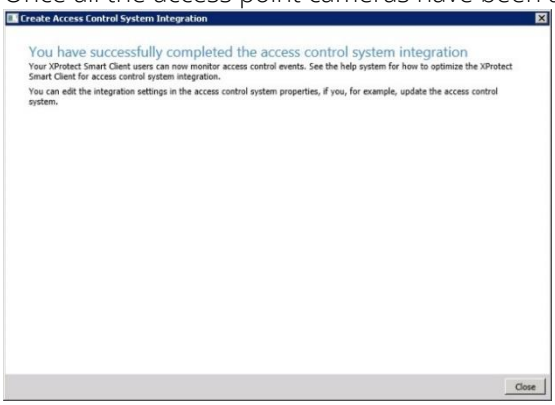




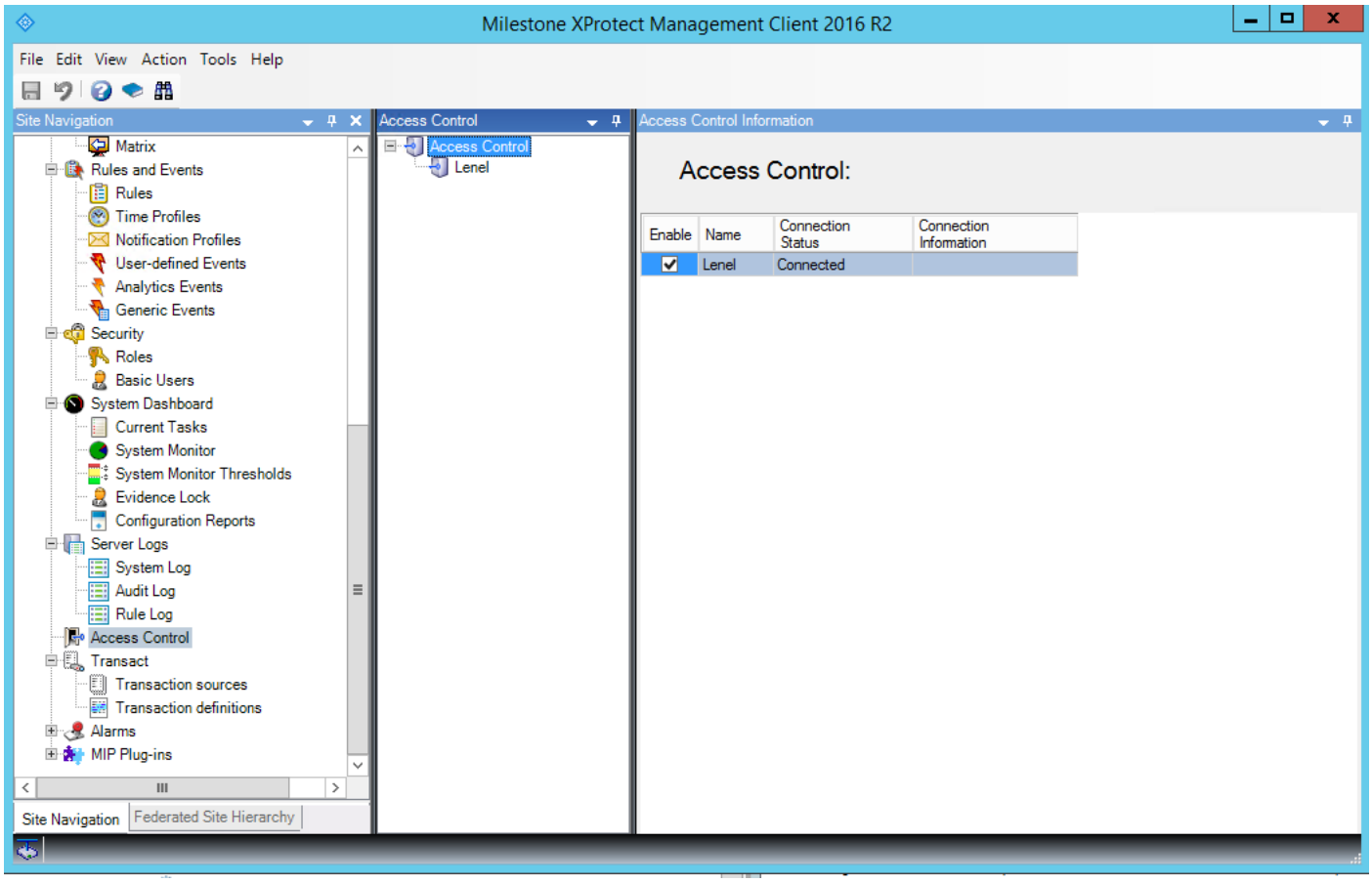
When there is more than one access point per door, you can select the different cameras for the different angles. You can also select more than one camera per access point:



Once all the access point cameras have been associated, the wizard completes.



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



Reducing Permissions

In the image above, the "Database Name" and "Database User" fields defined the credentials the OnGuard ACM integration uses for read-only access to the OnGuard database. This section is only about minimizing the database permissions for *this* database access.

Since you're considering changing the Sql Server permissions for the login used by the OnGuard ACM integration, this section assumes you know how to perform the required steps in Sql Server to create/modify a login.

We've tested the OnGuard ACM integration with the following minimal database permissions:

- Has only the "public" server role.
- User mapping to only the OnGuard AccessControl database.
- Has only the following database roles for the AccessControl database:
  - db_datareader
  - public
- Has only the "Connect SQL" securable.

Personalized Login

Personalized login is an optional feature of XProtect access control plugins. If enabled, when someone logs into the Smart Client, for *each* access control instance with personalized login enabled in the Management Client, the smart client will ask for user credentials. These credentials will be validated against the specific access control system, and, if valid, will be used to fetch a personalized configuration from the access control system. The personalized configurations will be used throughout that instance of the Smart Client.

When personalized login is being used, XProtect manages two configurations – a "global" one used by the Management Client, and, as described above, personalized configurations used by the Smart Client. The personalized configurations are always subsets of the global configuration. This is necessary to ensure proper event handling, command execution, etc.

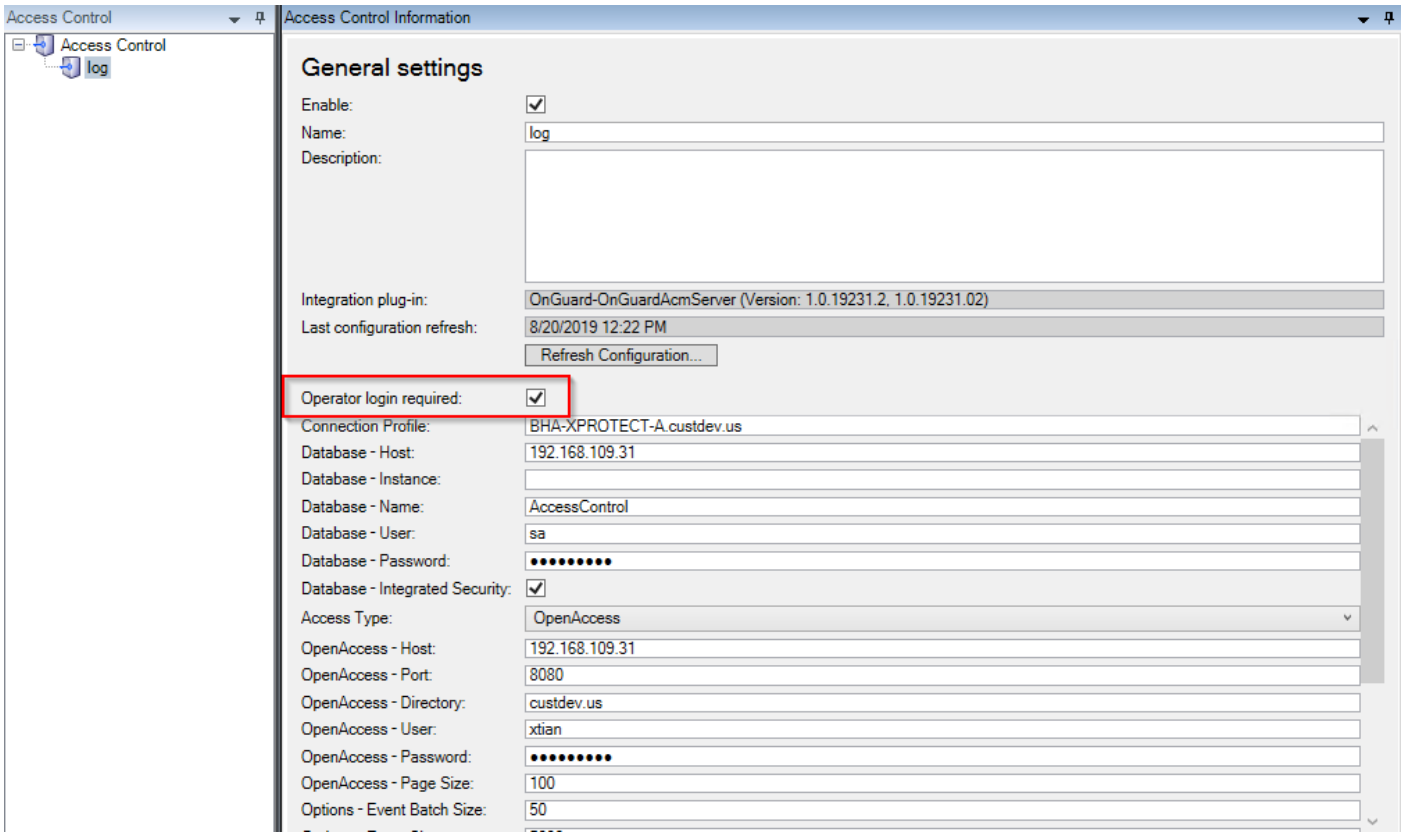
An access control plugin must specifically support personalized login. The OnGuard ACM plugin does support it only when running on OnGuard 7.4 or greater since the OnGuard OpenAccess API is required to support it.

Enable/Disable Personalized Login

Enabling/disabling personalized login for a specific access control plugin is done in the Management Client.

The first step is to configure your access control instances as described in Milestone Management Client Configuration.

For access control instances that support personalized login, XProtect adds an additional property which is used to enable/disable personalized login for that specific access control instance. If the property is checked, personalized login is enabled:

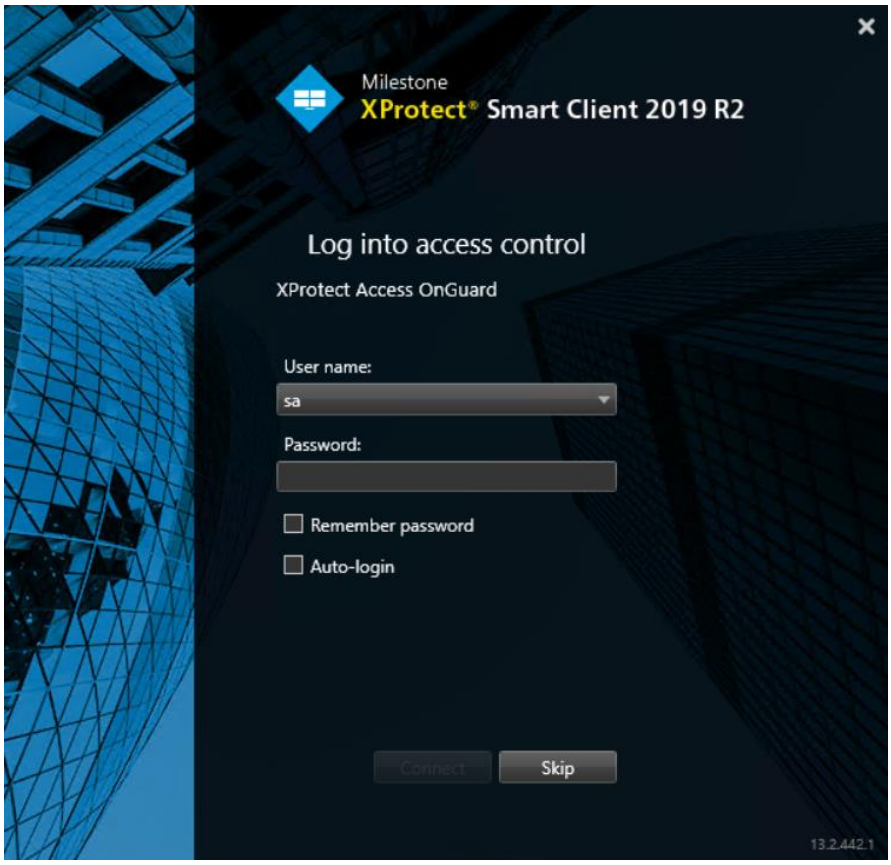


Smart Client Personalized Login

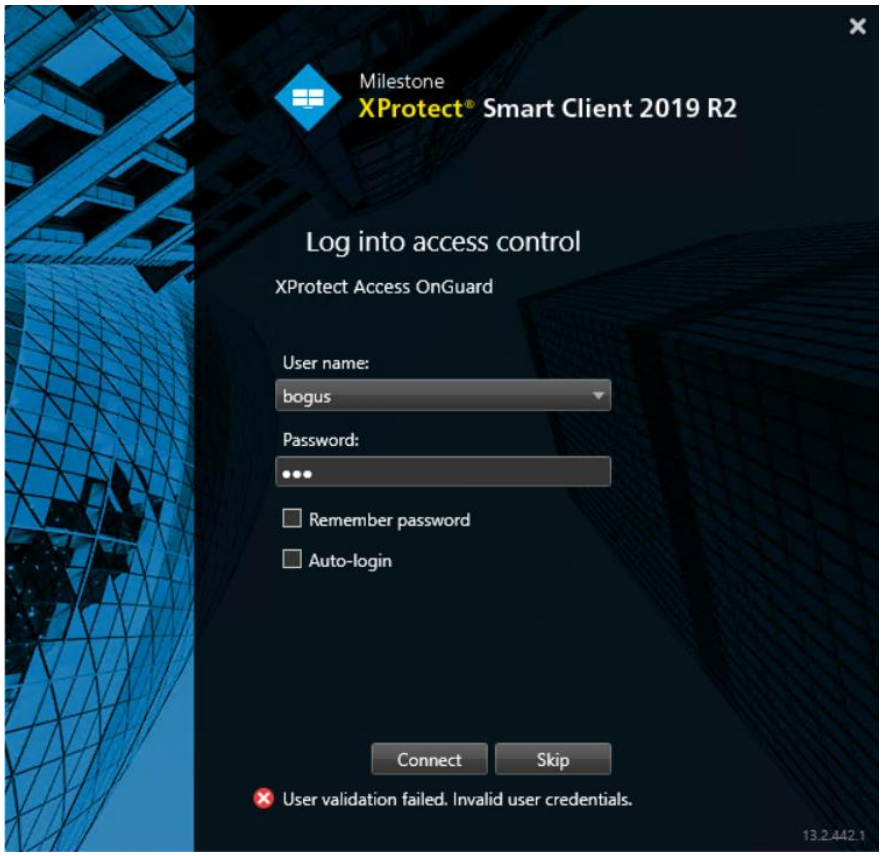
If personalized login is enabled for any access control instance configured in the Management Client, the Smart Client will request user credentials for each of those access control instances. This is done after the standard Smart Client login screen.

For manual sign-on, OnGuard OpenAccess requires three pieces of data – the user name, the password, and the directory. XProtect only provides fields for the user name and password; it doesn't know anything about "directories". To get around this, you can enter the directory along with the user name in the format "directoryName\userName". You can also use the forward slash as a separator. If you omit the directory, the OnGuard "internal" directory will be used.

Be aware that the OnGuard System Administration application allows non-word characters in directory names. Obviously, this will break our user name parsing if the directory name contains embedded slashes! We're assuming the user name doesn't contain slashes either.



After entering the user name and password, the XProtect will attempt to validate the credentials against the specific access control system. If the validation fails, you'll see:



If you click Skip, the Smart Client is opened *without* using personalized login.
If the credentials are successfully validated, the Smart Client will load a personalized configuration from that access control instance. This personalized configuration is used by the Smart Client to filter entities viewed/operated on in the Smart Client. For example:

- Events
- Doors
- Hardware visible in a map's Element Selector
- Alarms

The Smart Client will not show any entities that are not in (or related to entities in) the personalized configuration. For example, a personalized user will only see:

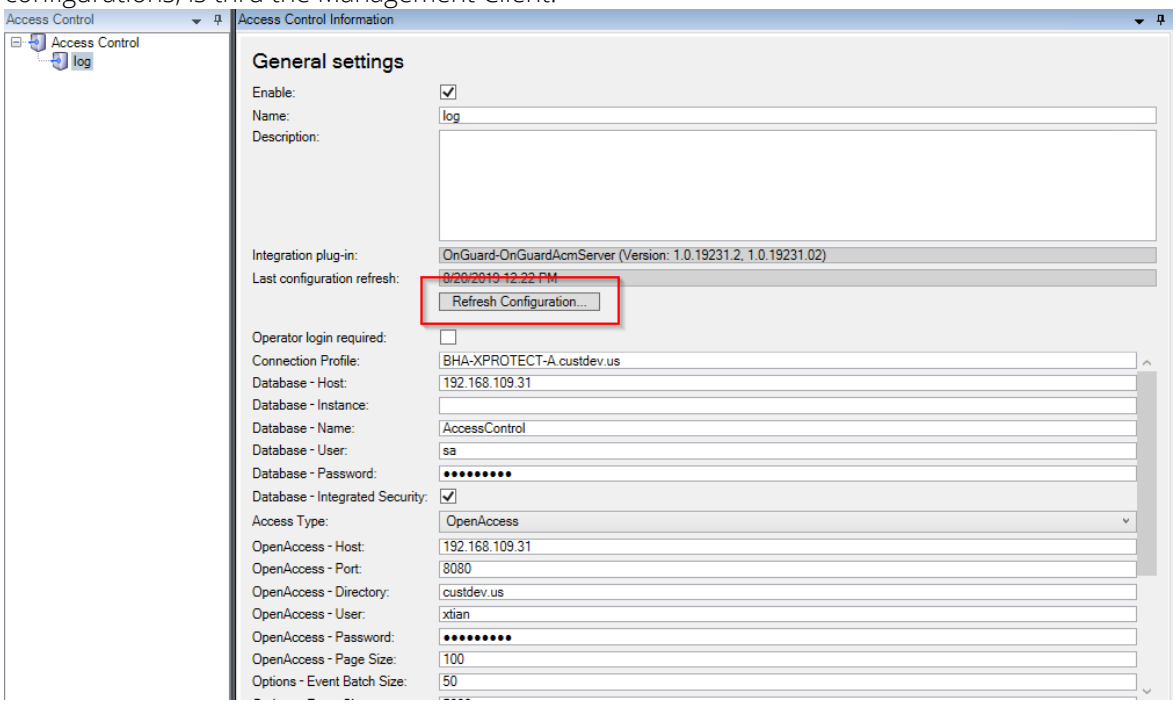
- Alarms related to hardware in their personalized configuration.
- Events related to hardware in their personalized configuration.
- Devices in the map element selector that are in their personalized configuration.

XProtect Personalized Login doesn't specifically include personalized alarm acknowledgment. Rather, as with non-personalized login, any user can acknowledge any alarm that is visible in the Smart Client. Since

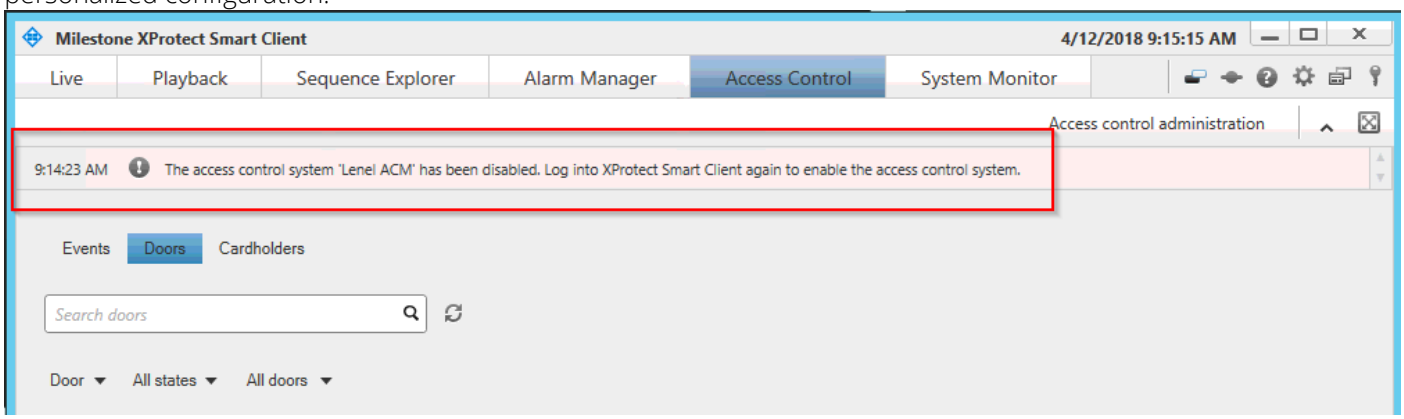
alarms will only be visible if the underlying device is in their personalized configuration, then users can only acknowledge alarms related to hardware they can see.
OnGuard does not support personalized command execution. That is, a user can execute any applicable commands on any devices that are visible to that user.

Refreshing the Personalized Configurations

The XProtect Event Server caches personalized configurations. When the global configuration is refreshed, ***and changes applied***, the Event Server refreshes all the personalized configurations in its cache. The personalized configurations are not refreshed if there were no changes applied to the global configuration. The only way to refresh the global configuration, and, hence, the personalized configurations, is thru the Management Client:



The personalized configuration cache is cleared upon Event Server restart.
If there is a running Smart Client using a personalized configuration, after the configuration is updated, you may see the following message in the Smart Client. Simply log back in to get the updated personalized configuration:



Common Actions

Editing OnGuard Event Types

The OnGuard event types are originally read from the OnGuard database Event table. After initially reading from the database, the event types are stored in a comma-delimited disk file located at C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\EventTypes.csv on the OnGuard machine.

The columns are: Id, Type, SubType, Description, Name, HardwareType, AllowDoorAnimation

The rows are sorted by Type, then SubType.

The hardware type values are a bitwise OR'ed combination of the following:

- Unknown = 0x0
- Server = 0x1
- Panel = 0x2
- Reader = 0x4
- Input = 0x8
- Output = 0x10
- IoControlModule = 0x20
- Door = 0x40
- MaskGroup = 0x80
- All = 0xFF

An example from the file is shown below:

```
1,0,0,Access Granted,granted_access_granted,0x000000FF,True
2,0,1,Access Granted on Facility Code,granted_facilitycode,0x000000FF,True
3,0,2,Access Granted No Entry Made,granted_noentrymade,0x000000FF,False
4,0,3,Access Granted on Facility Code| No Entry Made,granted_fcnoentry-
made,0x000000FF,False
```

When the event types are initially processed, all the hardware types are set to All (i.e. 0xFF)

The intent of this file is to allow an administrator to tailor the description, hardware types, and door animation for specific event types. **The Id, Type, SubType, and Name fields should never be changed as they correspond to identifiers used by OnGuard.**

If you're going to modify an event type's description **be aware that any description containing embedded commas *must* have those embedded commas changed to pipe characters (i.e. "|")**. See the last line of the example lines shown above where the logical string "Access Granted on Facility Code, No Entry Made" has its embedded comma replaced.

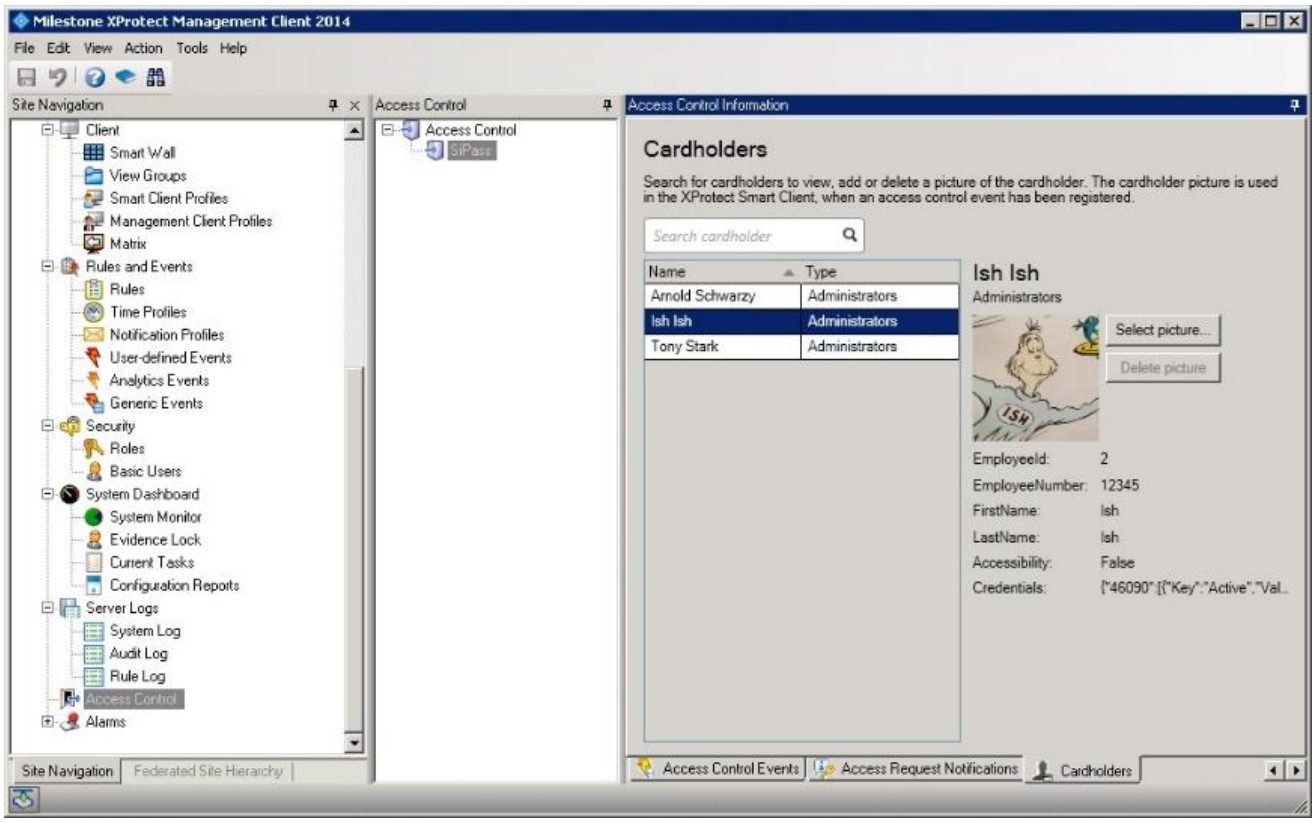
After making and saving changes to the event type file, the administrator should do the following:

1. On the OnGuard machine – restart the ACM server.
2. On the XProtect machine – refresh the configuration from within the XProtect Management Client. See MIP Plugin Upgrades for an image showing the Management Client's Refresh Configuration button.

Searching for cardholders

Only "active" cardholders are downloaded from the OnGuard server. "Active" is defined as a cardholder having at least one badge with a status of "active". Therefore, cardholders with no badges or with no active badges, will not be shown in the Management Client Cardholder tab.

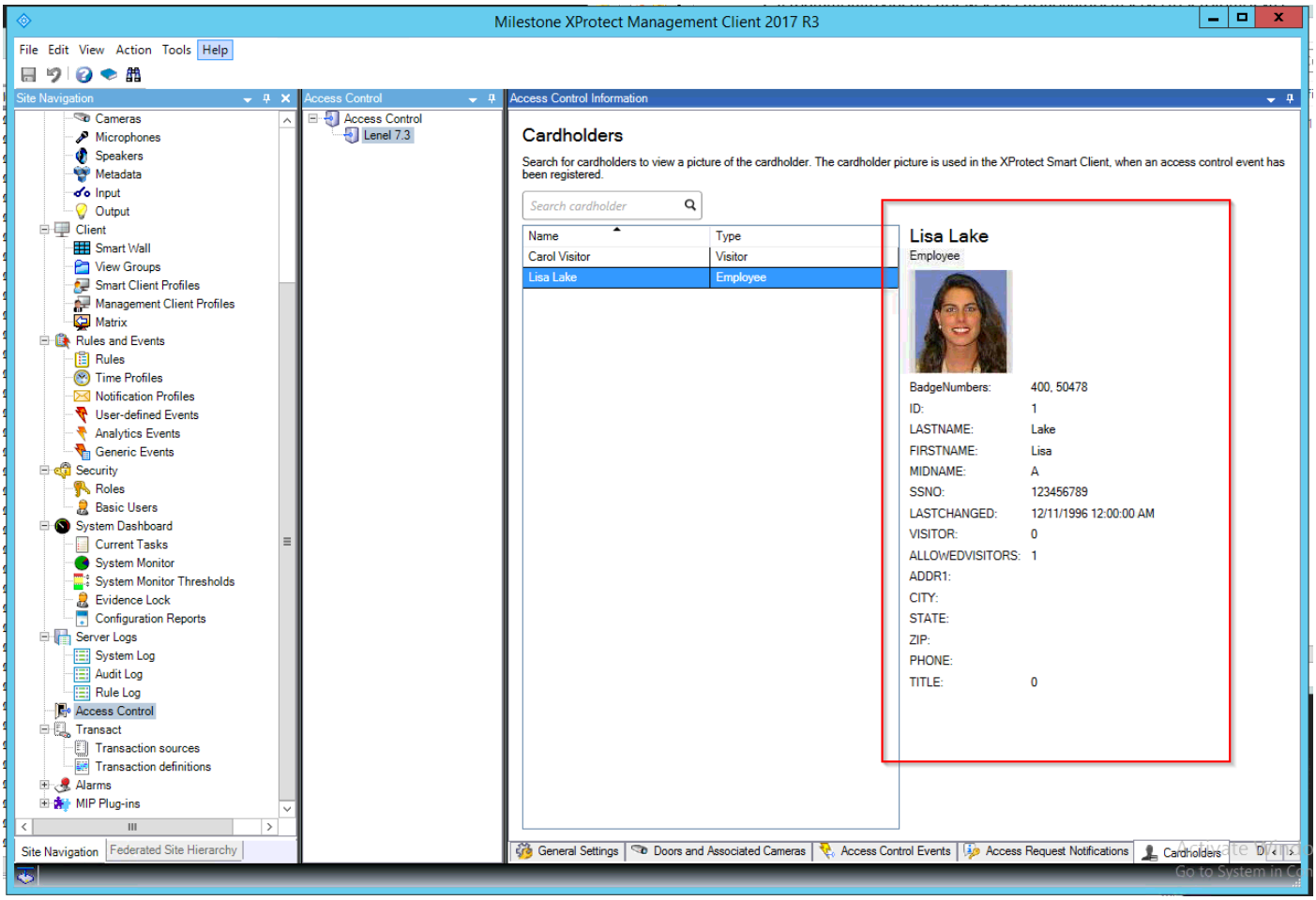
The user can search for existing cardholders in the OnGuard system through the management client interface:



The search can be made by first name, last name, card number, and employee id. Enter the search string in the search cardholder text box.

Cardholder Properties:

The XProtect Management Client does not provide scrolling for the cardholder properties. In the image below, if the properties (see the red square) are so many that the list is longer than the display area, they will simply run off the bottom edge of the screen and will not be visible.



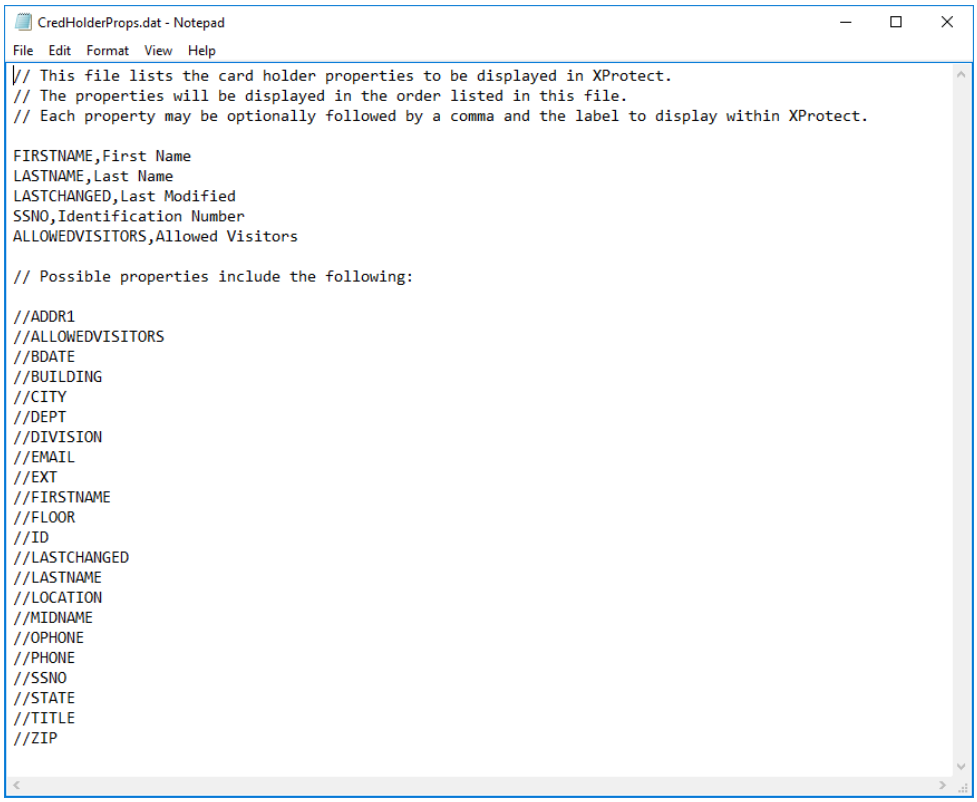
OnGuard allows customization of the Cardholder UI in their System Administration application. It's easy for a customer to define enough custom fields to extend beyond the visible region shown above for the XProtect Management Client.

The OnGuard ACM plugin manages a configuration file C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\CredHolderProps.dat. This configuration file is created the first-time credential holders are fetched. By default, it includes *all* cardholder fields.

Its contents are simply a list of column names from the OnGuard EMP and UDFEMP database tables that you want shown in the XProtect Management Client. The properties will be displayed in the order and case (i.e. uppercase, lowercase, or a mixture) they are defined in CredHolderProps.dat. You can remove any fields you don't want displayed and change the order of the fields. Column names that don't exist will be ignored.

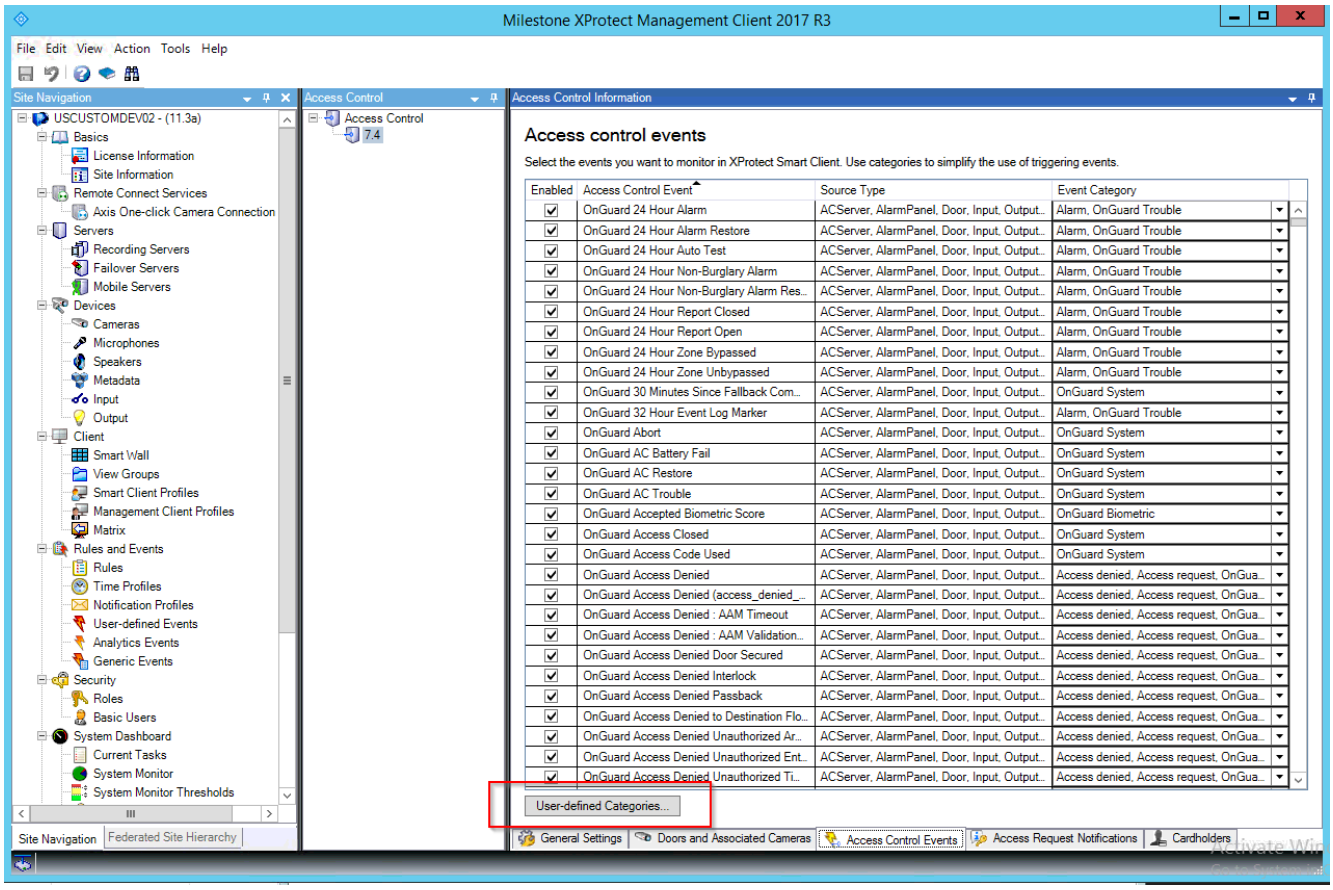
Note that the cardholder's badge numbers are always displayed as the first property.

After making changes to CredHolderProps.dat, you should restart the ACM Server; then close all XProtect clients, restart the XProtect Event Server, and then re-open the XProtect clients. This is necessary as XProtect caches cardholder data. Restarting everything clears those caches and then you'll see the cardholder properties displayed as you have them configured in CredHolderProps.dat.

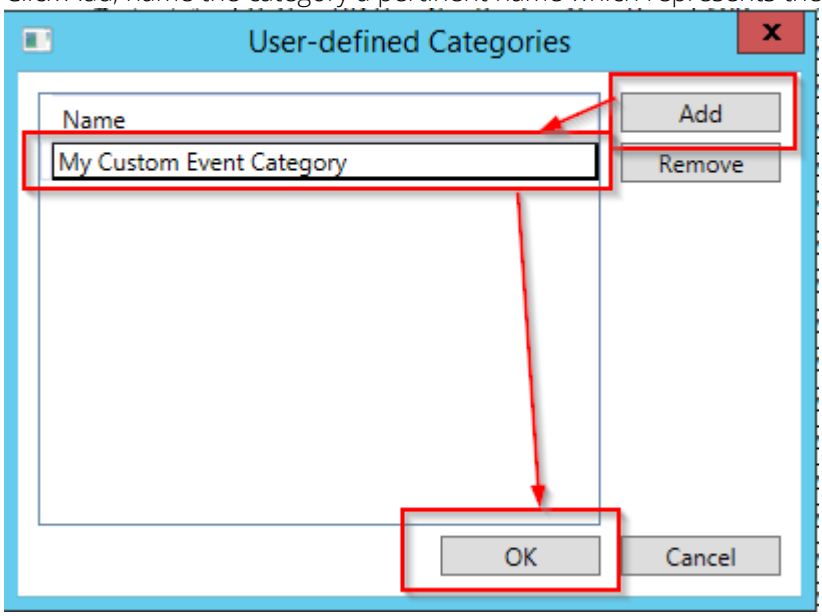


Defining alarms based on OnGuard events

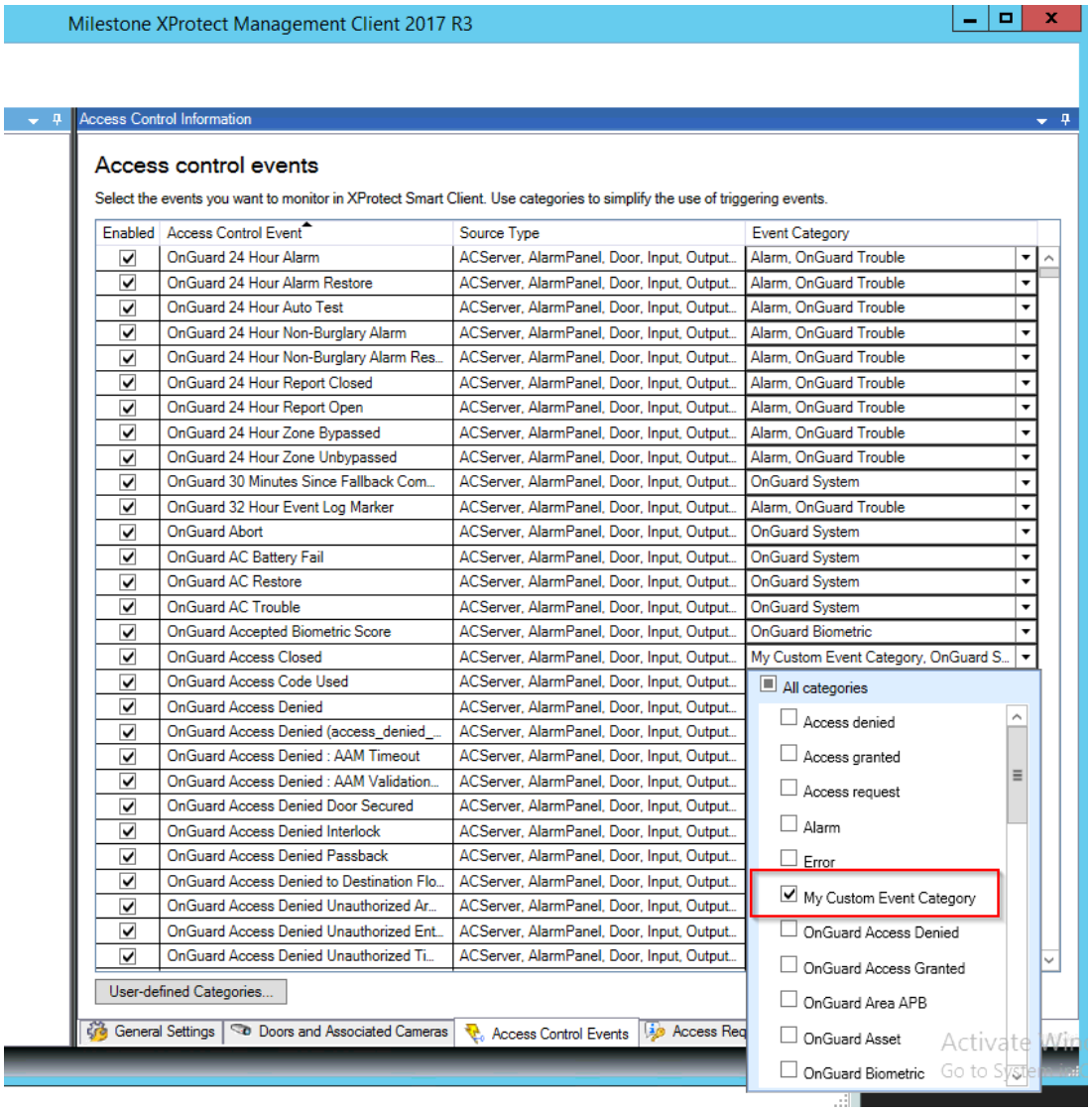
To define alarms based on OnGuard events, the events must be part of an event category. The category can be one of the pre-defined Access Control Event categories such as (Access Granted, Access Request, Access Denied, Alarm, Error, and Warning) or a user-defined category. Here is how to create an alarm based on a user-defined access control event category. First define the category if it does not already exist:



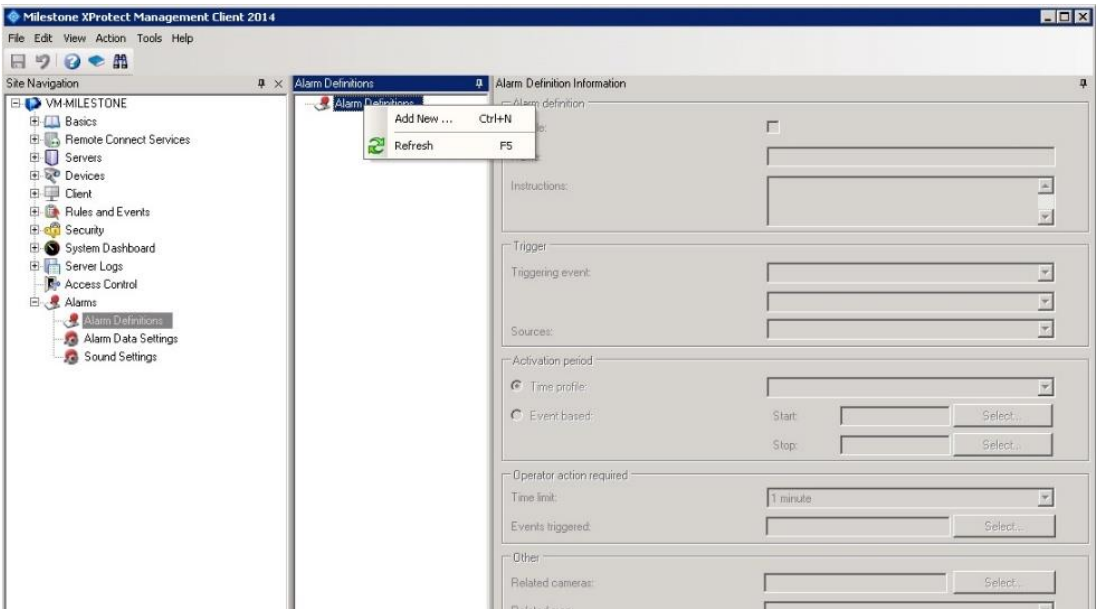
Click Add, name the category a pertinent name which represents the group of events, and press OK.



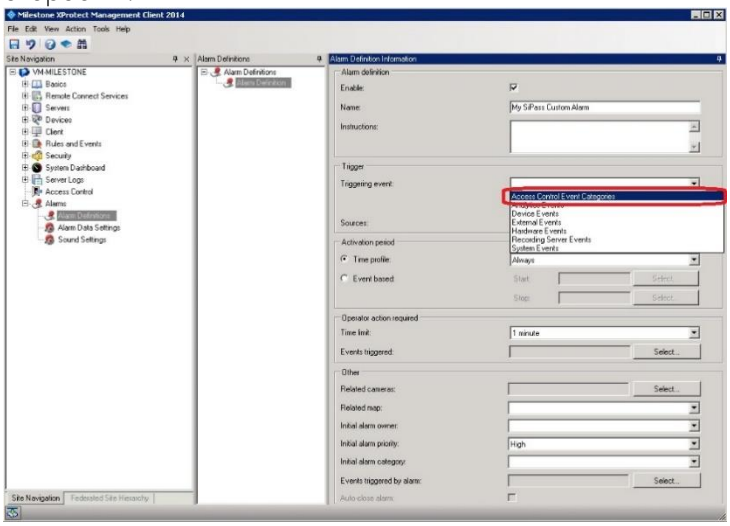
Associate the category with one of the OnGuard AC events:



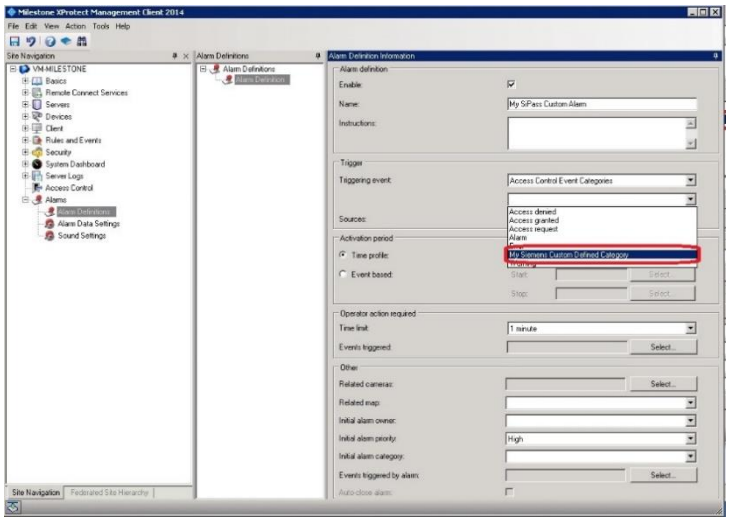
Save your changes and move to the Alarm Definitions section to create an alarm based on that user-defined event category.



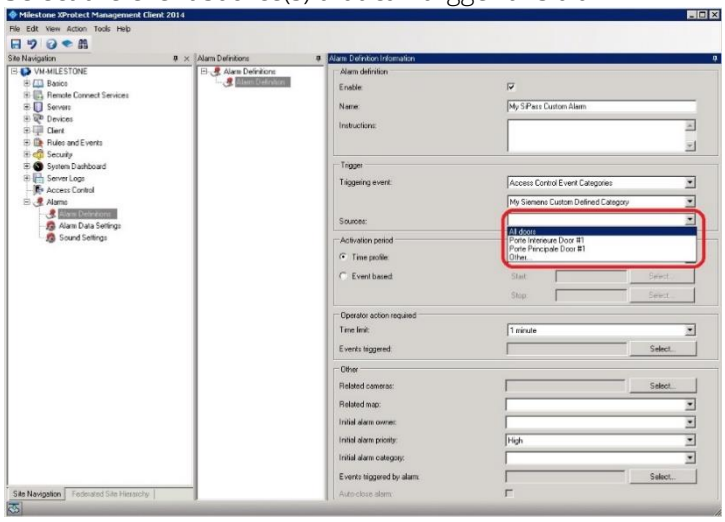
Name the alarm a pertinent name and select Access Control Event Categories in the Triggering event dropdown:



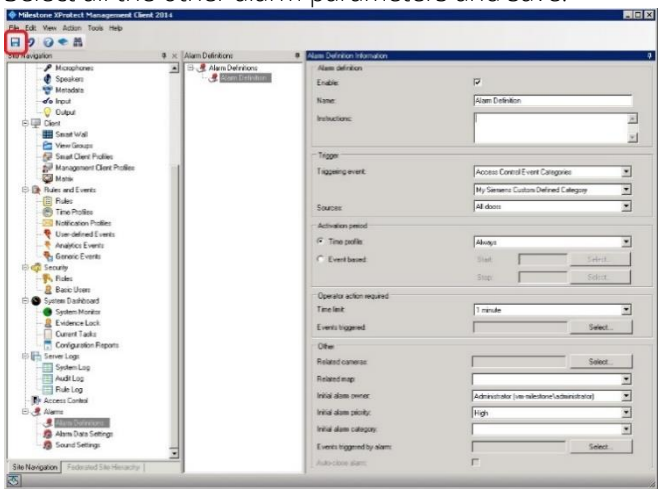
Select the new user-defined event category that was defined earlier:



Select the event source(s) that can trigger this alarm



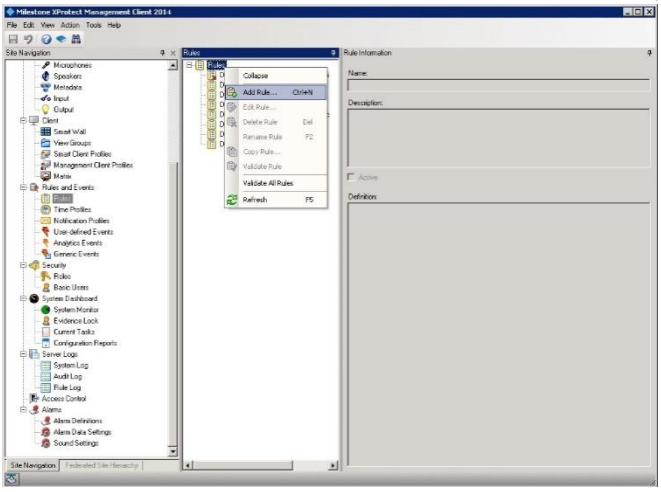
Select all the other alarm parameters and save:



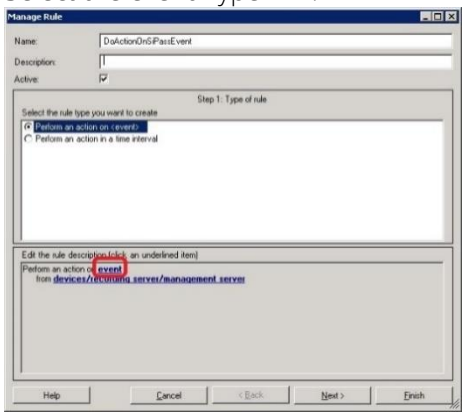
Alarms acknowledged in Milestone are acknowledged in OnGuard.

Defining rules based on OnGuard events

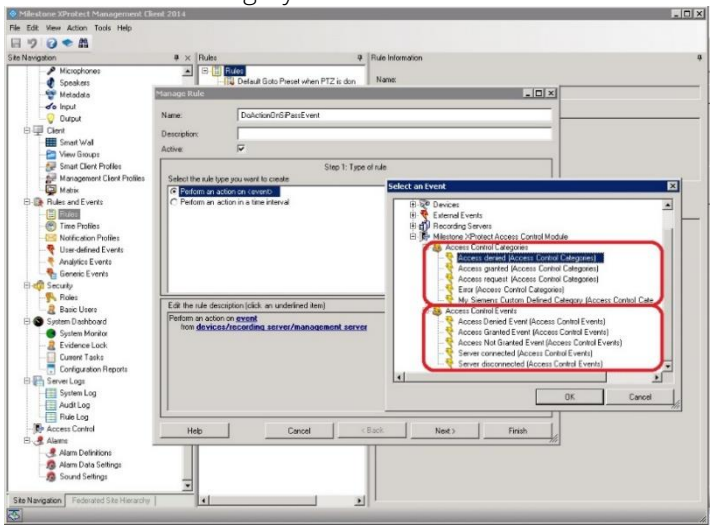
To define rules in Milestone based on OnGuard events, create a rule in the Rules tab:



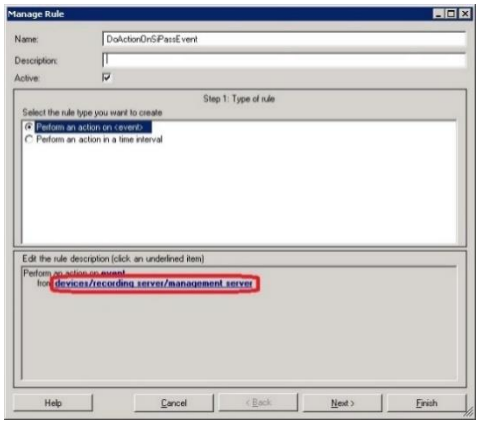
Select the event hyperlink:

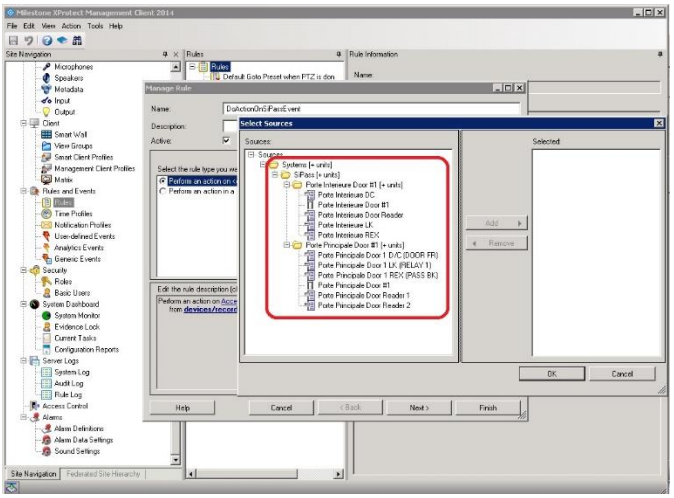


Select an event category or event from the Select an Event dialog:

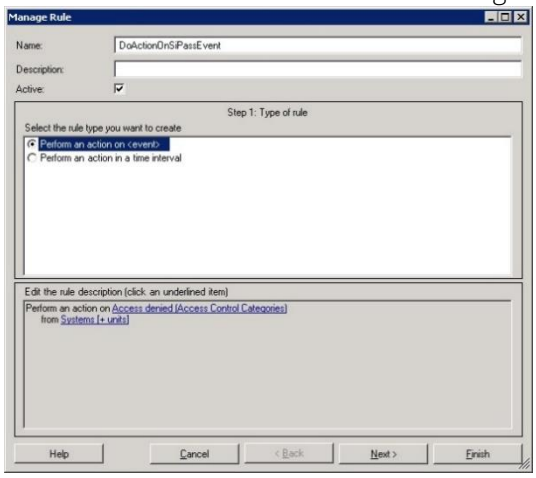


Select the devices/recording server/management server hyperlink and select the event source. To select any source select the System (+units) node.

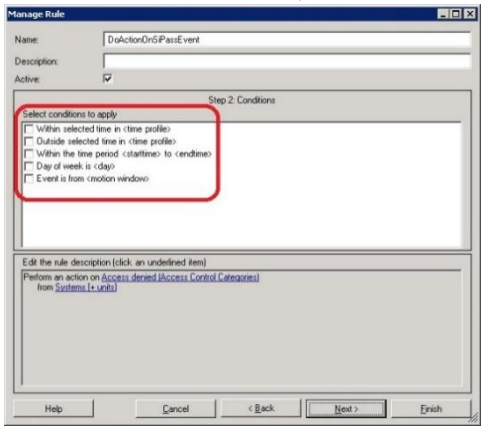




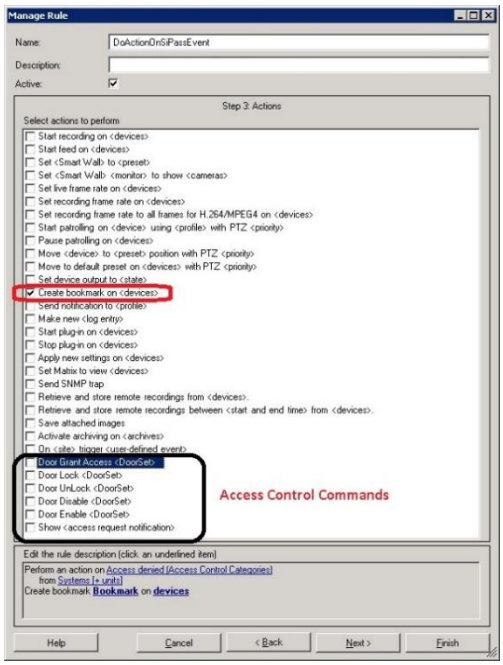
The wizard will look like this after selecting the “Access Denied” event and System (+ units) source:



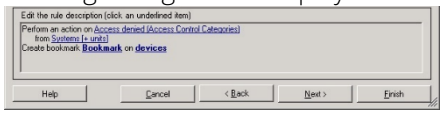
Press next and select the optional time frame when the action will take place. In this example no time frame has been selected, this means it will always execute.

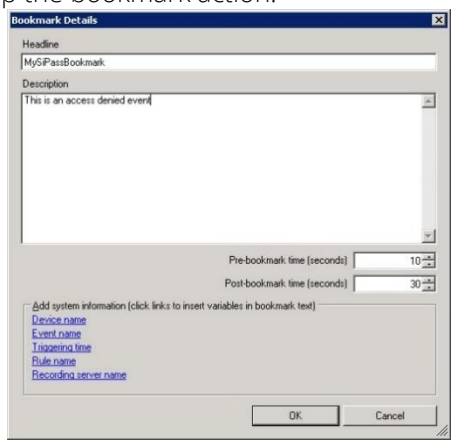


Select the action that will be executed when the OnGuard event occurs. Notice that AC commands can be used as actions based on any events that come into Milestone:

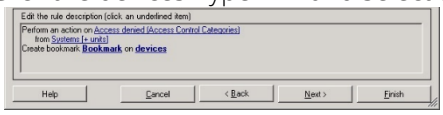


In this example “create bookmark on <device>” will be selected, click the Bookmark hyperlink and the following dialog will be displayed to setup the bookmark action:

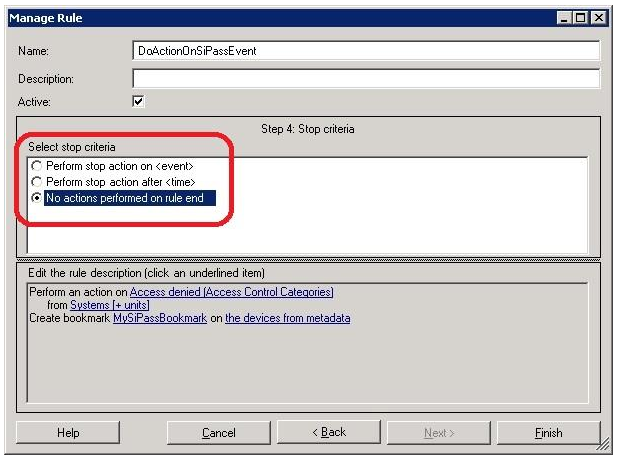




Click the devices hyperlink and select the device on which the bookmark will be applied:



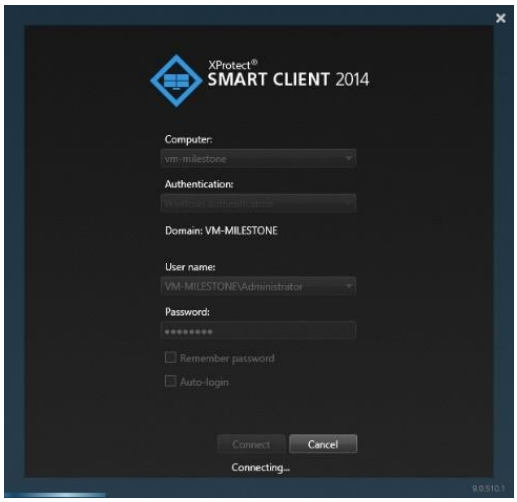
Click next on the rule wizard and select an optional stop criteria, in this example there is no stop criteria.

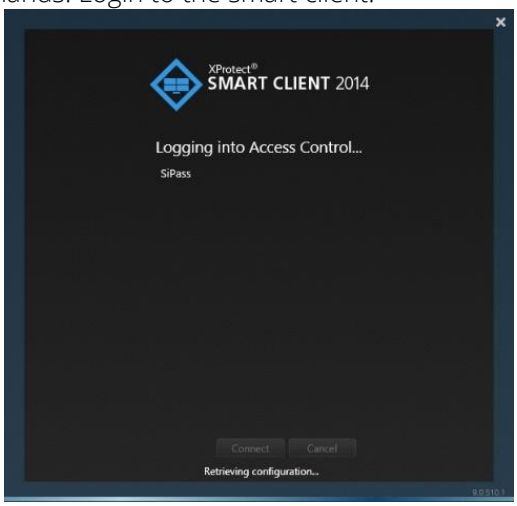


Click finish and the rule is set.

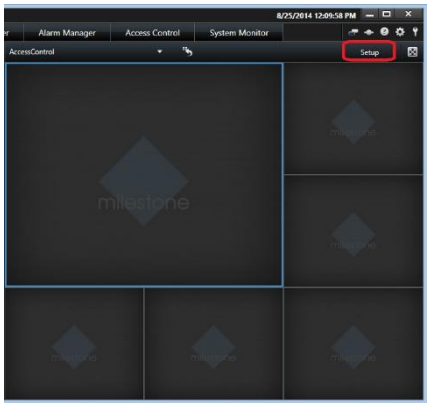
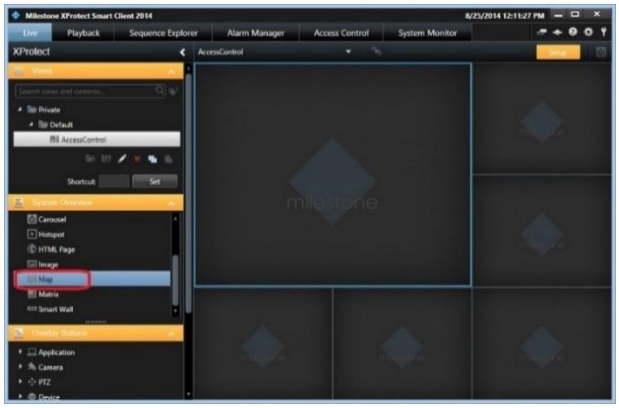
XProtect® Smart Client Maps

It is possible to put doors and OnGuard server(s) on an existing Smart Client Map to display door and server status as well as execute manual commands. Login to the smart client:

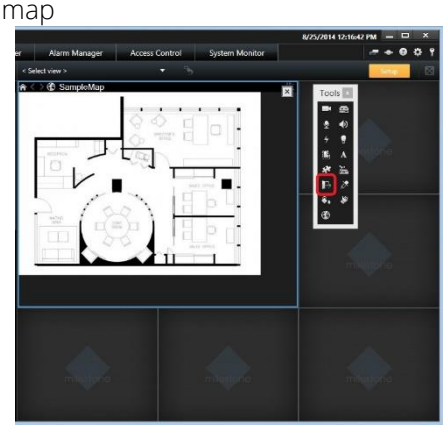
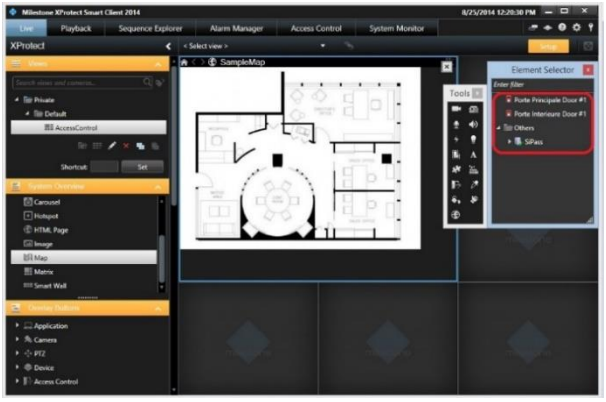




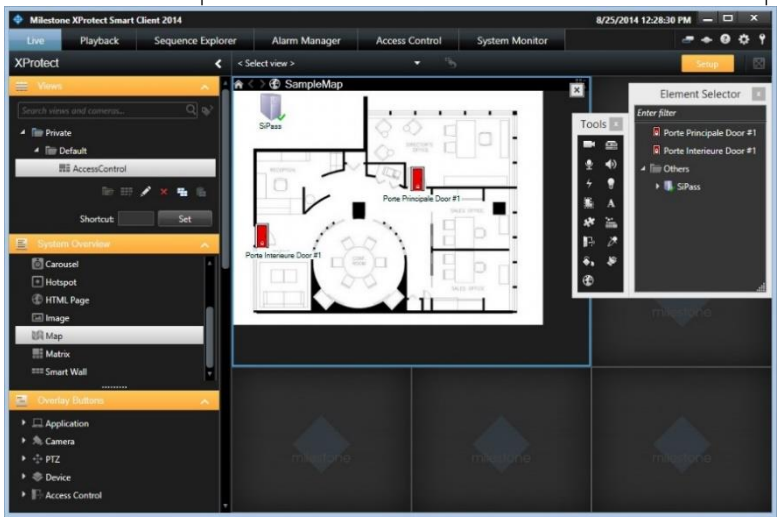
Use an existing view, go into setup mode by pressing the setup button in red below and create a map by dragging it onto a tile once in setup mode.

Select the access control button on the map overview and drag doors from the Element Selector to the map

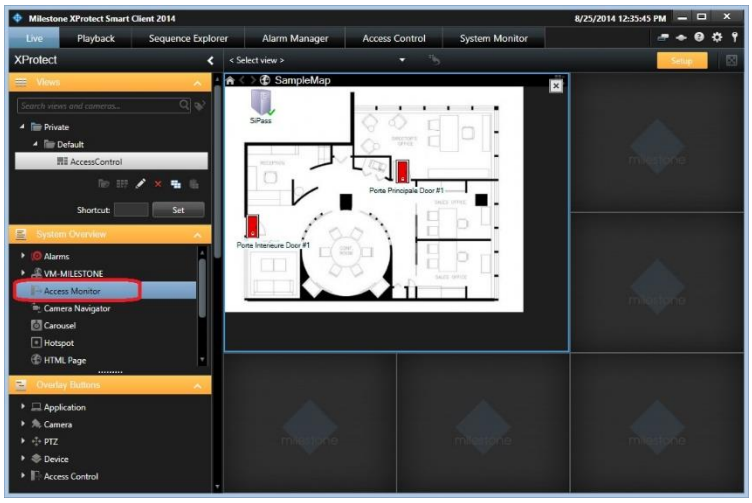



The finalized map with the doors and server added in this example will look like this:

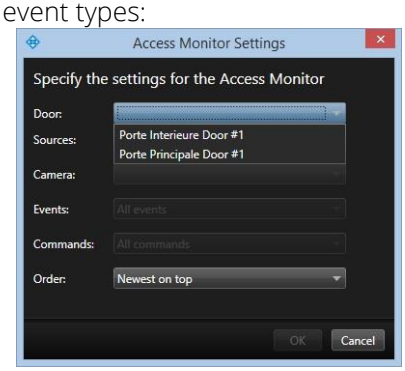


XProtect® Access Monitor tiles

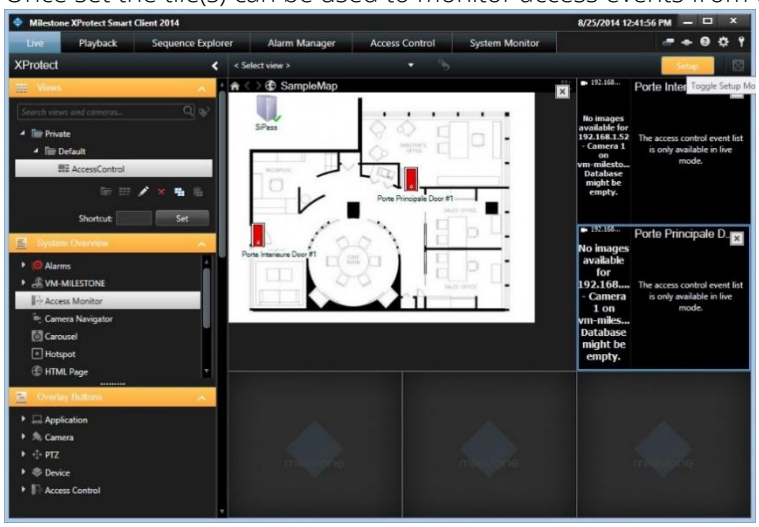
Access monitor tiles allows the monitoring of access events on a specific door by displaying cardholder credentials next to the video content. Drag the "Access Monitor" item from the System Overview onto a tile:



The following dialog will appear: to set access monitor tile settings select the door, sources, camera, and event types:



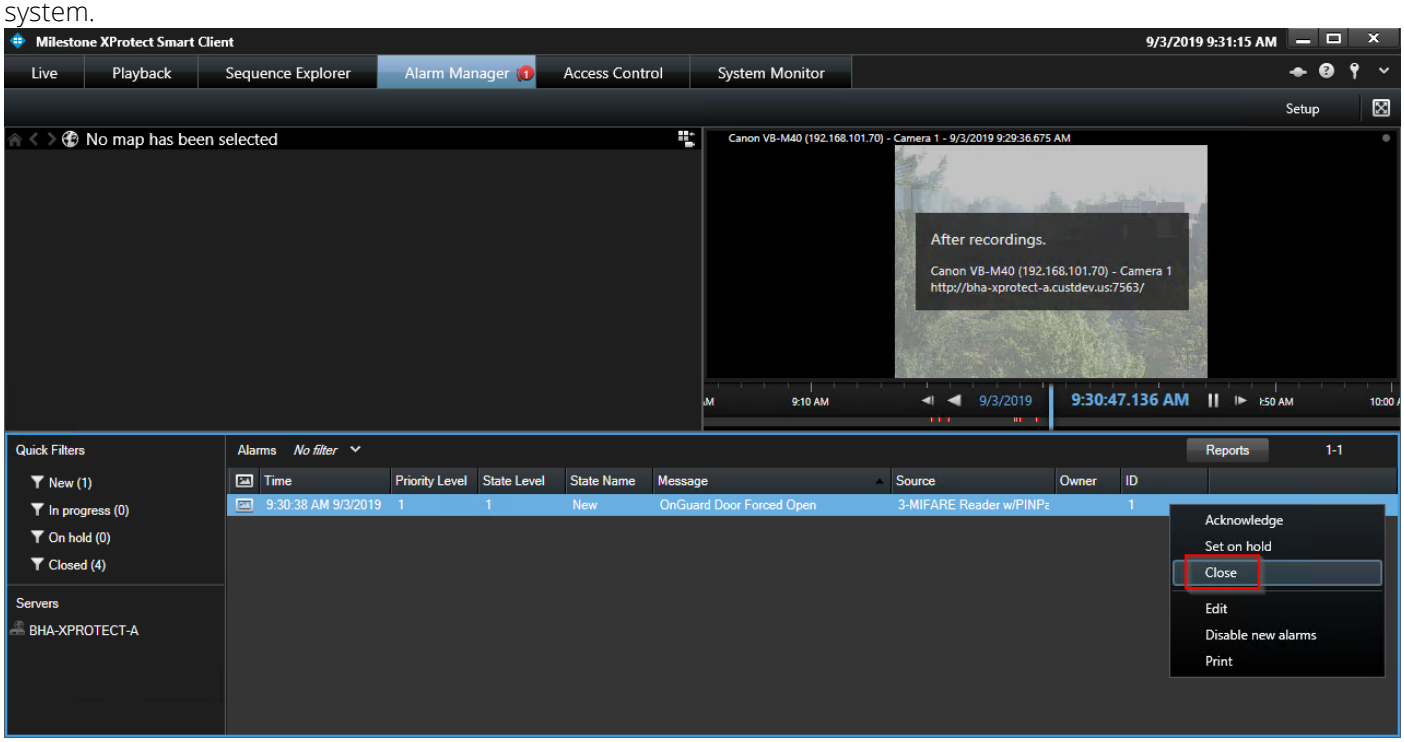
Once set the tile(s) can be used to monitor access events from each door configured above:

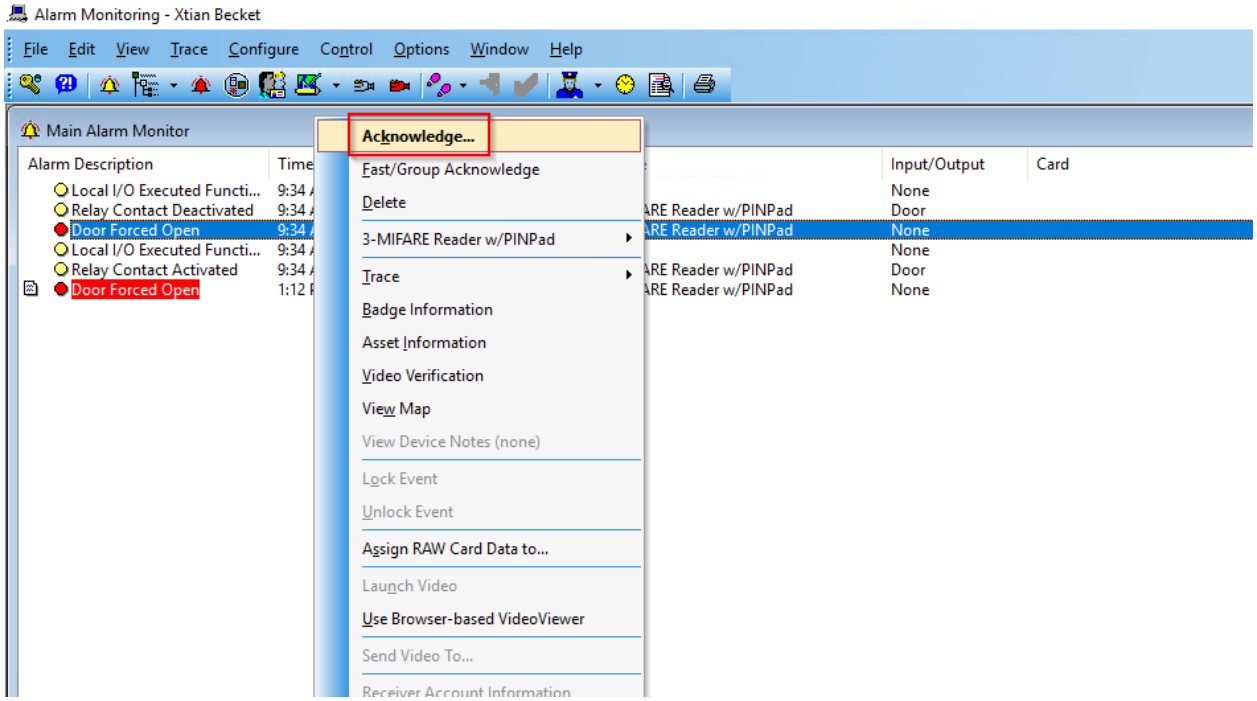


Alarm Acknowledgment

Alarm acknowledgment from XProtect (2016 R3 or greater) to OnGuard, and from OnGuard to XProtect is implemented. In XProtect versions earlier than 2016 R3, you can still perform alarm acknowledgment in XProtect, but it will not be propagated to OnGuard.

Alarm acknowledgment is done in the XProtect Smart Client's Alarm Manager tab. If you right-click an alarm, and select Close, the event will be closed in OnGuard. Note, if you acknowledge an event in OnGuard, it closes the event in the OnGuard system, thus closing the associated alarm in the XProtect system.





Fetching OnGuard event types

To see the events that a particular version of OnGuard generates, there is a utility called LenelFetchEventTypes.exe provided with the OnGuard ACM integration release. Look in the Tools directory within the release's zip file.

This application does *not* require the OnGuard ACM integration at all. It is completely independent of the integration.

This application must be run on the OnGuard machine where the OnGuard database is located. Enter the database connection parameters when requested by the application.

After fetching the events from the database, it will prompt you to write the event list to the console window or a file. If you choose the console window, ensure that you've increased the console's buffer size; for example, OnGuard 7.3 systems have about 1820 events and the default Windows console buffer size is 300. If you choose to write the list to a file, that file will be overwritten if it already exists; otherwise, it will be created.

Note that piping the output of the application to a file on the command line does *not* work due to the interactive prompts generated by the application.

Defining cardholder properties to display in Milestone XProtect

After connecting to an integration in the Milestone XProtect Management Client, a file will be created on the system running the Milestone ACM Server (generally the OnGuard machine). It will be located here by default:

C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\CredHolderProps.dat

This file may be modified to customize the properties displayed for a cardholder within Milestone XProtect. To change the file, first stop the Milestone ACM Server. Open the file in a text editor, such as notepad. Fields may be added to the top section, in the format of <database field>,<display text>, where the database field is the property within the OnGuard system, and the display text is the value displayed within Milestone XProtect. For example:

FIRSTNAME,First Name

Will display the FIRSTNAME field with the text 'First Name:'

The bottom of the file contains the fields detected in the integration at the time of installation, for your convenience. Once the file has been modified, save and close it.

For the changes to take effect, you will have to reset some values in the cardholder cache progress file, then restart the Milestone ACM Server service, and then finally restart the XProtect Event Server service. To reset the cardholder cache progress file, navigate to the following location on the machine that has the OnGuard plugin installed:

C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\cache

Open the file “cacheProgress.dat” with a text editor. Excluding "DaysBeforeCacheRefresh”, change the values of the properties to their listed default values. Save the file and then restart the Milestone ACM Server service. Finally, restart the XProtect Event Server service.

Feature Differences Between Connection Modes

Certain features will behave differently when the integration is configured for DataConduIT instead of OpenAccess.

Alarm Acknowledgement

If you acknowledge an alarm in the XProtect Smart Client, OnGuard will receive the acknowledgement when the integration is configured to use OpenAccess or DataConduIT. However, if you acknowledge alarms in OnGuard, XProtect Smart Client will only receive updates when the integration is configured for OpenAccess.

User Privileges

OpenAccess uses the authenticated login to communicate with OnGuard, allowing the system to enforce privileges on a per-user basis. DataConduIT uses a single user account for all operations making it impossible to enforce user privileges.

Events

When configured for OpenAccess, the integration will receive notifications from OnGuard when events occur. When configured for DataConduIT, the integration will poll for event changes at a regular interval, configurable in the plugin configuration in the XProtect Management Client. The actual loop and event processing time may vary while the plugin is caching or while the system is under heavy load.

Logging

By default the debug logs are enabled on both the milestone event server plugin and the OnGuard server but they are at a reduced log level (Info). They can be increased for diagnostics purposes to Debug (or even Trace) but be aware that this change causes more information to be logged using more disk space and possibly slowing down operations on busy servers. DO NOT LEAVE logging at Debug levels for extended periods of time for performance reasons. It should only be used for diagnostics purposes and put back to Info afterwards.

Gathering the logs

Milestone Event Server side

1. On the machine running the Milestone Event Server go to x:\ProgramData\VideoOS\ACMServer-Plugin, where X: is the drive where Windows is installed
2. Create a zip file of the contents of that whole folder, name it ACMServerMIPlogs.zip
3. On the machine running the Milestone Event Server go to x:\ProgramData\Milestone\XProtect Event Server\logs, where X: is the drive where Windows is installed
4. Create a zip file of the contents of that whole folder, name it MilestoneEventServerLogs.zip

OnGuard Server side

5. On the machine running the OnGuard server go to X:\ProgramData\VideoOS\ServiceHost\logs, where X: is the drive where windows is installed
6. Create a zip file of the contents of that whole folder name it MilestoneHostLogs.zip
7. On the machine running the OnGuard server go to X:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\logs, where X: is the drive where windows is installed
8. Create a zip file of the contents of that whole folder and name it MilestoneACMServerServiceLogs.zip
9. On the machine running the OnGuard server go to: X:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\logs
10. Create a zip file of the contents of that whole folder and name it OnGuardAcmServer-PluginLogs.zip

Changing logging level

Sometimes for diagnostics purposes, it is necessary to obtain more information about the running state of the integration. The logging information can be increased by changing what we call the logging level. The logging level can be set at any of the following values in increasing amount of information recorded to file (Off, Fatal, Error, Warn, Info, Debug, Trace). Off writes no information to the file and Trace writes the most information to file. The default setting is Info. The logs auto-delete after 10 days, so they do not take up too much disk space. Here is the procedure to change the log levels in the different modules of the integration:

Milestone Event Server side

1. On the machine running the Milestone Event Server go to x:\ProgramData\VideoOS\ACMServer-Plugin, where X: is the drive where Windows is installed

2. There should be subfolders that use a unique identifier (GUID) something like "4c53f6e5-e951-1616-83f0-e44fb813e451". For each of these folders do the following:
    a. Find a file named "ACMServerPluginNLog.xml", open it with a text editor like 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" in that line 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 Server side

1. On the OnGuard server machine go to x:\ProgramData\VideoOS\ServiceHost. X: would be the drive where windows is installed.
    a. Find a file named "ServiceHostNLog.xml", open it with a text editor like notepad
    b. Near the bottom of the file, find the lines starting with "<logger name="*"", "<logger name="lenel.*"", and "<logger name="OnGuard.*"".
    c. Change the "minlevel" attribute values in those lines from their current values to "Debug" or "Trace" 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.
2. On the OnGuard server machine go to x:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService. X: would be the drive where windows is installed.
    a. Find a file named "VideoOSACMServerNLog.xml", open it with a text editor like 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" in that line and save the file.

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

OnGuard loses communication with the access control hardware

Communication can be lost for the following reasons:

1) Firewall blocking the 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).

Failure of the ACM plugin to communicate with Window Management Interface (WMI)

The OnGuard ACM plugin runs in the ACM Server service. That service must be running in the security context of a local machine admin user which is linked to a OnGuard Directory that is configured for

single sign-on. See Configure OnGuard for Single Sign-On and ACM Server: Configure to RunAs OnGuard Single-Sign-on Account above for details.
If the ACM Server is not running in the required security context, the OnGuard ACM plugin log (see log locations below) will show lines similar to the following:

05-11-2016 12:28:32 Error 9 EventHandler.registerForWmiEvents() - Failed to register for hardware events.
05-11-2016 12:28:32 Error 9 EventHandler.registerForWmiEvents() - Failed to register for software events.
05-11-2016 12:28:32 Error 9 EventHandler.start() - Failed to register for WMI events.

Milestone Event Server MIP Plugin cannot communicate with the ACM Server (DataConduIT only)

When the system is properly running, the Milestone Event Server MIP plugin "pings" the OnGuard ACM plugin about every 5 seconds. At a log level setting of Trace, you'll see lines like the following in the OnGuard ACM plugin log (see log locations below):

05-11-2016 13:02:01 Trace 11 AcApi.IsApiConnected()
05-11-2016 13:02:01 Trace 11 AcApi.IsRunning()
05-11-2016 13:02:01 Debug 11 DataConduit.isConnectedToServer() - m_Started = True, wmiSvcIsRunning = True, dbIsAccessible = True.

If you don't see these lines, or you expect a communication failure between the Evert Server MIP plugin and OnGuard ACM plugin, take a look at your firewall settings, rules, etc. You may need to adjust them to allow communication.
Note that, by default, the ACM Server's web service uses HTTPS on port 8443. You may have configured your ACM Server differently (see ACM Server: XProtect ACM MIP Plugin for where you configured the ACM Server connection on the Milestone Event Server).

Debug log shows SqlAccess.connect() failed

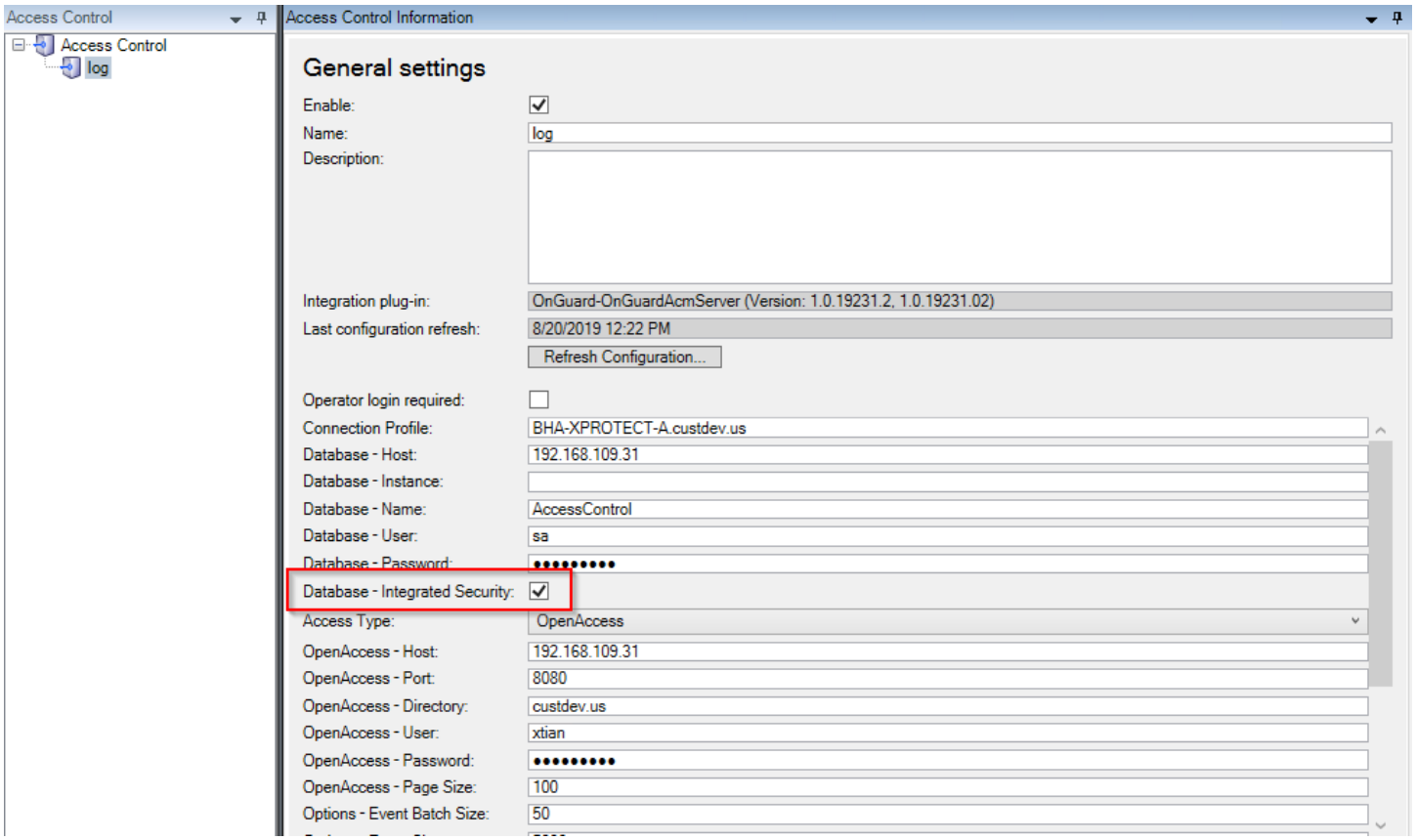
If the debug log shows an error similar to:

06-22-2016 20:26:40 Error 14 SqlAccess.connect() - Failed to connect. System.Data.SqlClient.SqlException A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Go to Configure SQL Server for Connections for properly configuring the SQL Server supporting your OnGuard installation.

Failure to connect to SQL Server

If you believe that you've entered the correct user name and password (and optionally the database instance name), and the OnGuard integration logs show that the SQL Server connection is still failing, ensure that you've checked DbUsesIntegratedSecurity.



Not receiving card holder or badge changes

If you don't see card holder or badge changes reflected in either the Milestone Management or Smart Clients, ensure that you've enabled software events in OnGuard.

Optimizing Event Processing Performance

To maximize event processing performance, adjust the following settings. Note that the combination of settings that will give the best performance on any given system is not clear. You may have to experiment to determine the most optimal combination of settings.

- Debug log level – should be set to "Info". The "debug" or "trace" settings write too much data to the event log affecting overall performance.
- Adjust the following ACM instance settings (see Milestone Management Client Configuration):
  - ReaderPollingInterval – Set this to a large number (e.g. 60). Frequently reading reader information can have a large impact on overall performance.
  - CardHolderProcessSleepInterval – Set this to a large number (e.g. 60). Frequently reading cardholder information can have a large impact on overall performance.
  - EventProcessBatchSize – Only applies to OnGuard versions less than 7.4. Tailor this value as needed. The larger the number, the more events processed in one batch. Note that a larger

number doesn't always result in better performance because, depending on the rate of events coming in, more time could be spent waiting for events than processing them.

- EventProcessSleepInterval – Only applies to OnGuard versions less than 7.4. Tailor this value as needed. The smaller the number, the less time the event processing subsystem waits between attempting to query for more events. A smaller number doesn't always give better overall performance since it causes batches of only a few events to be processed each time rather than less batches with more events in the them.
- LivePropertyUpdateInterval – Increase this value to reduce the number of times device live properties (e.g. reader mode, hardware status, etc) need to be refreshed. If you make the value very large (e.g. 3600 seconds), then only cached values of the live properties will get used for that time interval. The value of this setting is irrelevant if DoProcessStateChanges is disabled since live property updating only applies to state change events.
- DoEventPropagation – Uncheck this option to avoid sending possibly a very large number of child hardware events.
- DoProcessStateChanges – Uncheck this option to completely bypass state change event creation. All events received from OnGuard will be processed. But the system will not even attempt to create state change events related to the OnGuard events.

No matter what settings you adjust, all raw events received from OnGuard get sent to XProtect.
If DoProcessStateChanges is enabled, for every raw event received from OnGuard, the OnGuard ACM integration will create corresponding "state change" events. If the raw event is for a "parent" device (e.g. panel, door, I/O control module), and if the DoEventPropagation setting is enabled, state change events may also be created for child devices (e.g. reader, inputs, outputs). When added together, state change and propagated state change events add a large number of events to be sent to XProtect.
Therefore, if you're only interested in optimizing raw OnGuard event processing, disabling DoProcessStateChanges will result in better performance as it drastically reduces the number of events sent to XProtect. However, XProtect Smart Client map icons won't display status changes since no state change events get sent to XProtect.
On one of the Milestone test systems, we achieved almost real time firing of OnGuard events to XProtect with all the default settings except:

- DoProcessStateChanges disabled
- LivePropertyUpdateInterval = 3600 seconds (effectively disabling live property updates for the duration of the test)

Refreshing cardholders

The XProtect Management Client's Cardholders tab doesn't provide a way to force a refresh of the cardholders. "Refresh" means performing a full download of all the active cardholders from OnGuard.
The OnGuard ACM integration downloads cardholders from OnGuard at the following times:

1) When the ACM Server is started.

2) When the CardHolderProcessSleepInterval (see Milestone Management Client Configuration) occurs.
3) When XProtect Management Client property values change (see Milestone Management Client Configuration) are saved.

So an easy way to force cardholders to be downloaded is to simply fake changing a property value in the Management Client and then click the Save button. "Fake changing" means simply changing a property value and then, before saving, reset the property value back to its original value.

WMI related errors

If you're getting WMI-related errors in the OnGuard ACM log files, they're typically due to the OnGuard Single Sign-On (SSO) user. The SSO user may not be set up correctly, may be missing some permissions, etc.

A workaround to verify that the errors are indeed due to SSO user permissions, is to change the currently configured OnGuard SSO user to the built-in "System Account" user. This built-in user has all possible permissions within OnGuard.

Steps:

1. Log into OnGuard's System Administration application as the OnGuard "SA" user. Open the Administration + Users view.
2. For the current SSO user, unlink the SSO domain account from the SSO directory.
3. Link the built-in "System Account" user to the SSO directory using the SSO domain account.
4. Restart the LS DataConduIT service.
5. Verify that the Milestone ACM service is running as the SSO domain account.
6. Restart the Milestone ACM service.

Inspect the OnGuard ACM logs to see if the errors went away.

OnGuard OpenAccess connectivity

This only applies for OnGuard versions greater than or equal to 7.4.

OnGuard's OpenAccess API provides a web service for connectivity.

OnGuard's OpenAccess API uses a SignalR service to send events from OnGuard to the OnGuard ACM integration.

The OnGuard ACM integration uses a polling mechanism to verify connectivity to both OpenAccess and the SignalR service. If the OpenAccess web service goes down, the default HTTP timeout can be up to approximately 1 ½ minutes. So state change notifications for the server being disconnected can be delayed by that much. On the other hand, a subsequent attempt to check that the OpenAccess service is back up is much quicker. So state changes for coming back up happen much faster.

XProtect® Smart Client not showing alarm panels or their inputs/outputs

There is a known bug in the 2017 XProtect Smart Clients where certain configuration elements (e.g. alarm panels) and their inputs and outputs do not appear in the map's Element Selector. This bug was fixed in the 2018 R1 release.

OnGuard ACM integration flooding user transaction report

Milestone's XProtect system requests the current states of OnGuard hardware at various times throughout the life of the application. As prescribed by the OnGuard integration documentation (for both DataConduit and OpenAccess), 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.

The integration just responds to XProtect's requests for hardware status whenever XProtect asks for it. Currently, there is no extra logic for things like mapping the last time status was requested for a particular device and waiting some configurable time period before updating the parent panel's hardware status again, etc.

Technically, this works fine. But a transaction for each hardware status update/query is entered into OnGuard for the single sign-on (SSO) user. Per OnGuard, there is nothing the OnGuard ACM integration can do to prevent these transactions from being entered into OnGuard.

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. Because there's so many of these transactions, some customers feel that the OnGuard ACM integration makes this report useless. Per OnGuard, it's not possible to filter the User Transaction report to omit the SSO user.

The only options that customers have are:

- Install a compatible version of Crystal Reports and customize the report how they'd like. However, OnGuard Technical Support, OAAP, etc will not support these custom reports.

Contact the OnGuard Custom Solutions group and have them create/customize the reports. However, the customer will need to pay for this service.

OnGuard ACM instance is 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. Do the following steps in the following order:

- Close the Management Client and Smart Client
- Stop the Milestone Event Server
- Stop the Milestone ACM Service
- Ensure OnGuard is running successfully. This may require restarting the DataConduIT or Open-Access services, LS Web Service and the LS Web Event Bridge.
- Start the Milestone ACM Service
- Start the Milestone Event Server, and wait for it to come to ready
- Start the Management Client

If the instance still does not appear in the Management Client, investigate the logs (see Logging) to discover the specific cause.

LS OpenAccess service automatically stops seconds after starting

There is a known issue with OnGuard in which an active directory account logging into the OpenAccess service shortly after it starts can cause OpenAccess to crash. Because the Milestone ACM Server will attempt to log in to OpenAccess when both services are ready, this can trigger the problem. The recommended workaround is to switch the Single Sign-On user to be a local windows account, and

adjust the services to use this same login as mentioned above in Refreshing the Personalized Configurations.
For questions and information concerning a fix for this issue, please contact Lenel support for information regarding this bug at oaap@lenel.com. Reference Lenel 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 Lenel support for information regarding this bug at oaap@lenel.com. Reference Lenel Bug DE40122.

LS OpenAccess fails to send any events when running in an Enterprise configuration

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) running in an Enterprise configuration where 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 Lenel support for information regarding this bug at oaap@lenel.com. Reference Lenel 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

- This ACM integration was only tested against the MIP SDK 2017. The MIP SDK is backwards-compatible; so it is assumed that the ACM integration will work with MIP SDK 2016 and 2014.
- This ACM integration has only been tested when running the OnGuard and Milestone systems on Windows Server 2012 R2 and Windows Server 2016.
- This ACM integration is currently coded to only work with a OnGuard system using SQL Server as its database. Oracle integration has not been implemented yet.
- Only United States English installers are available.
- 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.
- See the negative side-effects of upgrading.

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