MAKE THE
WORLD SEE

Date: 1 October 2018

Guide

Milestone XProtect Access

Lenel OnGuard User Manual

Prepared by:
Brian Hayes, Software Developer, Custom Development Americas

milestone

Table of Content

Copyright, Trademarks & Disclaimers

Copyright

Trademarks

Disclaimer

Version Compatibility

Matrix

Here is the compatibility matrix between Lenel OnGuard and Milestone XProtect.

Please verify the version of Lenel OnGuard you are running against this compatibility table. Milestone always recommends that you run the latest versions of both OnGuard and XProtect

Lenel OnGuard	XP 2016 R3	XP 2017 R1-R3	XP 2018 R1	XP 2018 R2	XP 2018 R3
7.0	U*	U*	U*	U*	U*
7.1	S	S	S	S	S
7.2	S	S	S	S	S
7.3	S	T	S	T	S
7.4	S	S	S	T	S

*OnGuard 7.0 is end-of-life and no longer supported or maintained

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 2016 R1-R2	While these versions of XProtect remain compatible with the XProtect Access Lenel OnGuard integration, they do not however support user privileges and alarm acknowledgement functionality. Milestone does not recommend using these versions of XProtect for the Lenel OnGuard integration
XProtect 2016 R3	First version to add support for Alarm Acknowledgement in Lenel OnGuard
XProtect 2017 R1-R3 And 2018 R1-R3	These versions are fully supported*

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

Lenel OnGuard Version details

Version	Minimum update / patch level	Version Information
OnGuard 7.0	7.0.1107.0	This OnGuard version is end-of-life from Lenel and is no longer supported. Milestone follows the support lifecycle of Lenel OnGuard for the integration.
OnGuard 7.1 OnGuard 7.2	7.1.481.74 7.2.269.67	Make sure OnGuard is on at least version 7.1.481.74 or 7.2.269.67. Some bugs in DataConduIT prevent the integration from working on older versions of 7.1 / 7.2
OnGuard 7.3 OnGuard 7.4 RTM	7.3.345.0 7.4.457.0	These versions are fully supported
OnGuard 7.4 Update 1	7.4.457.69	OnGuard has issues detecting I/Os on OSDP connected readers.

Hardware Support

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

Verify your installation's panel model numbers against this list, if one of your panels is not contained in this list, please contact your integrator and/or Milestone support to verify compatibility

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 and performance metrics that can be expected of the integration

Lenel OnGuard Certification Tested Setup

Type of Device	Count
Panel	1927
Door	1031
Reader	1031
IOModule	14
Input	2074
Output	2055
Card Holders	44544

Events Handled

This integration has been tested against 15,000 events from Lenel OnGuard in both DataConduIT and OpenAccess modes. For more about supported events, see Milestone-ACM-Lenel-OnGuard-Events.pdf

	DataConduIT	OpenAccess
Number of events sent from OnGuard	15,000	15,000
Time to send 15,000 events by OnGuard	3 minutes	11 minutes
Number of events received in XProtect	15,000	15,000
Time to receive 15,000 events in XProtect	4 minutes	26 minutes
Nb of events that had associated alarms in XProtect	10,200	10,200
Event Throughput from OnGuard to XProtect	15,000 evts / 4 mins *62.5 events / second*	15,000 evts / 26 mins *9.61 events / second*
Alarm Generation Throughput (XProtect)	10,200 alarms / 4 mins *42.5 alarms / second*	10,200 alarms / 26 mins *6.5 alarms / second*
XProtect Version	2018 R2	2018 R2
XPA Version	3.0.18262	3.0.18262
Lenel OnGuard Version	7.4.457.69	7.4.457.69
Test Date	September 20, 2018	September 19, 2018

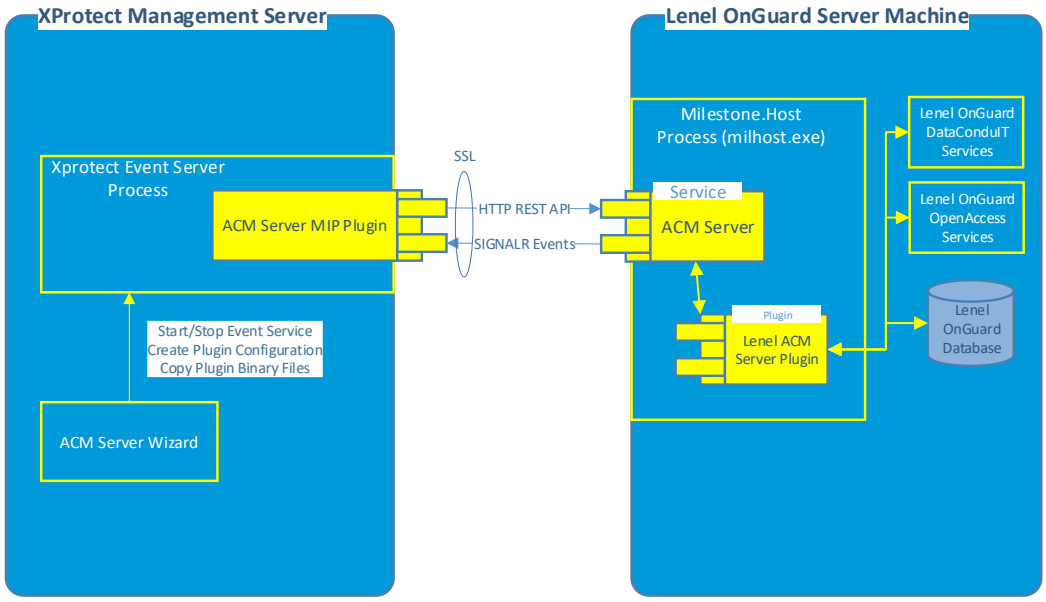
General Description

Introduction

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

- Retrieve configuration from the Lenel OnGuard AC system, e.g. doors and event types
- Receive AC event streams and state changes from the Lenel OnGuard system
- Get/Search cardholder information with picture association
- Create alarms in alarm manager based on AC events.
- Alarm state synchronization between XProtect (2016 R3 or greater) and Lenel OnGuard when the alarm is acknowledged in XProtect. Alarm acknowledgment synchronization when the alarm is acknowledged in Lenel OnGuard is not implemented due to the lack of support for this feature in the OnGuard SDK.
- 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 Lenel 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 Lenel OnGuard server (Milestone.ACMServer.msi)
3. The "Lenel OnGuard ACM Server Plugin" that runs on the Lenel OnGuard server (Milestone.ACMServer.LenelOnGuard.msi)

Prerequisites

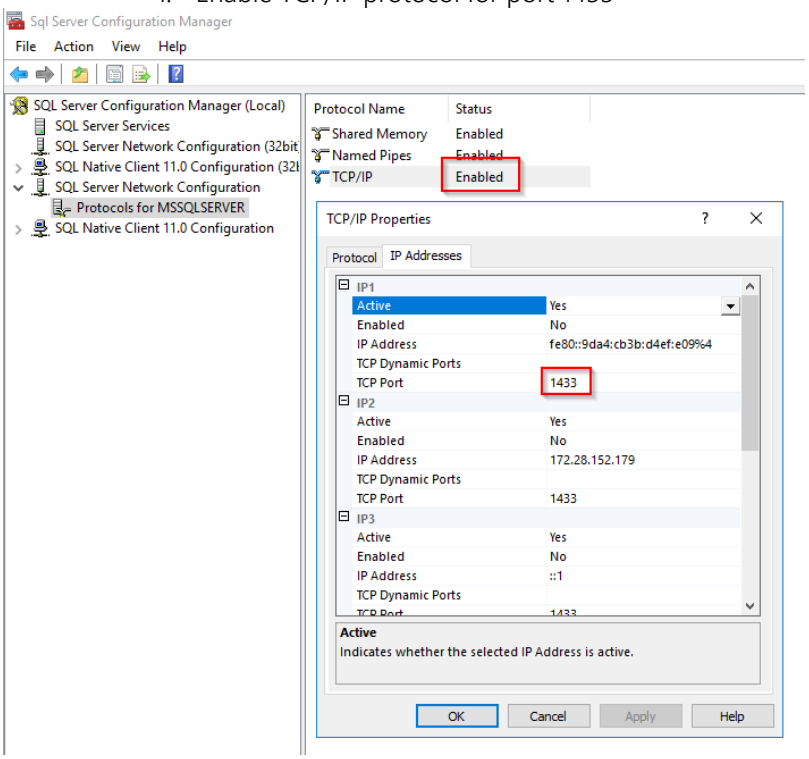
Time Synchronization

All servers (i.e. the Lenel 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 Lenel OnGuard SQL for remote connections

These instructions are here to help setup a SQL server instance to enable remote connections so that the Lenel 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 method of enabling 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 Lenel OnGuard Server machine

.NET Framework 4.5 must be installed on the Lenel 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.

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2018 R2 Test	M01-C01-	6/19/2019	N/A	N/A
Milestone XProtect Smart Wall	M01-P03-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-	6/18/2019	6/18/2019	

1

License Overview - All sites License Details - All Sites...

License Type	Activated
Hardware Device	13 out of 25
Access control door	7 out of 29

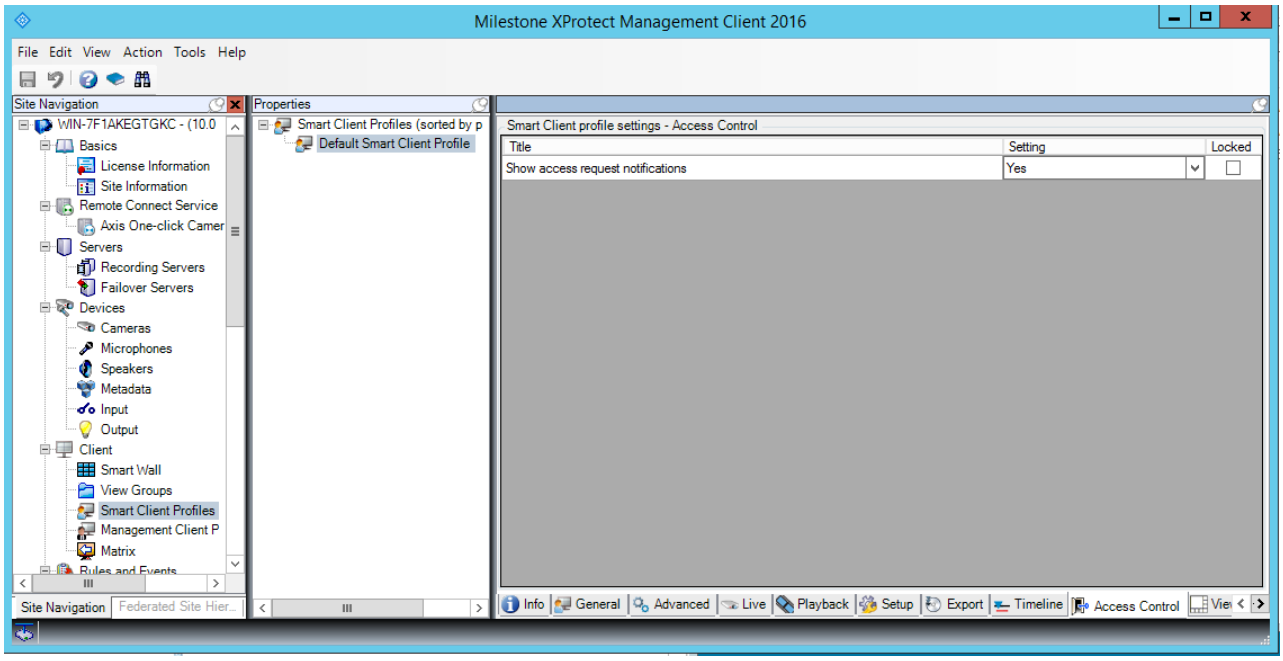
2

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 Lenel OnGuard Server machine (e.g. DNS, manual host file entry, etc). The Lenel 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.



Lenel OnGuard: License Options

To enable the integration to work in either DataConduIT or OpenAccess connection modes the following license options must be enabled in the Lenel OnGuard license:

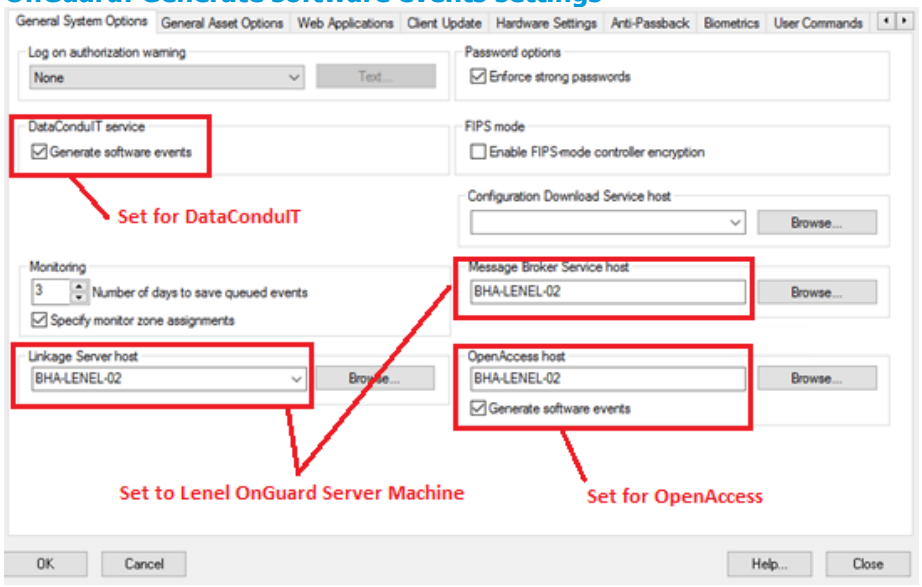
Type of Connection	Lenel OnGuard License Options Needed
DataConduIT	Maximum Number of DataConduIT Clients (SWG-1140) must be >= 1
OpenAccess	Maximum Number of Open Access Clients (ITM-MLST-001) must be >= 1

Lenel OnGuard: Mandatory Windows Services

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

Lenel OnGuard Windows Service Name	Description
LS Communication Server	Required for the hardware to communicate with the Lenel OnGuard system
LS Linkage Server	Required for event handling
For DataConduIT	
LS DataConduIT Service	Required for our integration to use the Lenel OnGuard DataConduIT API
For OpenAccess	
LS OpenAccess	Required to interface the Lenel OnGuard system web service-based API OpenAccess (REST/JSON web service)
LS Web Service	Required to interface the Lenel OnGuard system web-service-based events with OpenAccess (SignalR)

Lenel 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 a Lenel OnGuard version 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 Lenel OnGuard server's machine name.

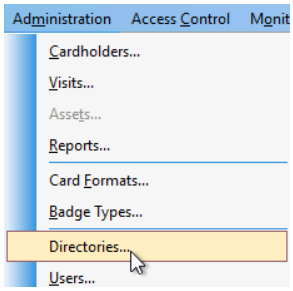
4. Set the Message Broker Service Host to the Lenel OnGuard server's machine name.

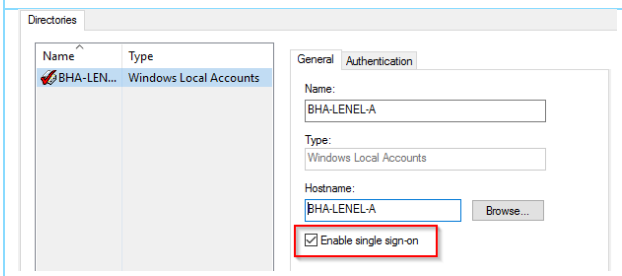
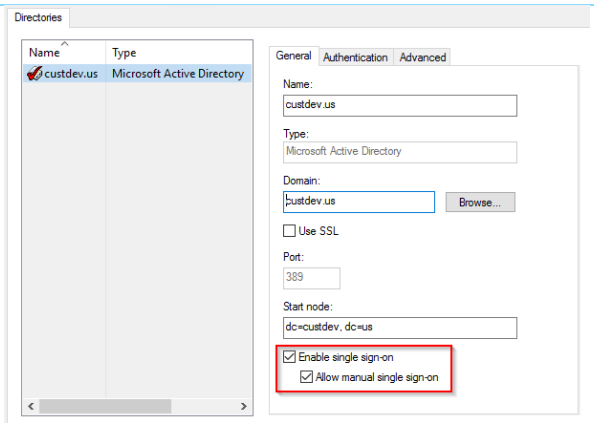
Lenel OnGuard: Create Single Sign-On (SSO) Directory

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 Lenel OnGuard system.

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

Using the Lenel 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.
	

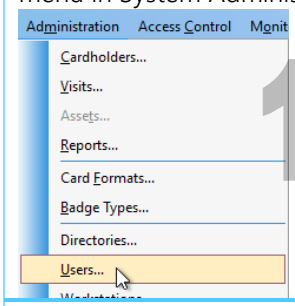
If you are creating a Directory of a type other than "Windows Local Accounts" (e.g. LDAP, Active Directory), ensure that the SSO user is a member of the Local Administrators group.

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

Lenel OnGuard: Create Single Sign-On (SSO) User

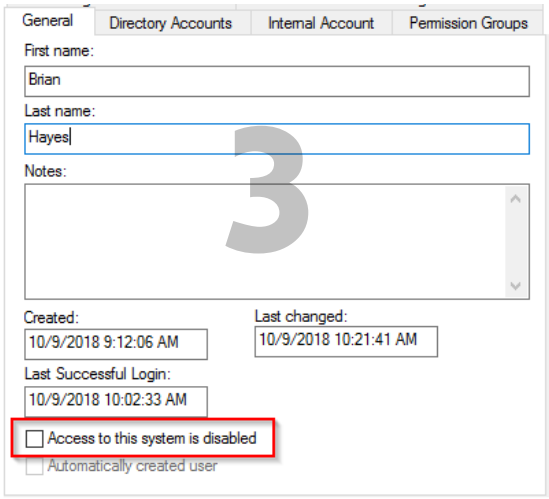
These instructions are not meant to replace the knowledge of a trained Lenel system administrator. They are here to enable the basic setup of an authentication directory and SSO user so that the integration can connect to the Lenel OnGuard system.

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

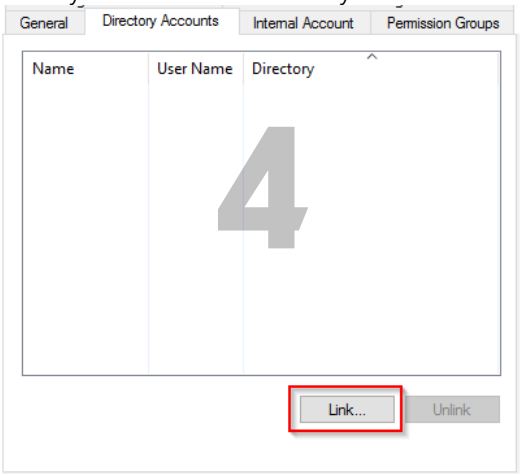


Add a new user.

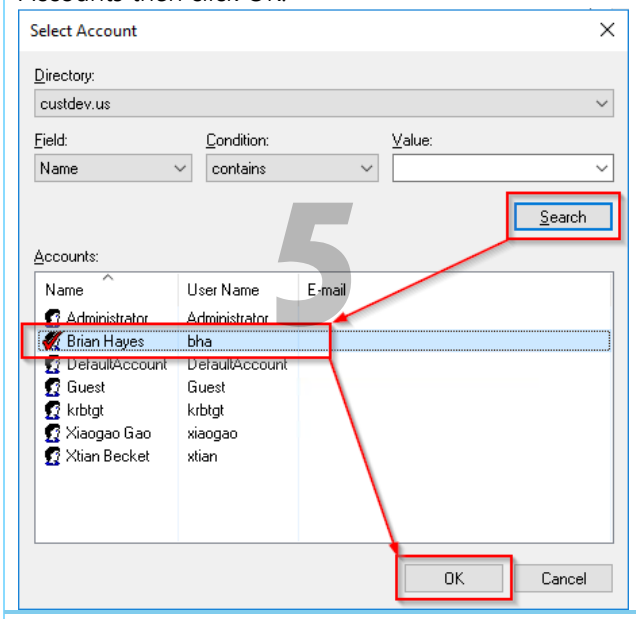
General tab -- Be sure that "Access to this system is disabled" is NOT checked.



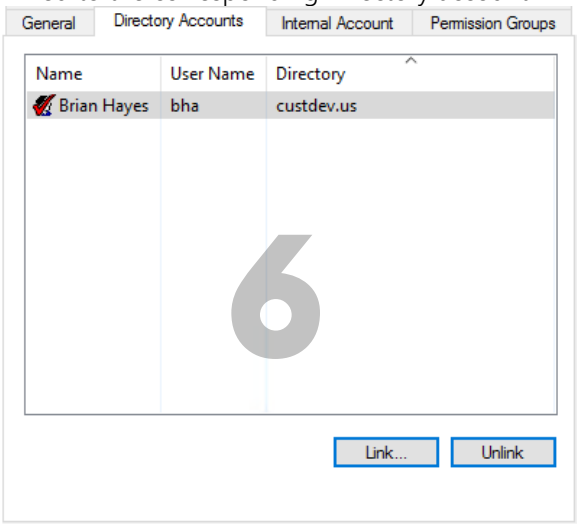
Directory Accounts tab -- Link the user to the directory user from the directory created above.



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

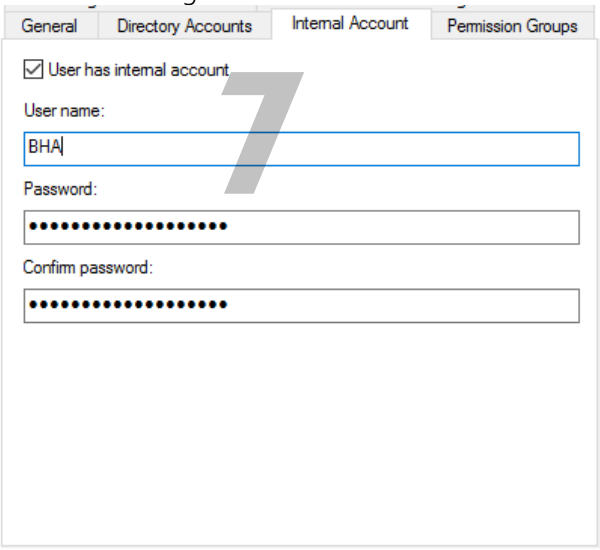


Once selected the Lenel OnGuard user account is linked to the corresponding Directory account



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:

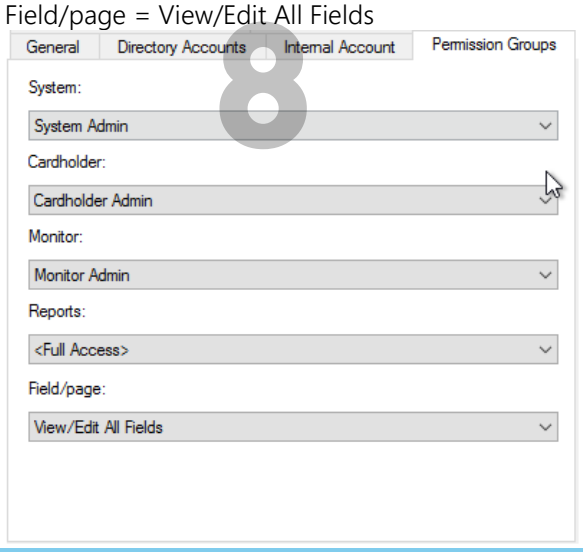
System = System Admin

Cardholder = Cardholder Admin

Monitor = Monitor Admin

Reports = Full Access

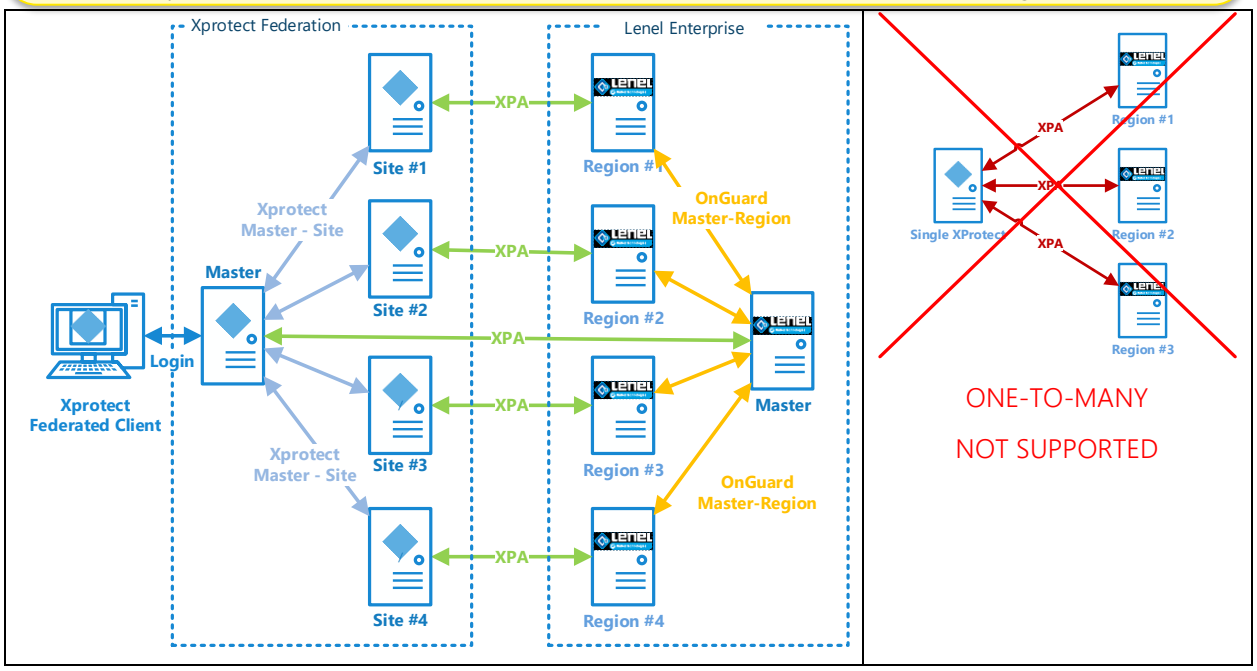
Field/page = View/Edit All Fields



Lenel OnGuard: Enterprise Configurations

If the Lenel OnGuard system is part of an Enterprise deployment, the Enterprise system must be correctly configured and functioning before setting up the integration. Each Lenel OnGuard Region of an Enterprise system must be independently connected through XProtect Access (XPA) to each Milestone XProtect Site of a Federated system.

Lenel OnGuard Enterprise scenarios require that each regional Lenel OnGuard installation has a maximum of one corresponding Federated XProtect site that connects to it. Each XProtect site, for performance reasons, should never have more than one Lenel OnGuard region connected.

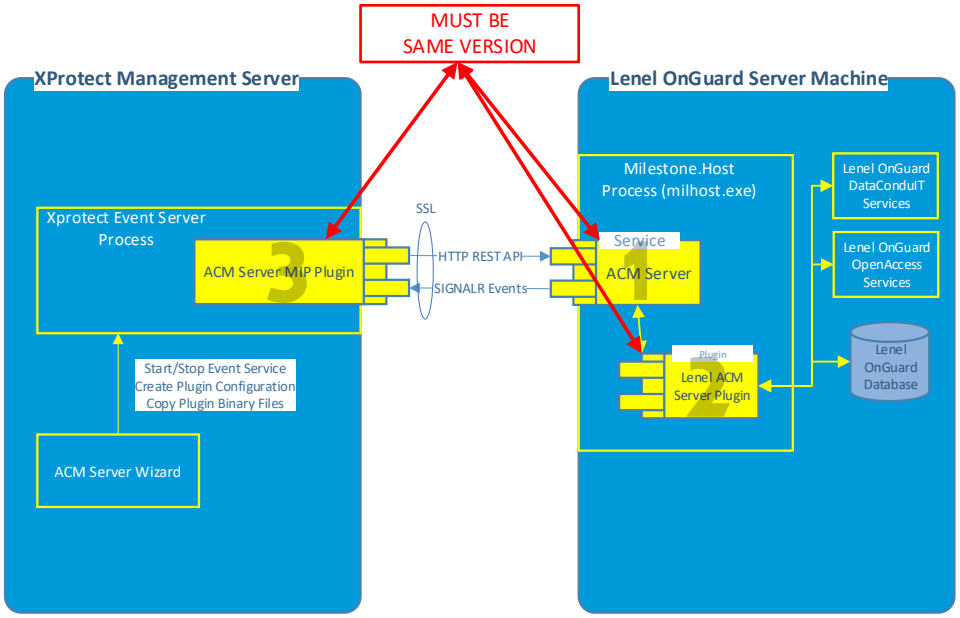


Installation

The installation package consists of three independent installers:

1. Milestone.ACMServer.msi: Installer for the ACM Server
   - Installed on the Lenel OnGuard server machine
2. Milestone.ACMServer.LenelOnGuard.msi: Installer for the Lenel OnGuard ACM Server plugin
   - Installed on the Lenel OnGuard server machine, after the ACMServer.
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

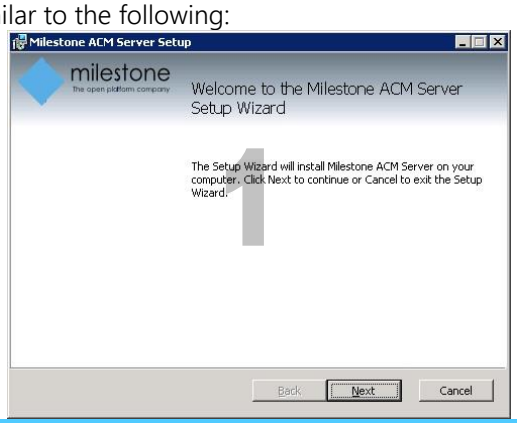
Please install them in the order specified above, following completion of the prerequisites section.



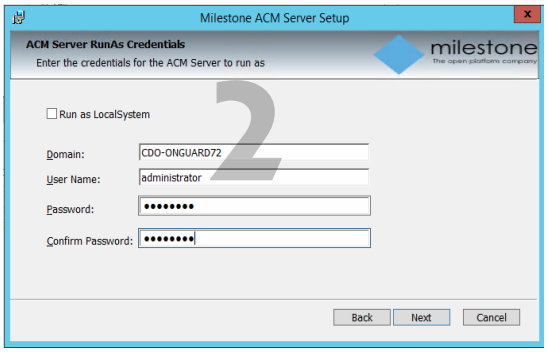
It is mandatory that the *same version* of the Lenel OnGuard ACM integration be installed on both the XProtect and Lenel OnGuard machines.

ACM Server Installation

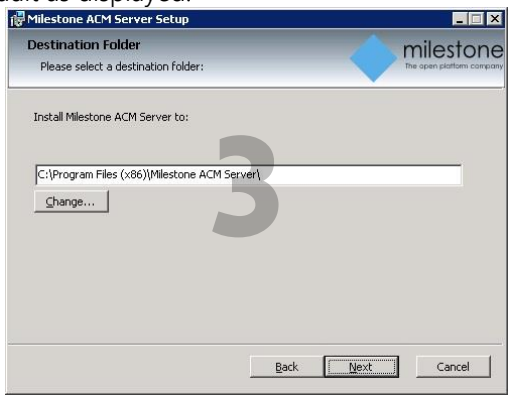
Double-click to install, you should see a screen similar to the following:



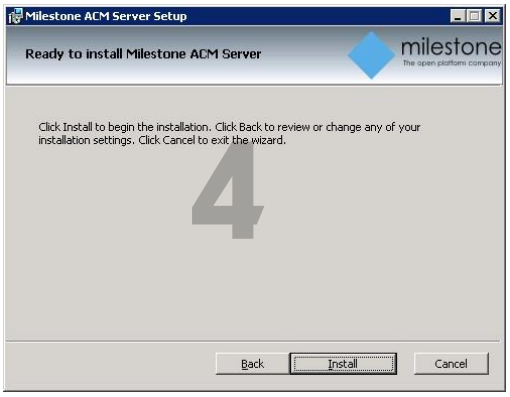
If using DataConduIT, you must enter the SSO credentials that will be used for the DataConduIT connection to Lenel OnGuard.



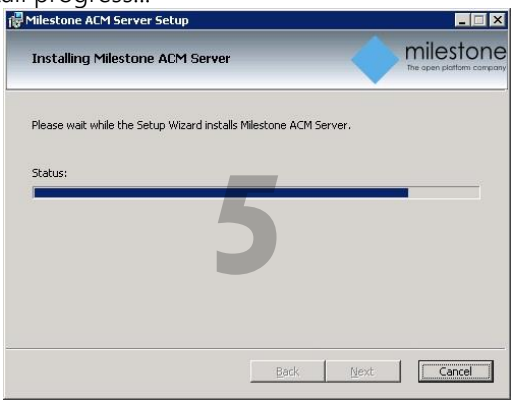
Press next and you will now be able to select the installation path, it is recommended to use the default as displayed:



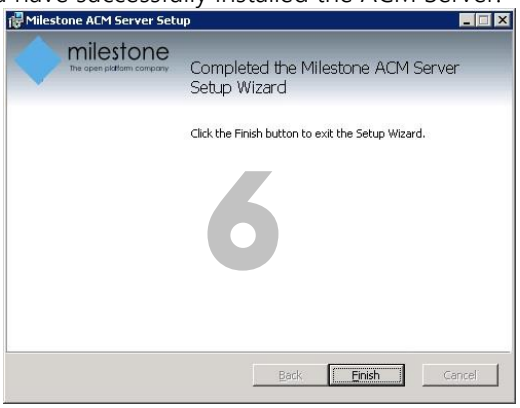
Press next and you are now ready to install, if you are satisfied with the selected options, press install to continue:



Install progress...



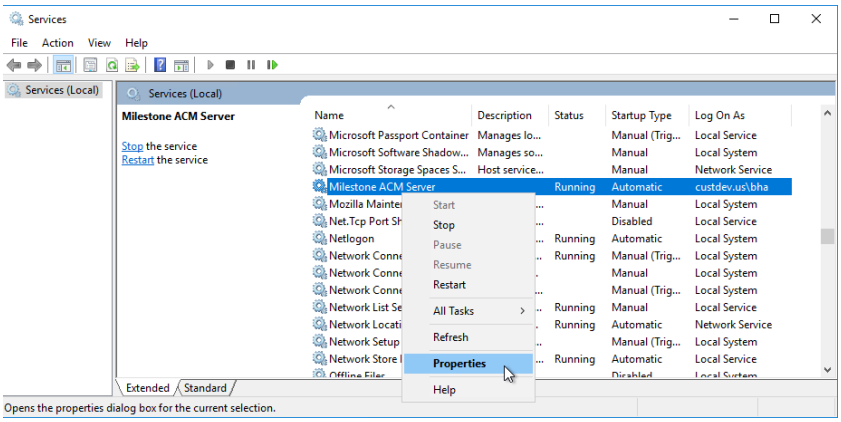
You have successfully installed the ACM Server:



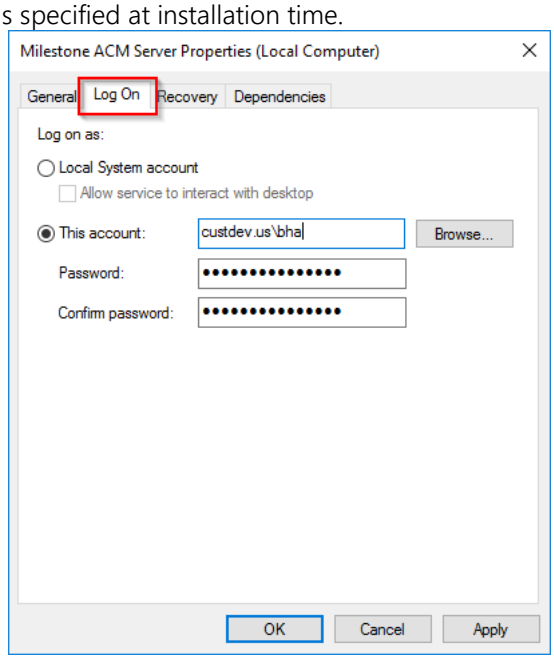
ACM Server Credentials

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

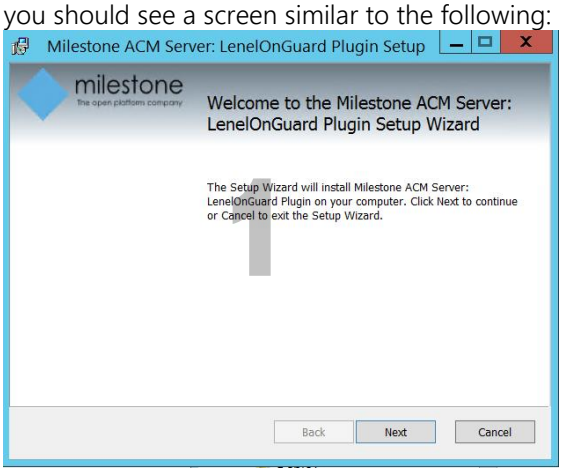


2- Go to Log On tab, select "This account", and enter/change the SSO credentials that will be used for the DataConduIT connection to Lenel OnGuard. You should only need to do this in case you need to modify the credentials specified at installation time.



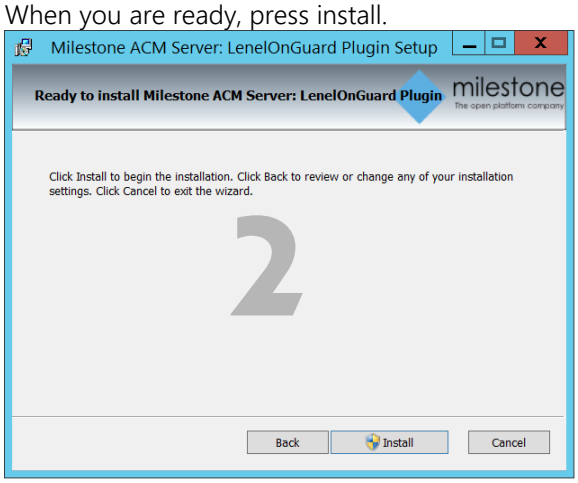
ACM Server: Lenel OnGuard Plugin Installation

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

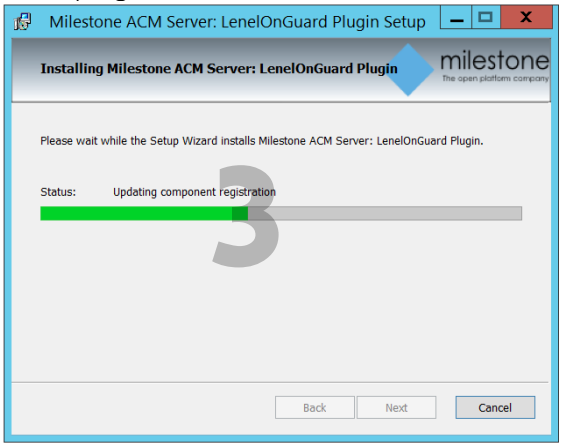


The Lenel OnGuard plugin automatically detects the presence of both the Lenel OnGuard server and the pre-installed ACM Server. If either is missing it will refuse to install.

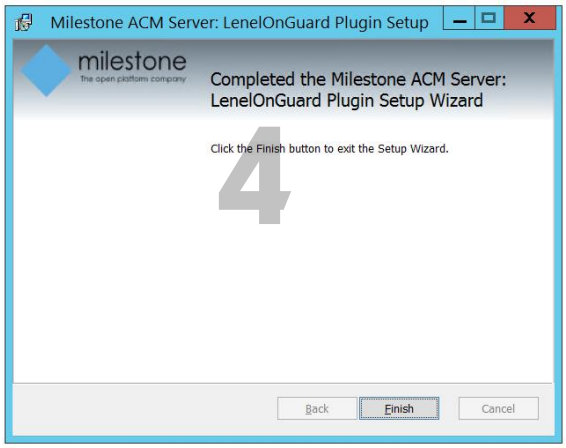
There are no configurable options in this installer. When you are ready, press install.



Install progress...

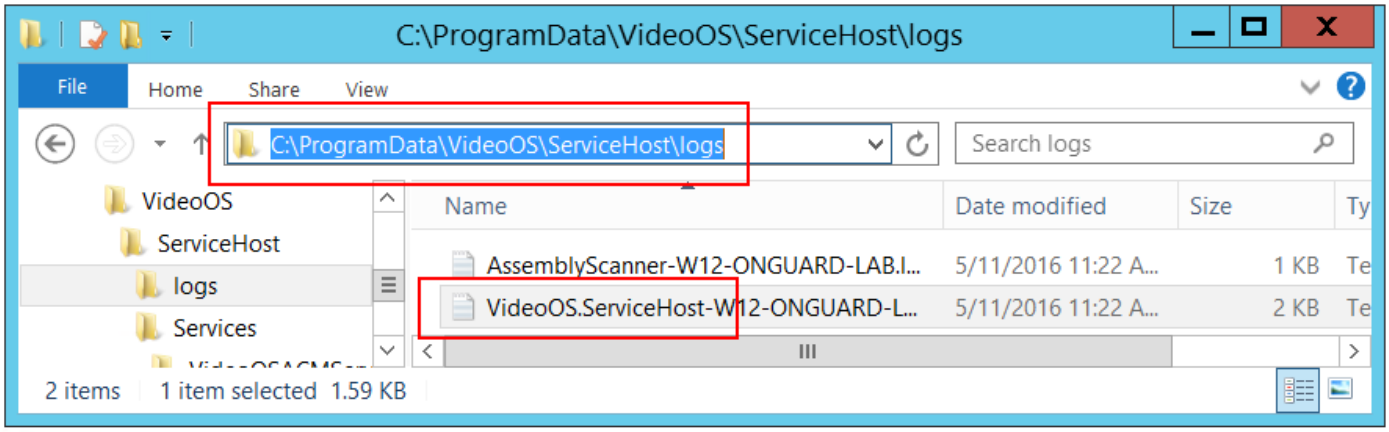


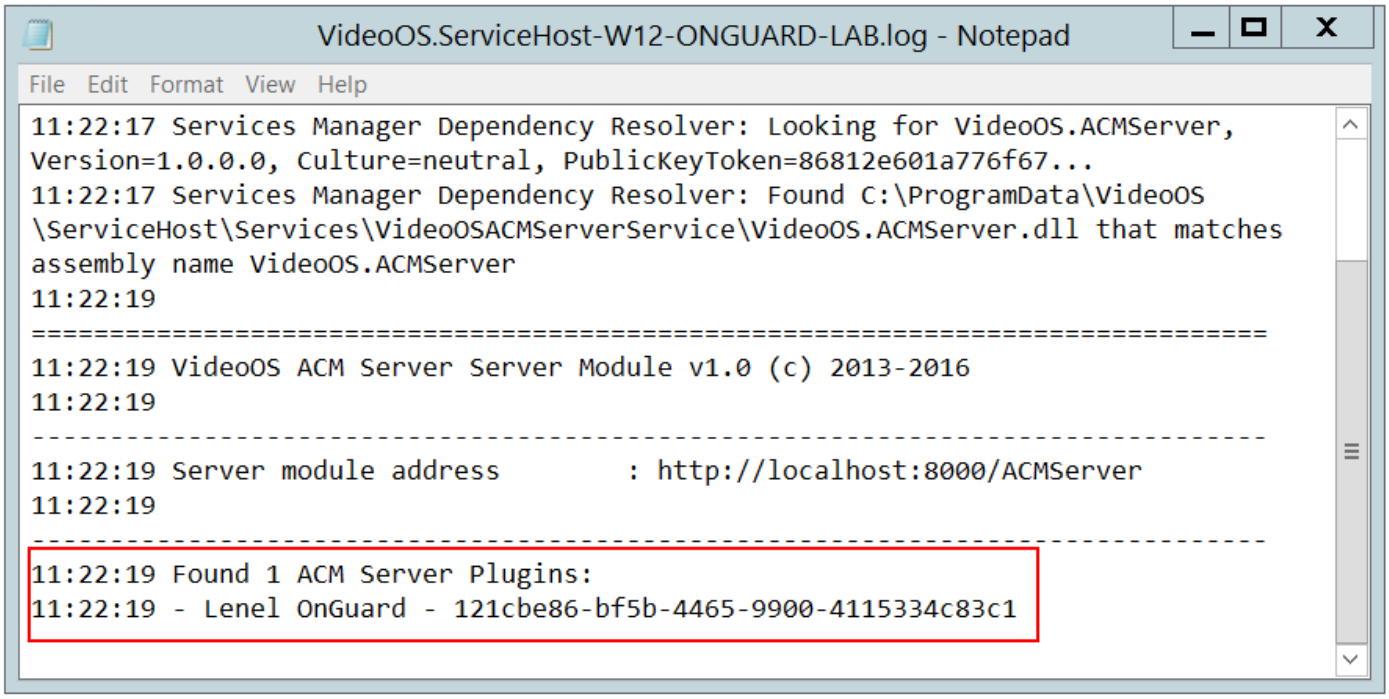
You have successfully installed the Milestone ACM Server Lenel OnGuard Plugin



ACM Server: Lenel OnGuard Plugin Post-Installation

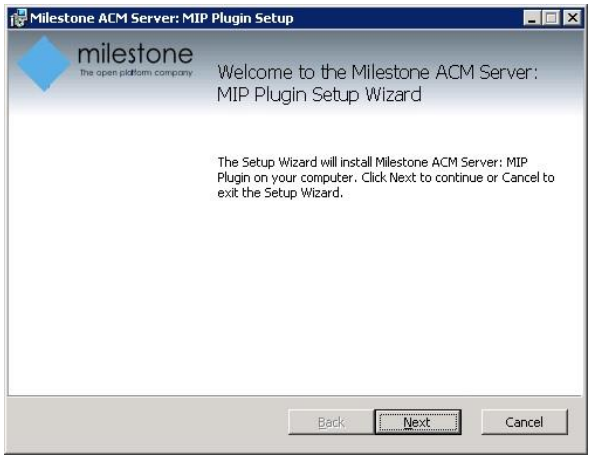
You can verify that the Lenel OnGuard Plugin is installed and loaded from the logs below:



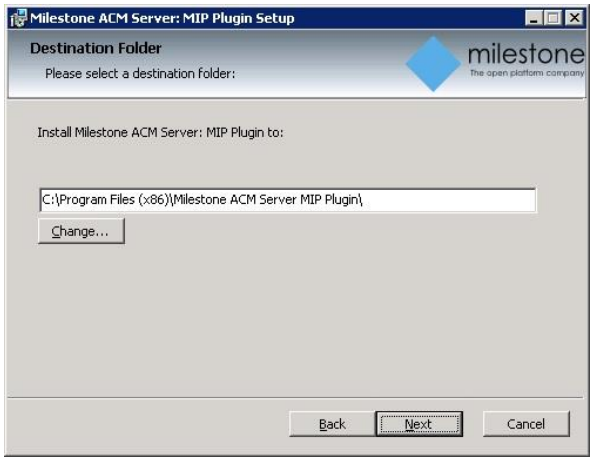


ACM Server: XProtect ACM MIP Plugin

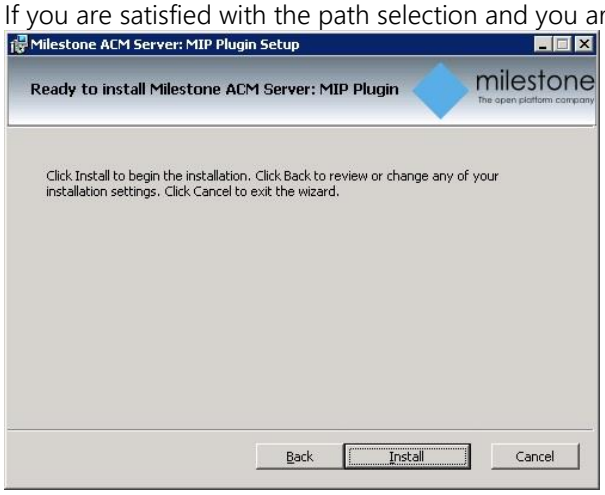
Copy the "Milestone.ACMServer.MipPlugin.msi" file to a temporay folder on the server where the XProtect Event Server is installed (in a typical deployment, this is the XProtect Management Server) and double-click to install. You should see a screen similar to the following:



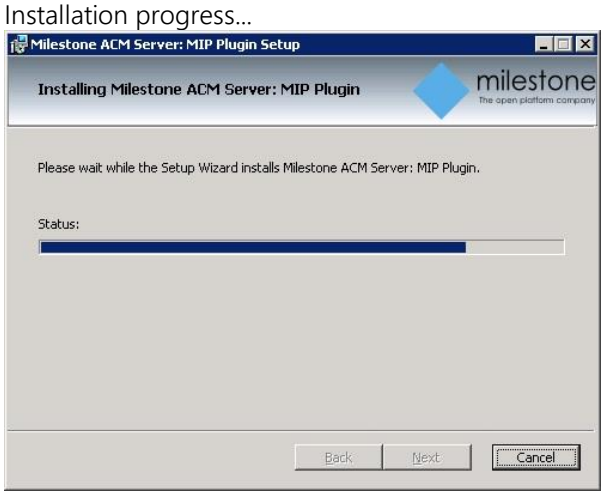
The installer will detect the presence of the XProtect Event Server on the machine and will refuse to install if it cannot be found. It is recommended to leave the default install path as displayed below and press next.



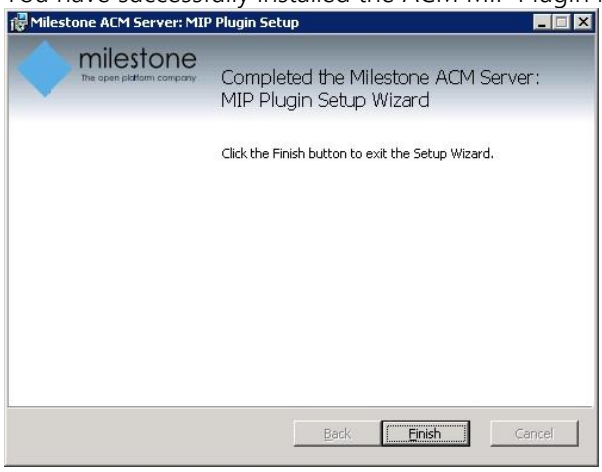
If you are satisfied with the path selection and you are ready to install press "Install"



Installation progress...

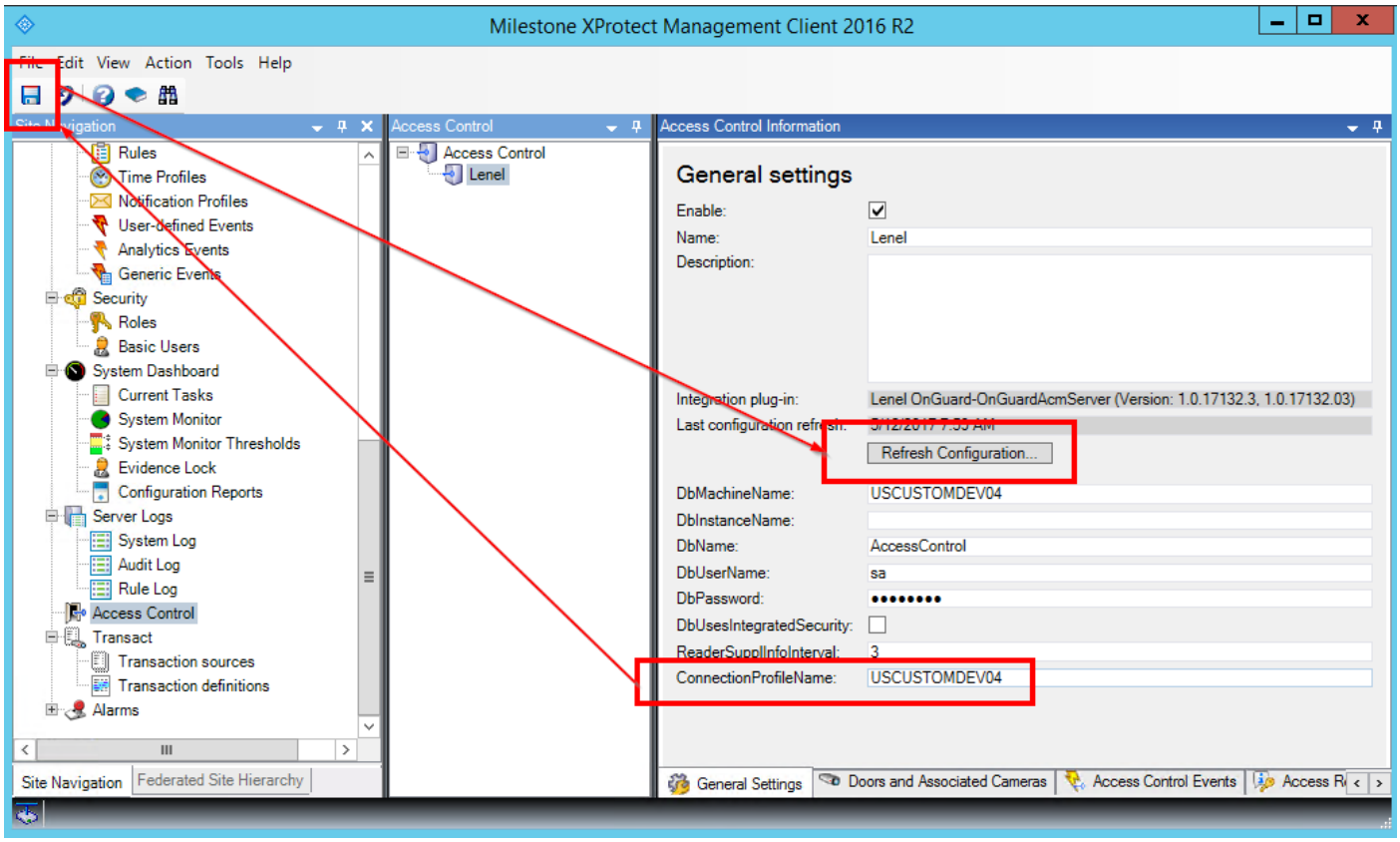


You have successfully installed the ACM MIP Plugin for ACM Server



MIP Plugin Upgrades

- IMPORTANT – Always upgrade *both* the ACM Server and Lenel OnGuard ACM plugin on the Lenel OnGuard machine *before* upgrading the MIP Plugin. We distribute all the installers with every new Lenel OnGuard ACM release.
- Automatic MIP Plugin upgrades of configured and installed instances in the Management Client are supported for all versions of the Lenel 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 ConnectionProfileName 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:

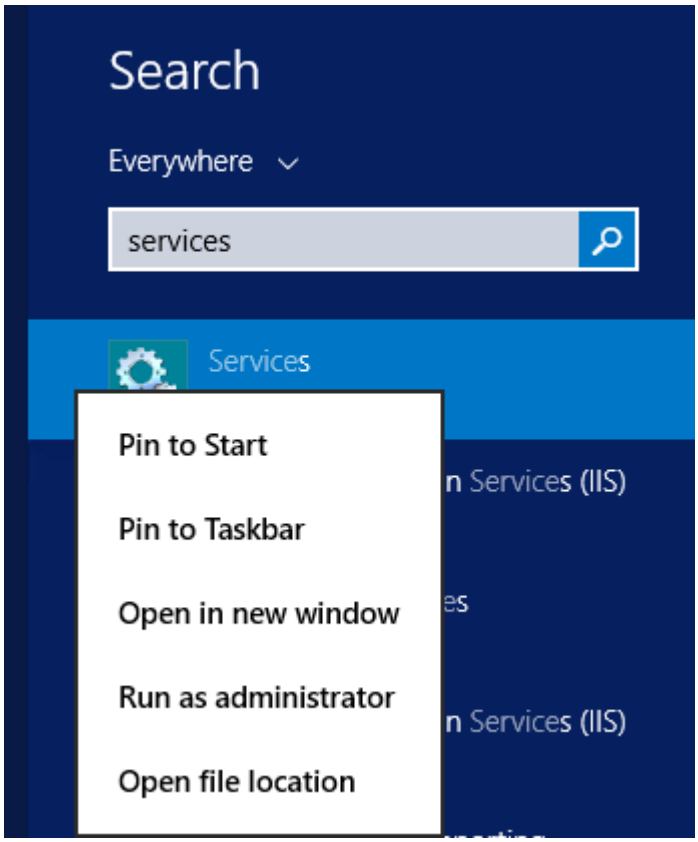
- Smart Client event history will be lost.
- Rules based off events and configured Lenel OnGuard hardware will no longer function. Rules based off the default access control event categories will not be affected and will continue to function.
- Custom event category assignments will be lost. The custom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

Lenel OnGuard Configuration

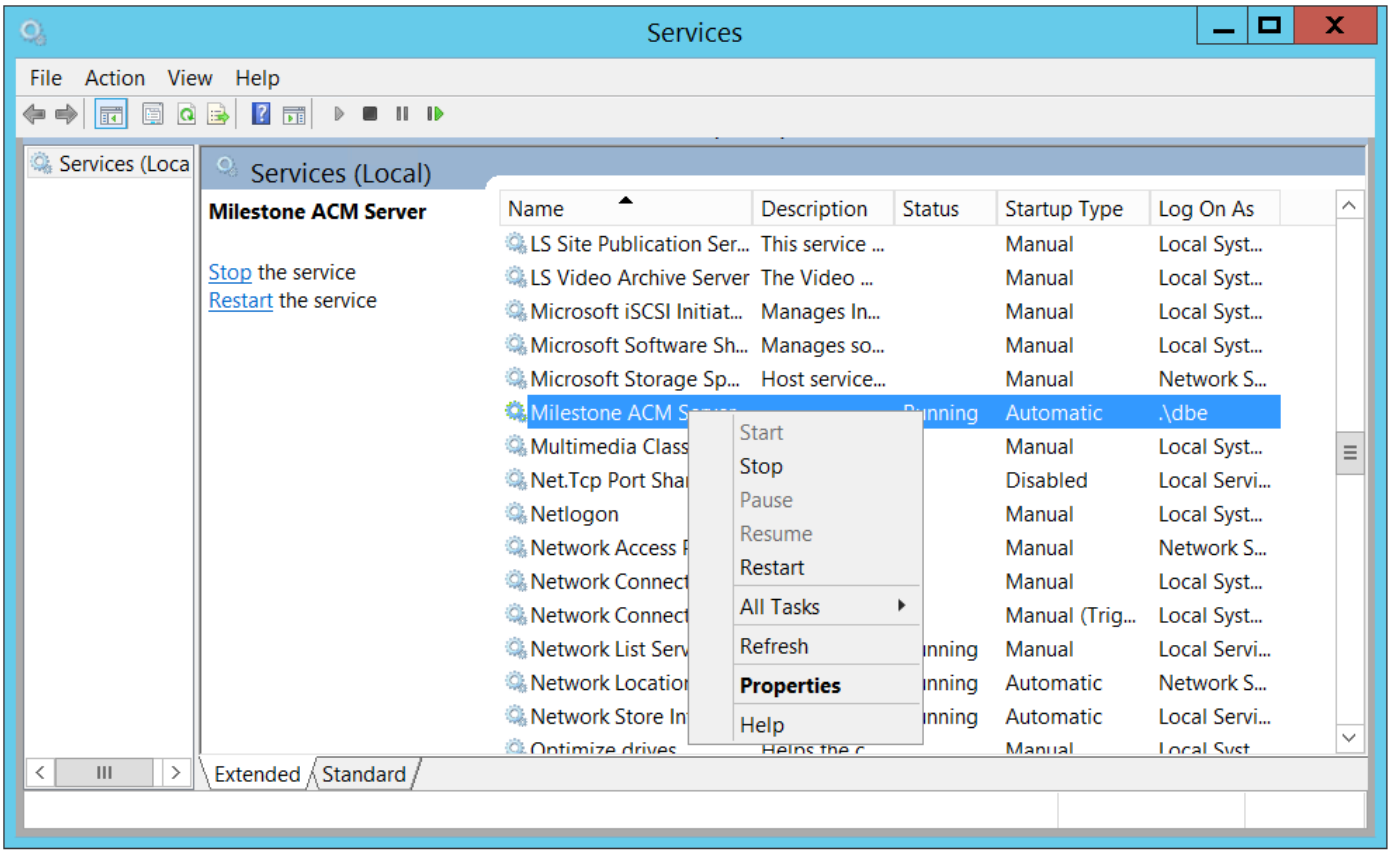
Configure to run as Lenel OnGuard Single-Sign-On Account

The Lenel 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.

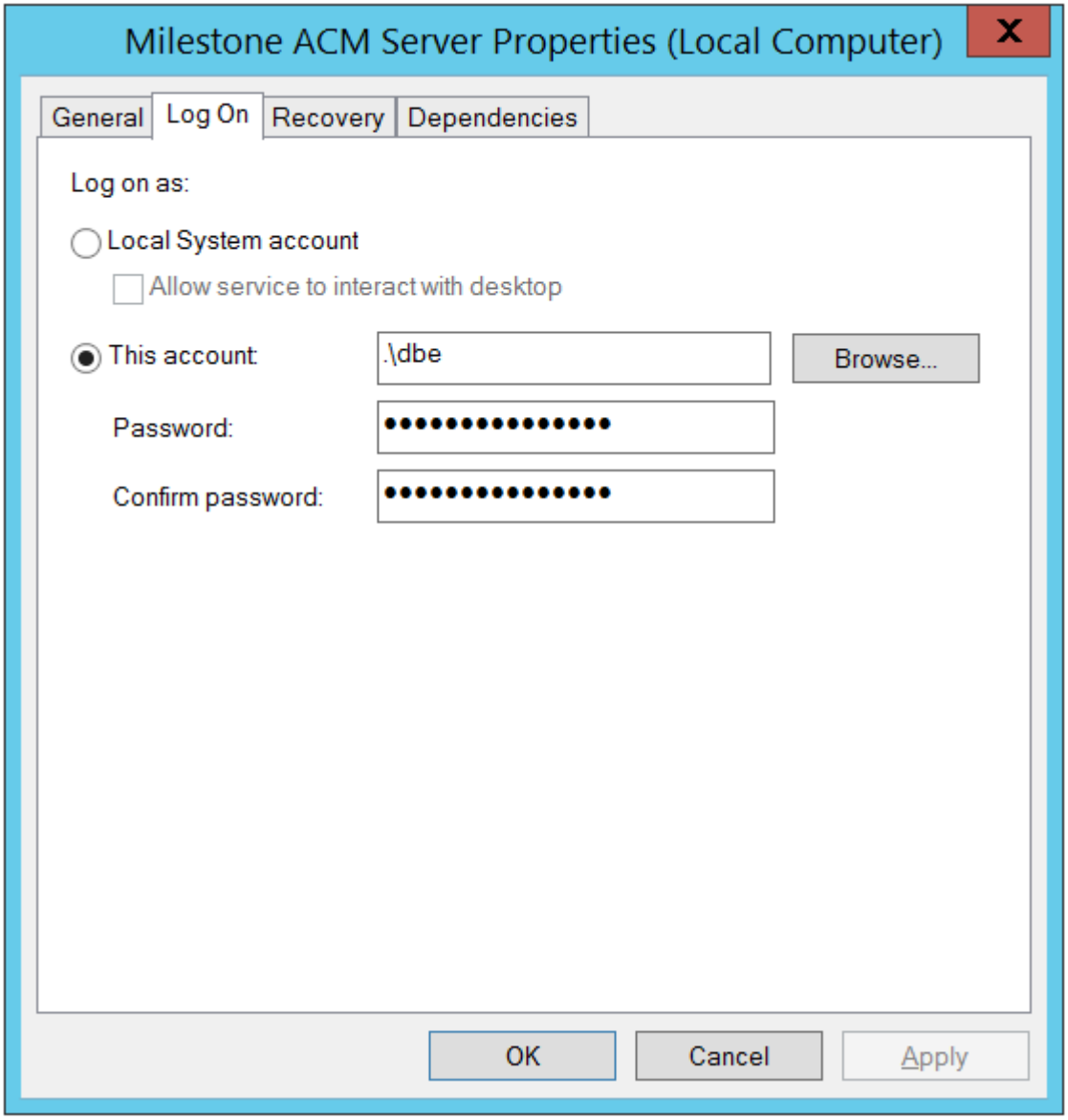
On the Lenel OnGuard server machine, click the Windows Start menu and type "services". Right click Services and select "Run as administrator".



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 Lenel OnGuard Directory that is configured for single sign-on (see above for configuring single sign-on).



IMPORTANT: Restart the Milestone ACM Server service.

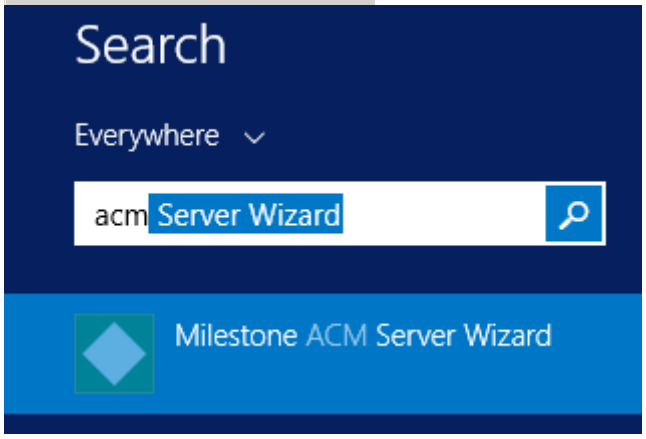
Reducing Permissions

It is not recommended to reduce the Lenel 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 Lenel OnGuard Support.

XProtect ACM MIP Plugin Configuration

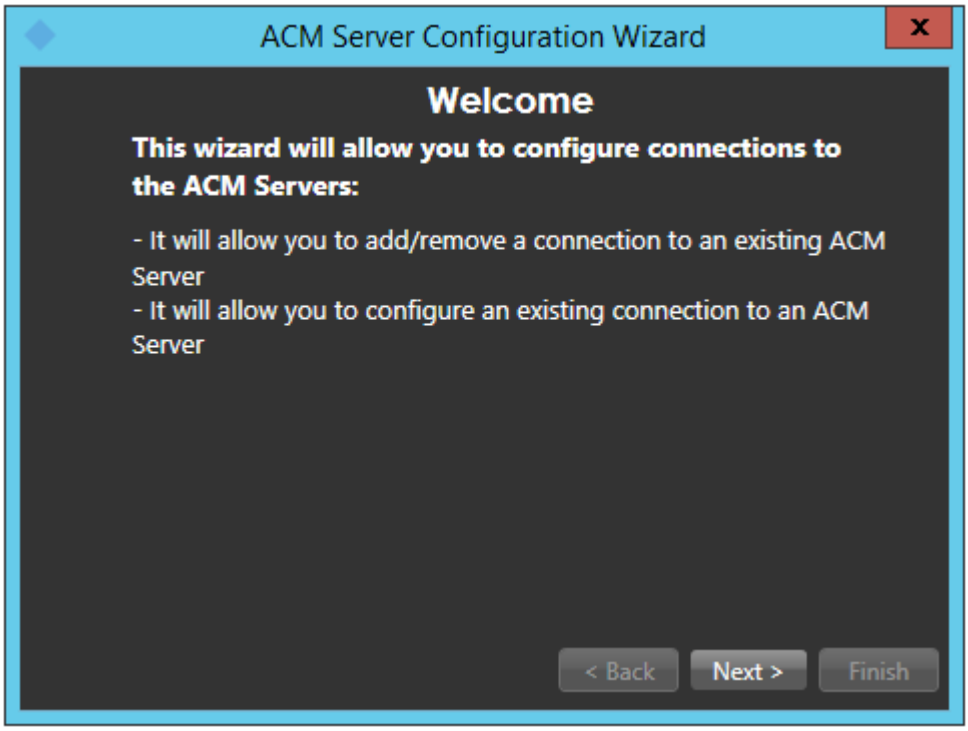
ACM Server Wizard

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:

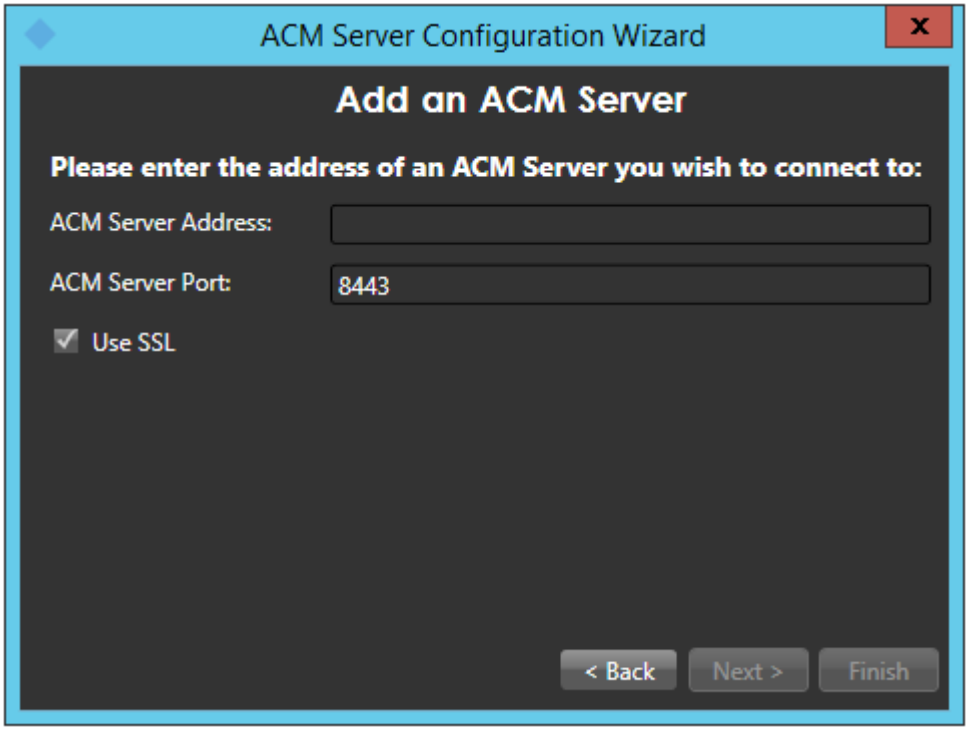


Installing an ACM Server

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

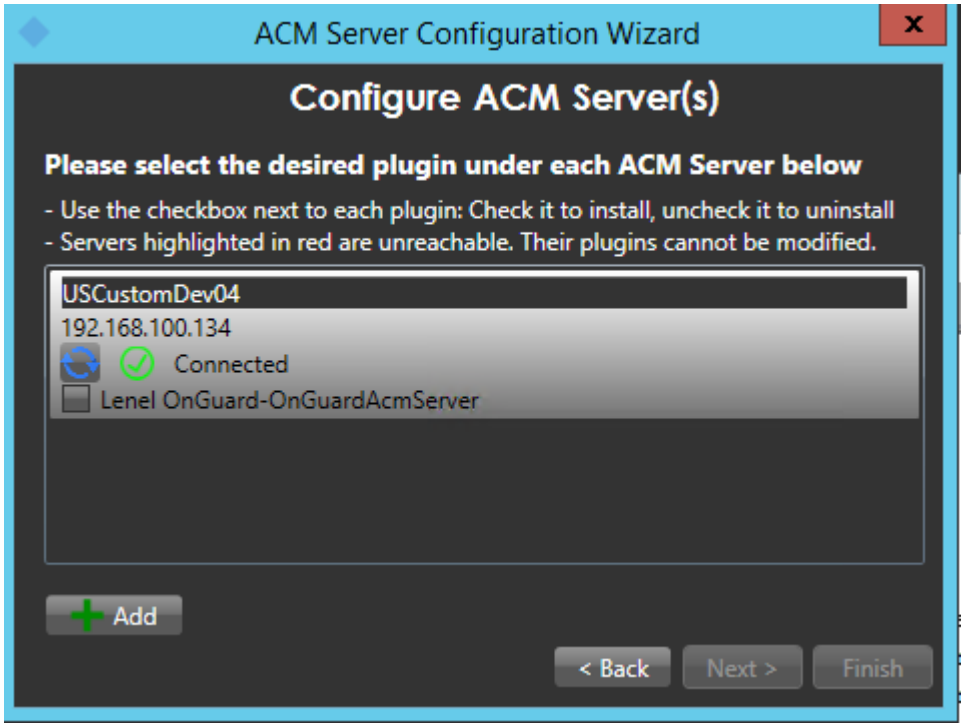


Once you click next, you will have to provide the IP Address / Machine name of the Lenel OnGuard server on which the ACM Server package was installed.

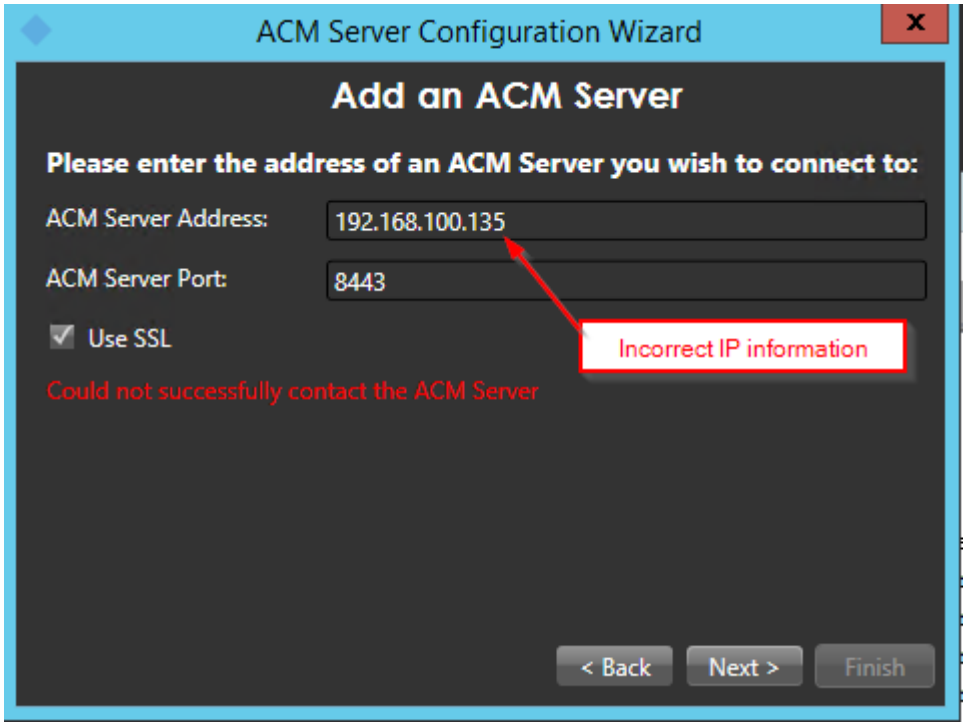


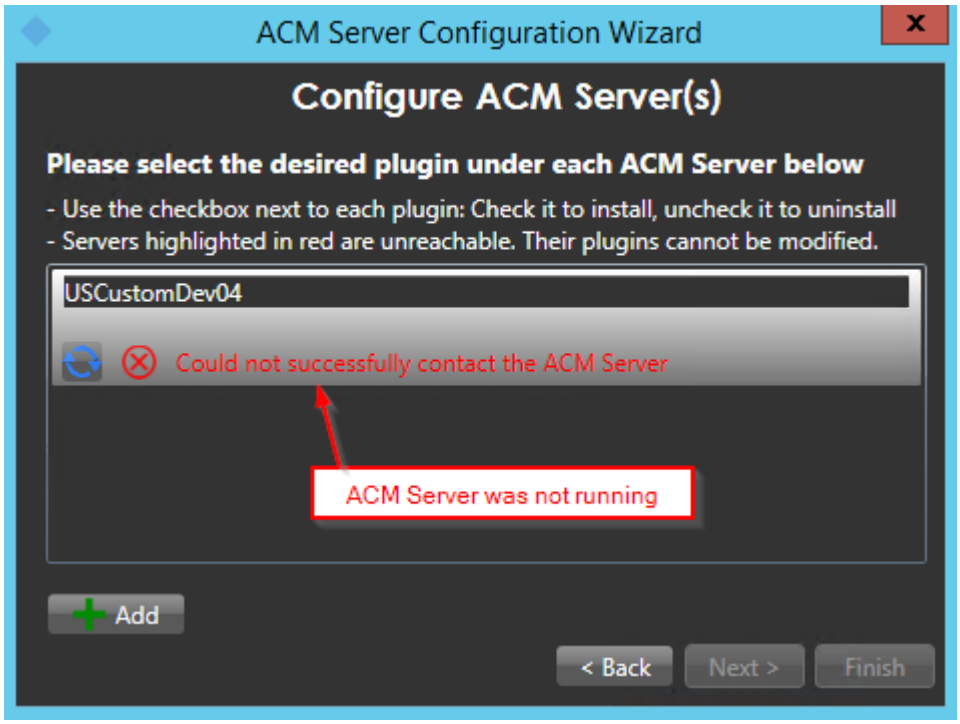
After you have provided the server name/ip address and pressed next, you should get the following screen after the software has validated that there is an ACM Server present at that address. The green checkmark means that it has successfully connected to the provided server name, the red x means that it failed to

connect to the provided server. The wizard will not allow you to proceed without a valid connection to the server.

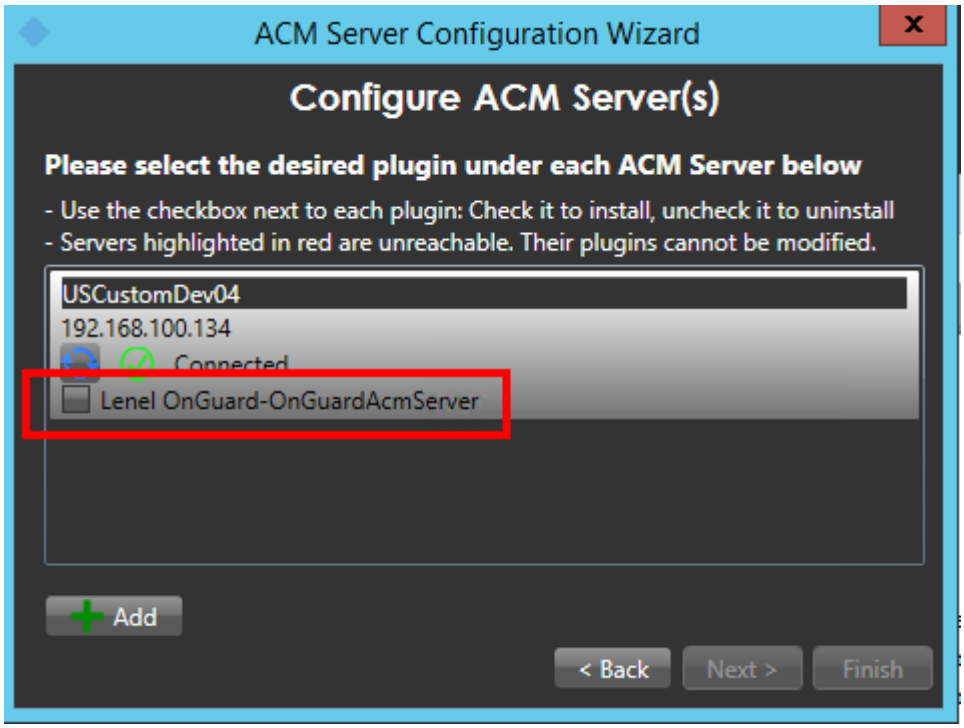


Note that the most common causes of the wizard not being able to connect to the provided server is that 1) you entered the wrong IP information, or 2) the ACM Server on the Lenel OnGuard machine is not running with sufficient administrative privileges.

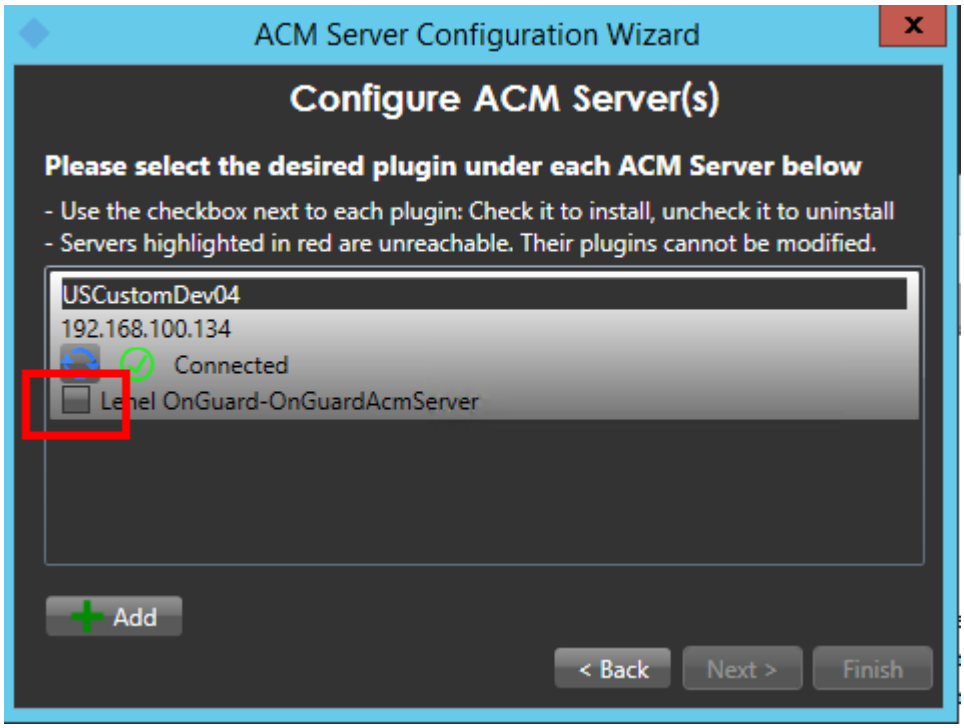




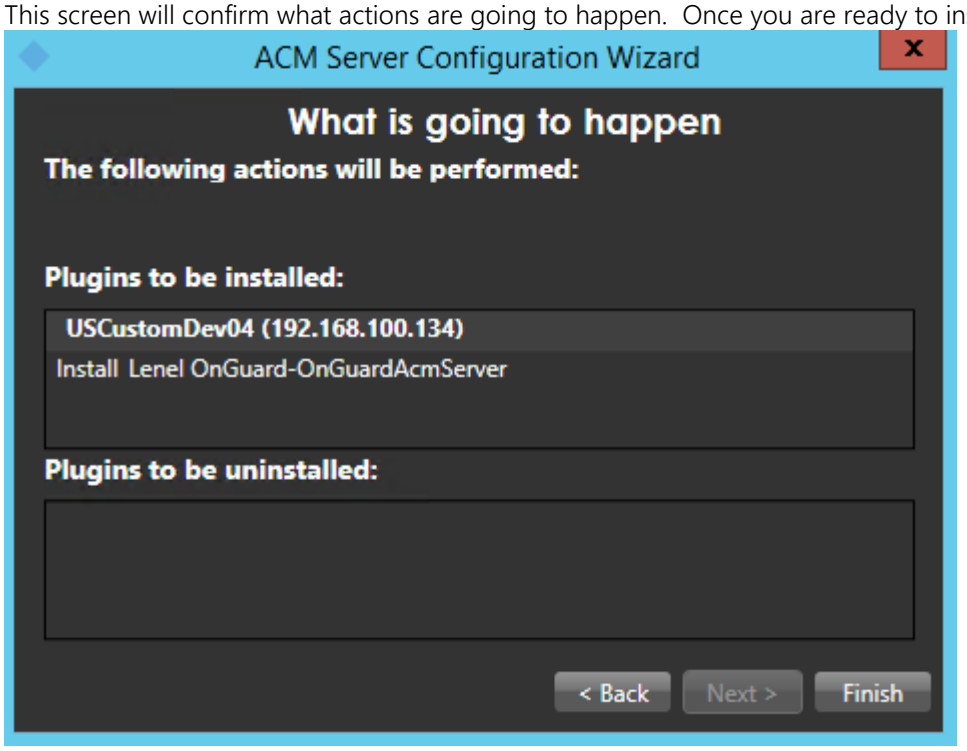
Once you have a successful connection, notice that there is a list of checkboxes under the server heading that represents all detected ACM server plugins installed on that machine. In this case we are looking for Lenel OnGuard.



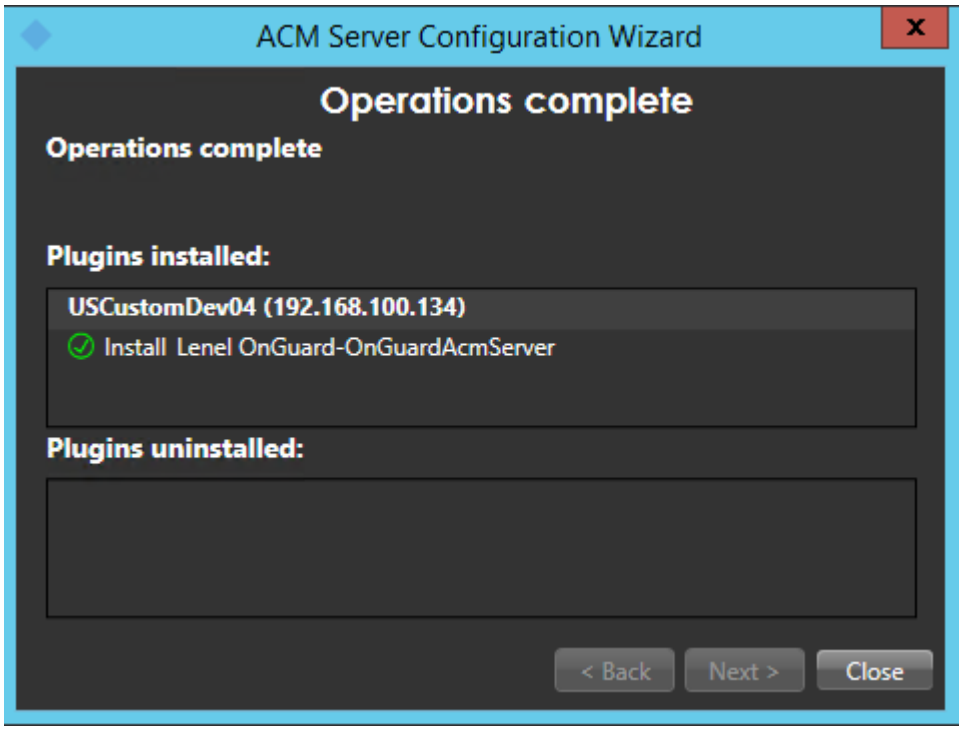
Check the box marked below and press next to install a MIP plugin on this host to connect to the Lenel OnGuard server identified.



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



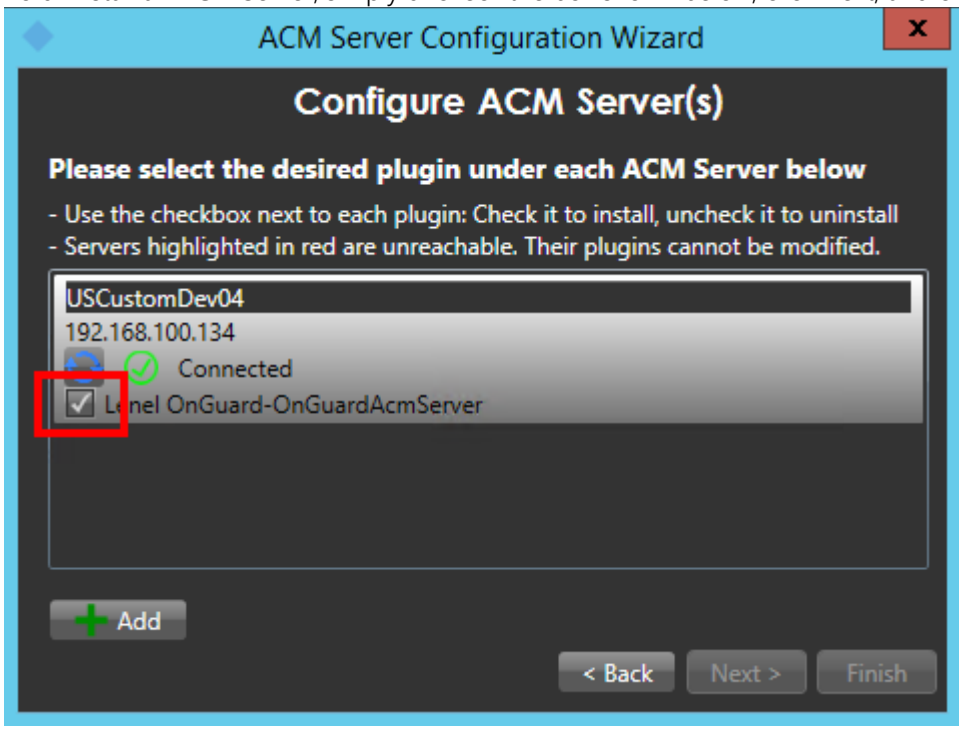
Once the operations are completed, the wizard will display a green checkmark for successful operations and a red x for failed operations.



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

Uninstalling an ACM Server

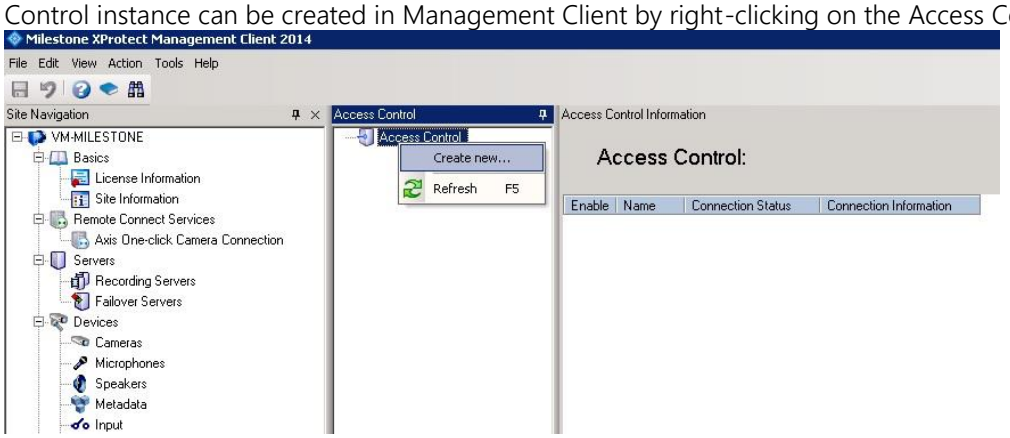
To uninstall an ACM Server, simply uncheck the box shown below, click Next, and click Finish.



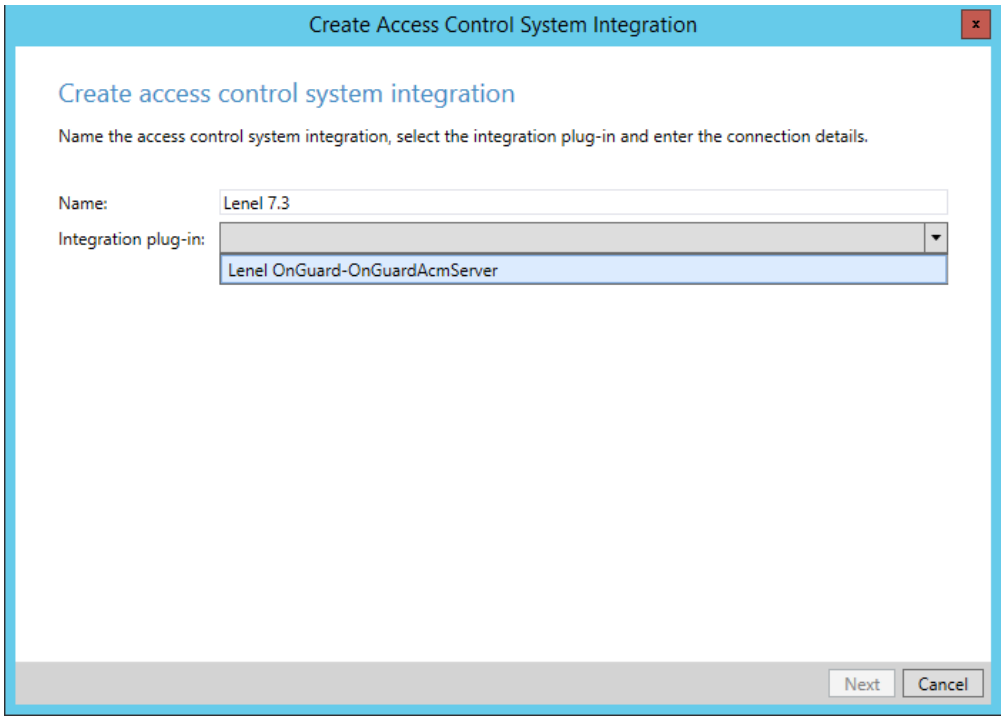
XProtect Management Client Configuration

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.

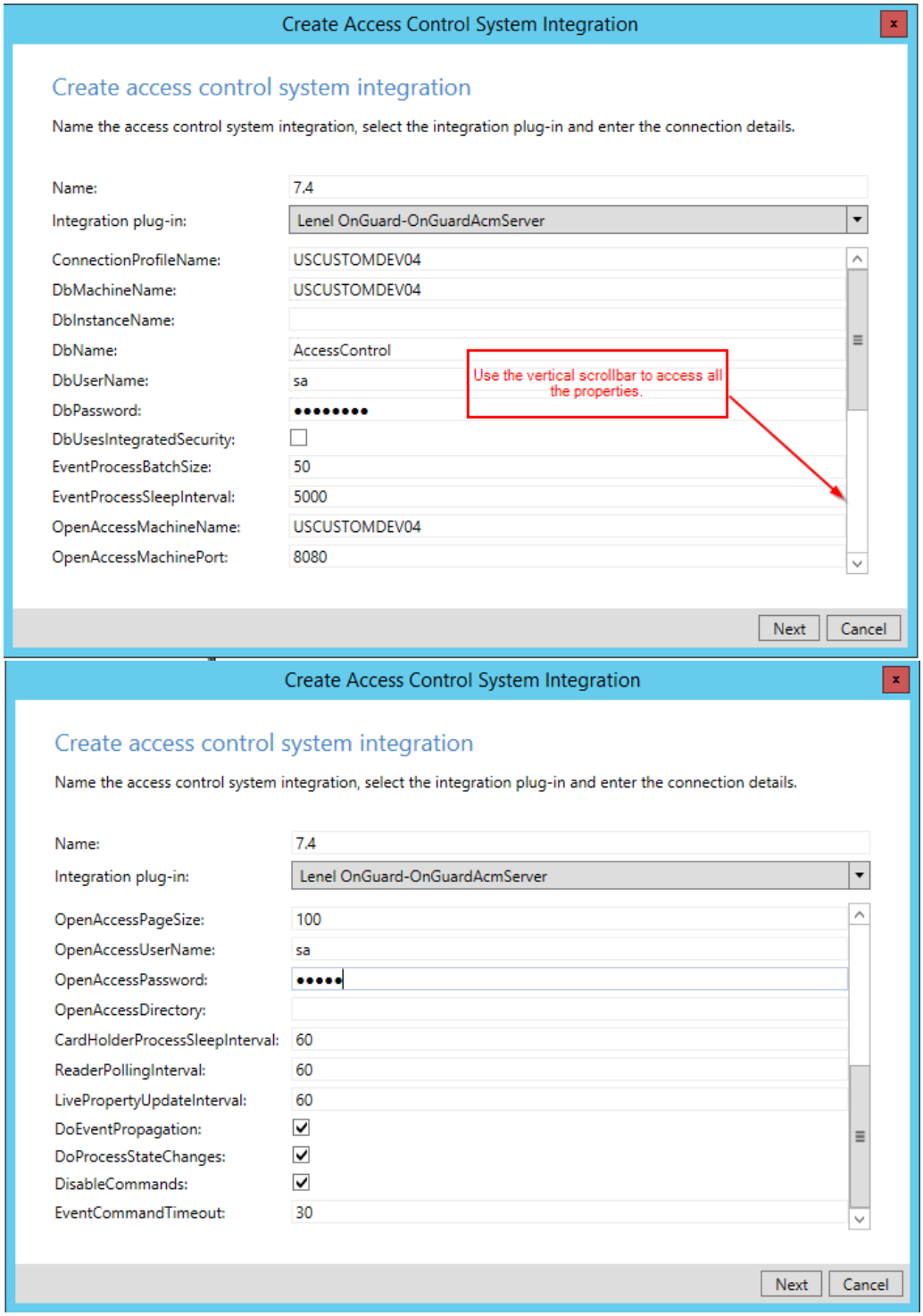


This will pop up a wizard to step you through the access control instance creation process. Type a name for the instance of the plugin you wish to create and select from the drop-down box the integration plug-in. Note that you will find a plugin named Lenel-OnGuardAcmServer-{ServerName} where {ServerName}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

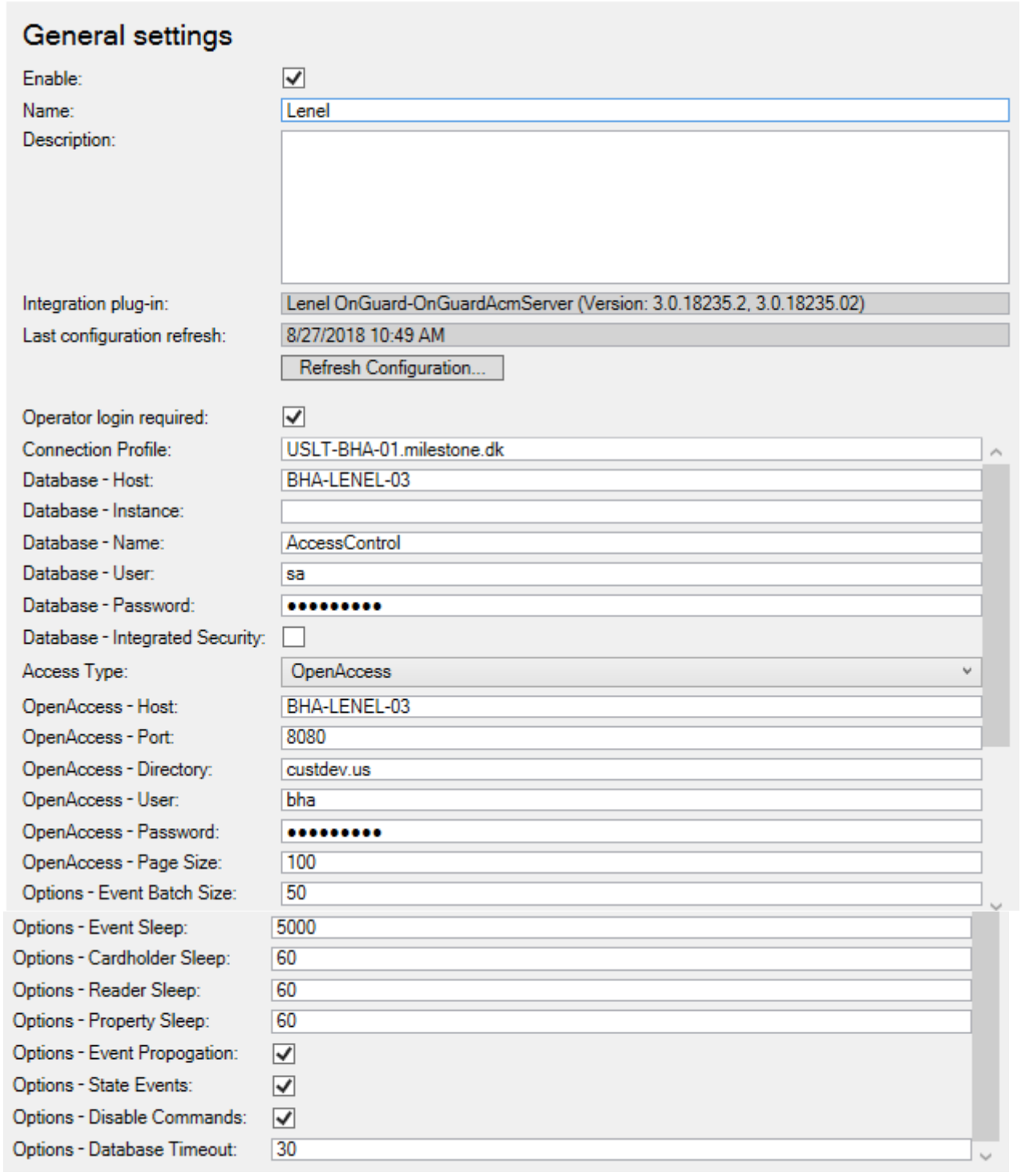


After selecting the plugin, you will have to provide credentials and parameters to configure the connection to the Lenel OnGuard database server, optimize particular settings, etc.

Some of these settings only apply depending on your type of access, DataConduIT or OpenAccess. However, all the properties used for all versions of Lenel OnGuard are shown in the Management Client wizard.



Properties



Below, the properties are listed by access type.

All Access Types

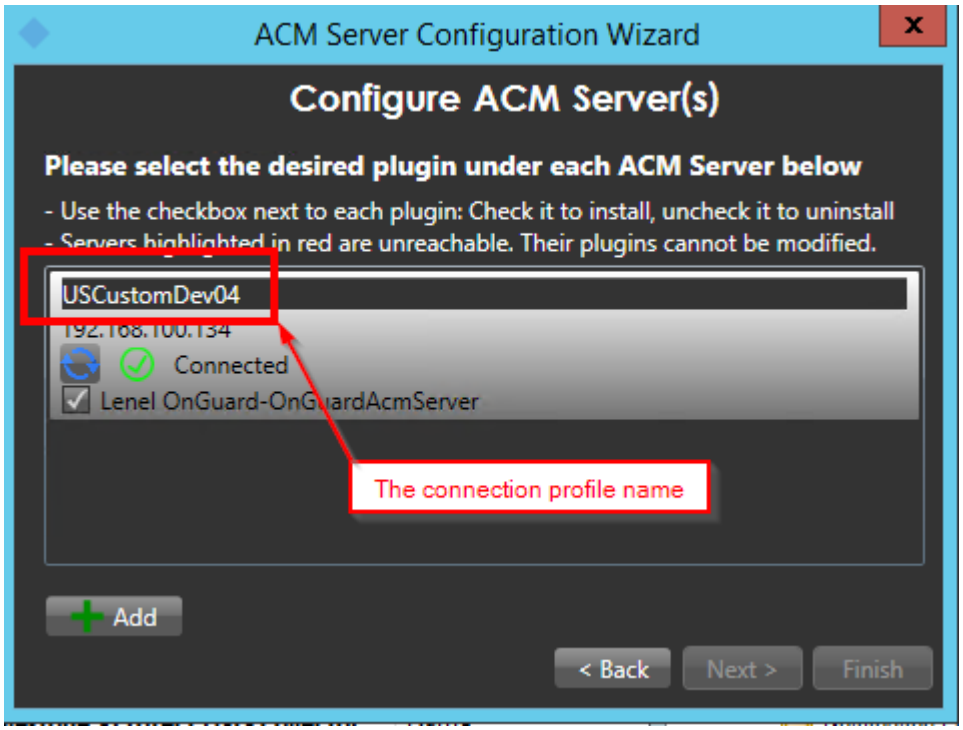
Connection Profile

Database - Host

Database - Instance

Database - Name
Database - User
Database - Password
Database – Integrated Security
Access Type
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:

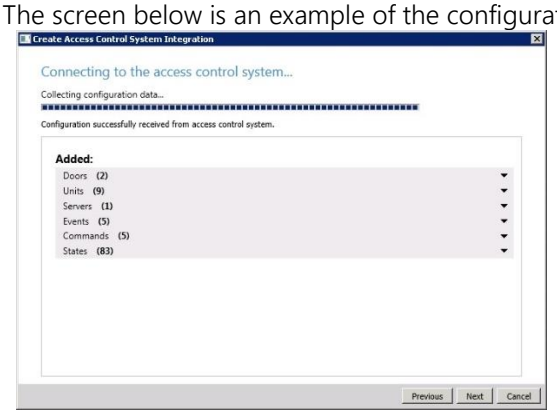


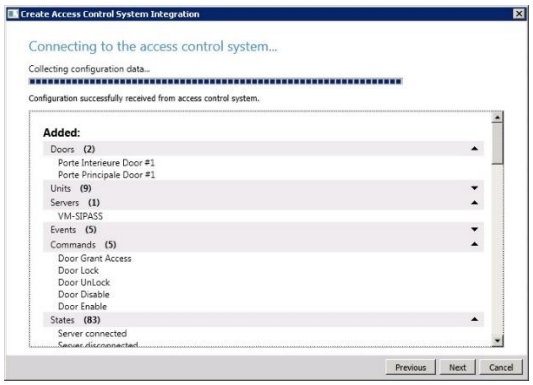
Database - Host – Name of the computer hosting the Lenel OnGuard SQL Server instance
Database - Instance – Name of the SQL Server instance hosting the Lenel OnGuard Access Control database. Leave blank to connect to the default SQL Server instance.
Database - Name – Name of the Lenel OnGuard Access Control database.
Database - User – User name to login to the Lenel OnGuard Access Control database.
Database - Password – Password to login to the Lenel OnGuard Access Control database.
Database – Integrated Security – Flag indicating if the Lenel OnGuard Access Control database uses integrated security. If false, the database user name and password is required.
Access Type – Defines the interface method used to access the Lenel OnGuard system.
Options – Cardholder Sleep – Defines how long the Lenel OnGuard plugin will sleep (in minutes) between fetching card holders from Lenel 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 Lenel OnGuard are not received or missed.
Options – Reader Sleep – Defines how long the Lenel OnGuard plugin will sleep (in minutes) between fetching door and reader information from Lenel OnGuard. Legitimate values are greater than zero. Lenel 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 Lenel 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 Lenel OnGuard event processing speed. For every hardware event received from Lenel OnGuard, the Lenel 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 Lenel 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.
Options – Database Timeout – Events are fetched from Lenel 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 Lenel 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 Lenel OnGuard EVENTS table to a reasonable amount. Lenel OnGuard provides the capability to archive events; contact Lenel OnGuard Support for help setting that up.
OpenAccess - Host – Name of the machine hosting the Lenel OnGuard OpenAccess service.
OpenAccess - Port – The port the Lenel OnGuard OpenAccess service is listening on.
OpenAccess – Page Size – The Lenel OnGuard OpenAccess service limits the number of instances returned for a given query. For example, multiple queries are required if the number of Lenel 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 Lenel OnGuard administrative user to use to log into the Lenel OnGuard OpenAccess web service. This user should have access to all hardware, cardholders, etc in the system.

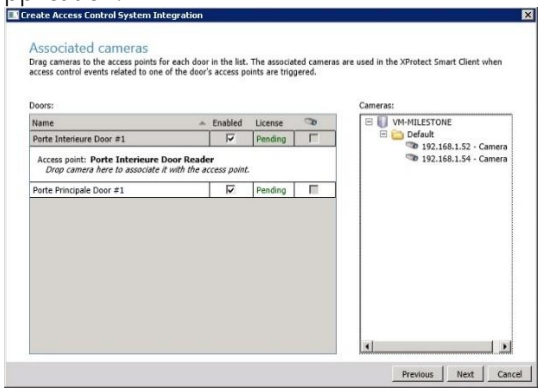
OpenAccess - Password – The password of an Lenel OnGuard user to use to log into the Lenel OnGuard OpenAccess web service.
OpenAccess - Directory – The name of the Lenel OnGuard directory to be used when loging into the Lenel Onguard OpenAccess web service. If left blank, the Lenel OnGuard internal directory will be used.

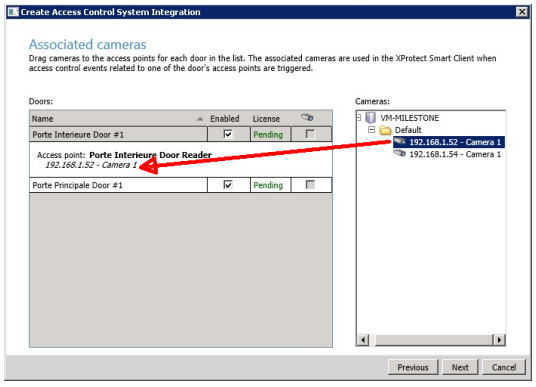
The wizard will now fetch the configuration of the Lenel OnGuard AC system into Milestone.
The screen below is an example of the configuration found on the server:



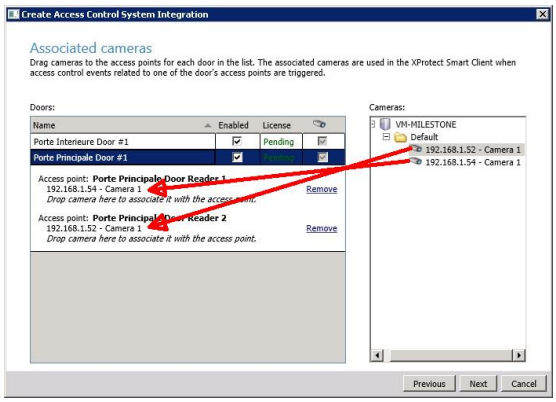


On this screen an association has to be created between each access point of a door and cameras in the Milestone system. This is done so that the system will know which cameras to display on door alarms. For each access point of each door drag a camera from the right tree and place it under the desired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

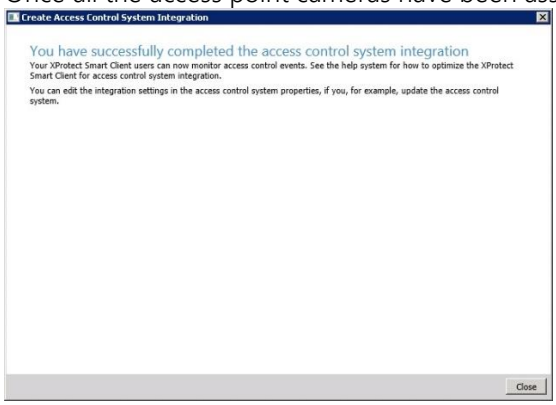




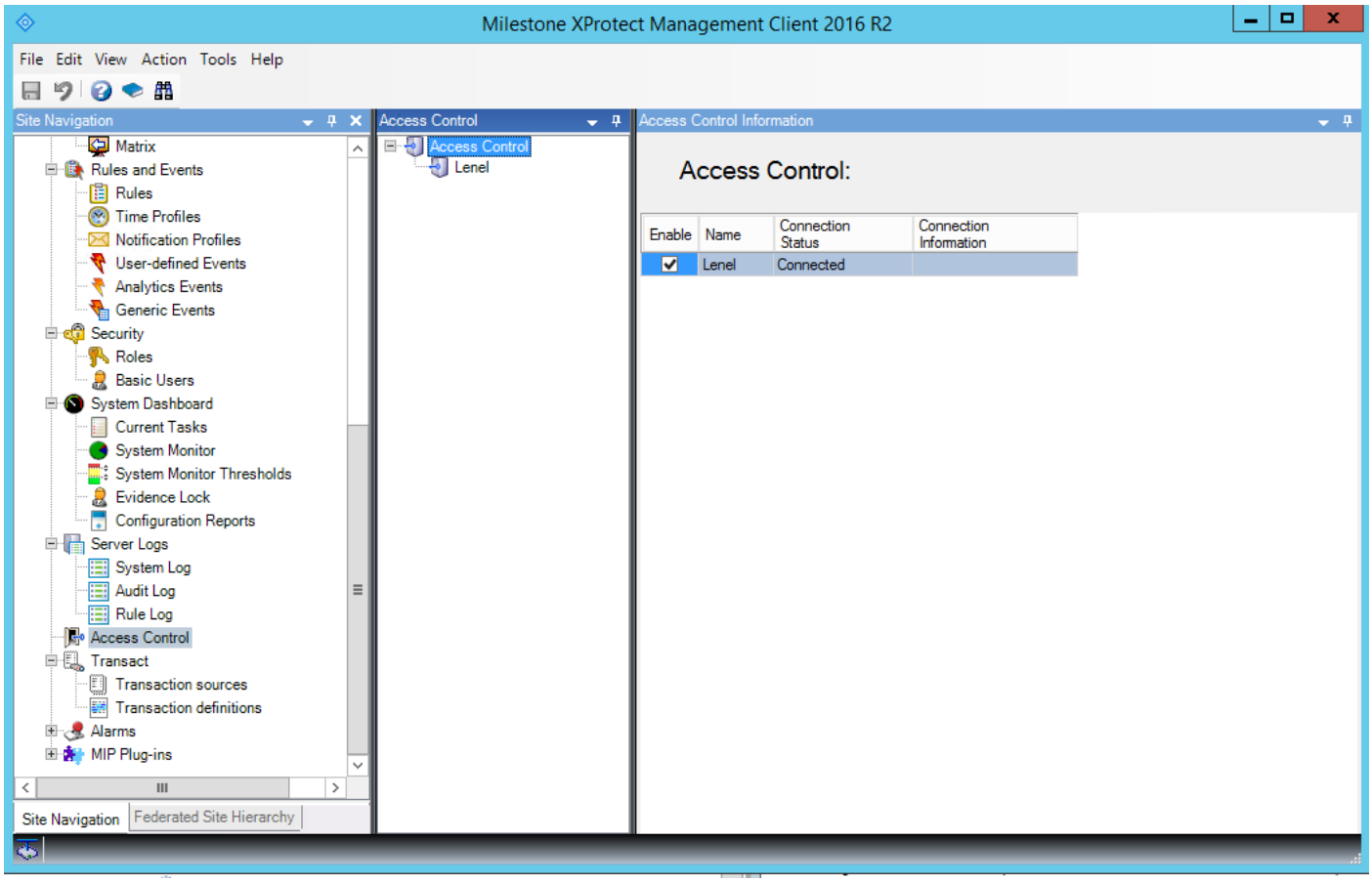
When there is more than one access point per door, you can select the different cameras for the different angles. You can also select more than one camera per access point:



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 DbName and DbUserName fields defined the credentials the Lenel OnGuard ACM integration uses for read-only access to the Lenel 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 Lenel OnGuard ACM integration, this section assumes you know how to perform the required steps in Sql Server to create/modify a login.

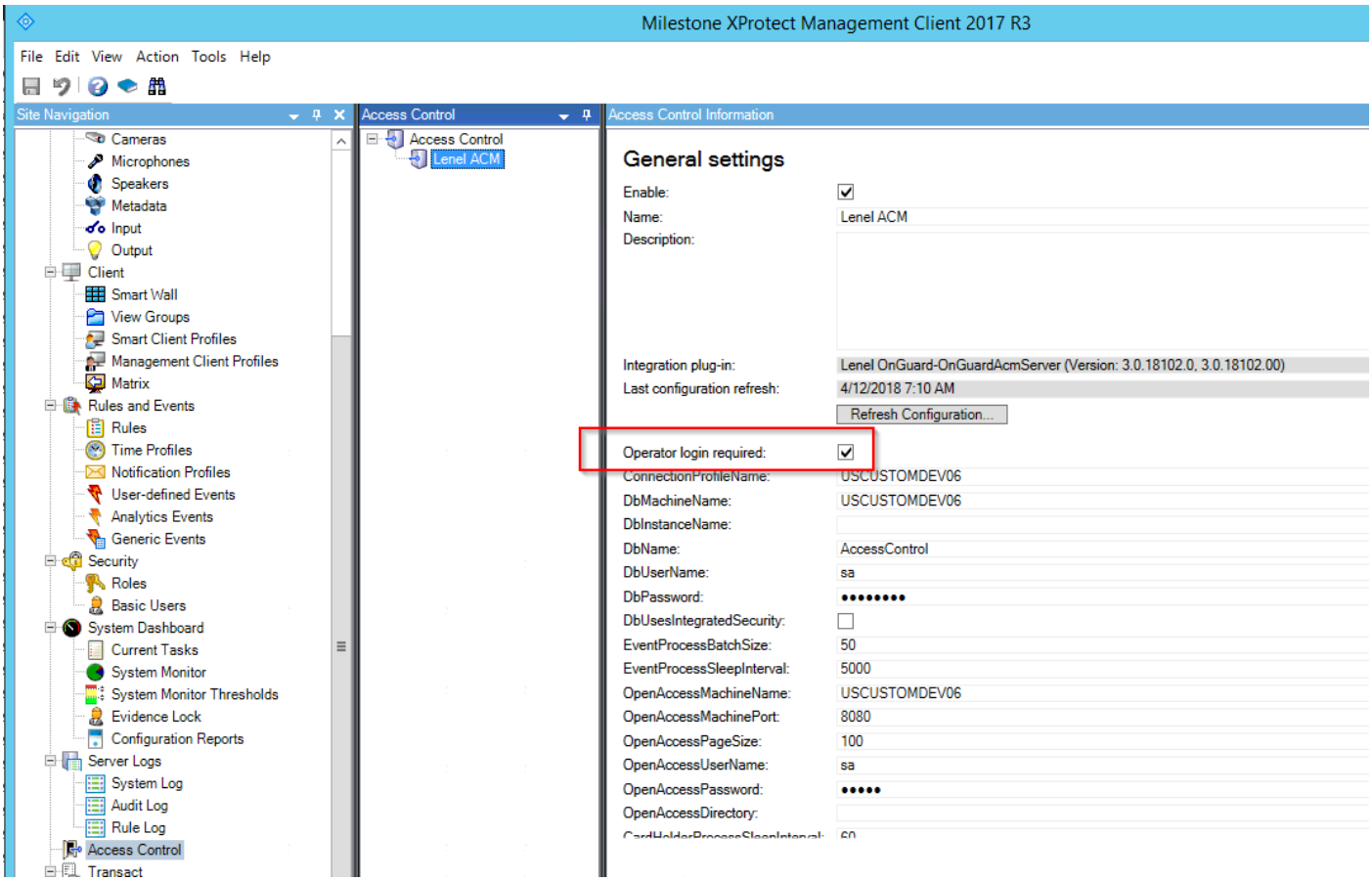
We've tested the Lenel OnGuard ACM integration with the following minimal database permissions:

- Has only the "public" server role.
- User mapping to only the Lenel 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 Lenel OnGuard ACM plugin does support it only when running on Lenel OnGuard 7.4 or greater since the Lenel 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:

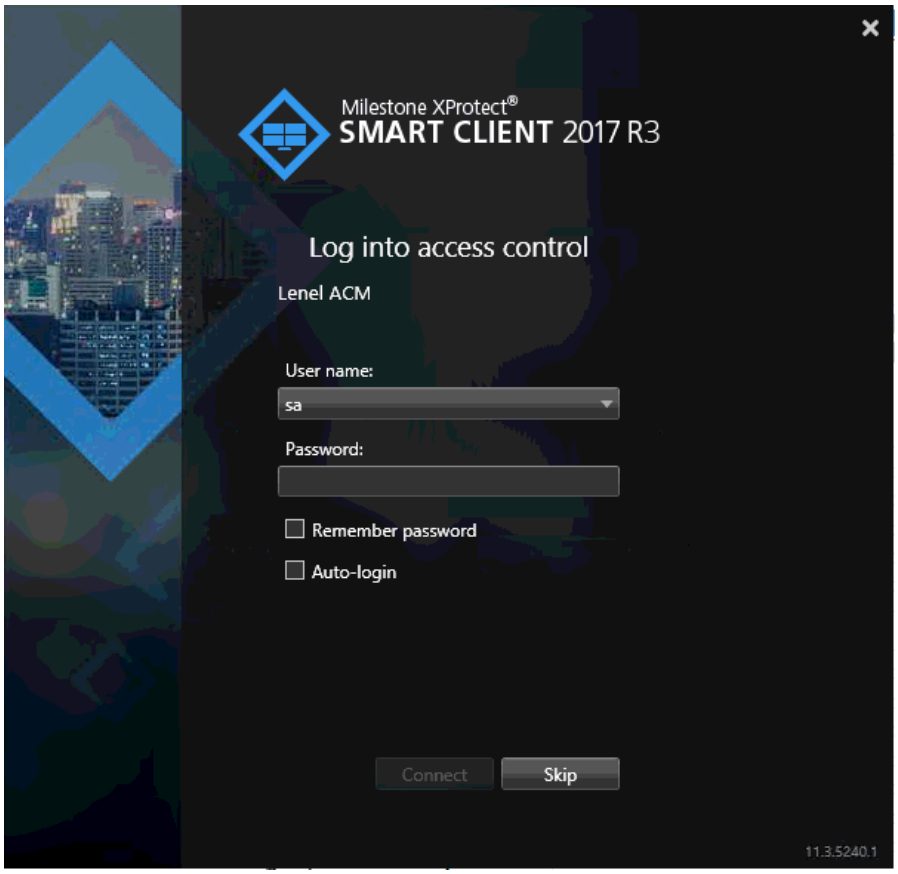


Smart Client Personalized Login

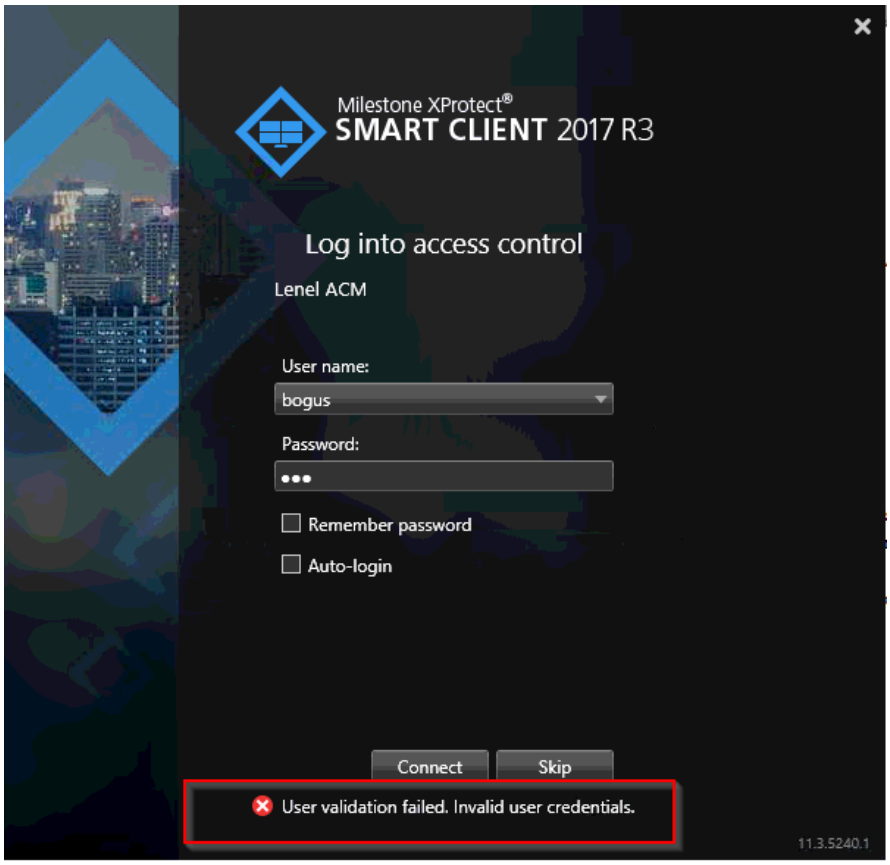
If personalized login is enabled for any access control instance configured in the Management Client, the Smart Client will request user credentials for each of those access control instances. This is done after the standard Smart Client login screen.

For manual sign-on, Lenel 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 Lenel OnGuard "internal" directory will be used.

Be aware that the Lenel 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

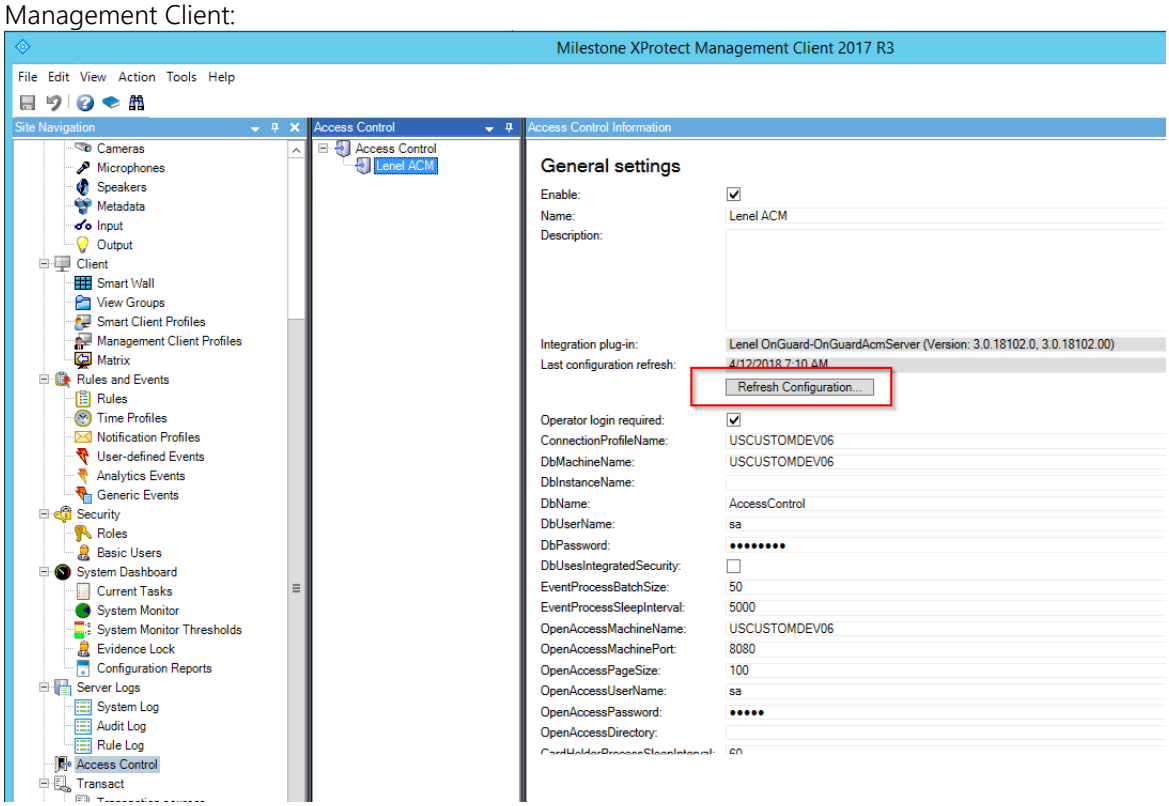
The Smart Client will not show any entities that are not in (or related to entities in) the personalized configuration. For example, a personalized user will only see:

- 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.

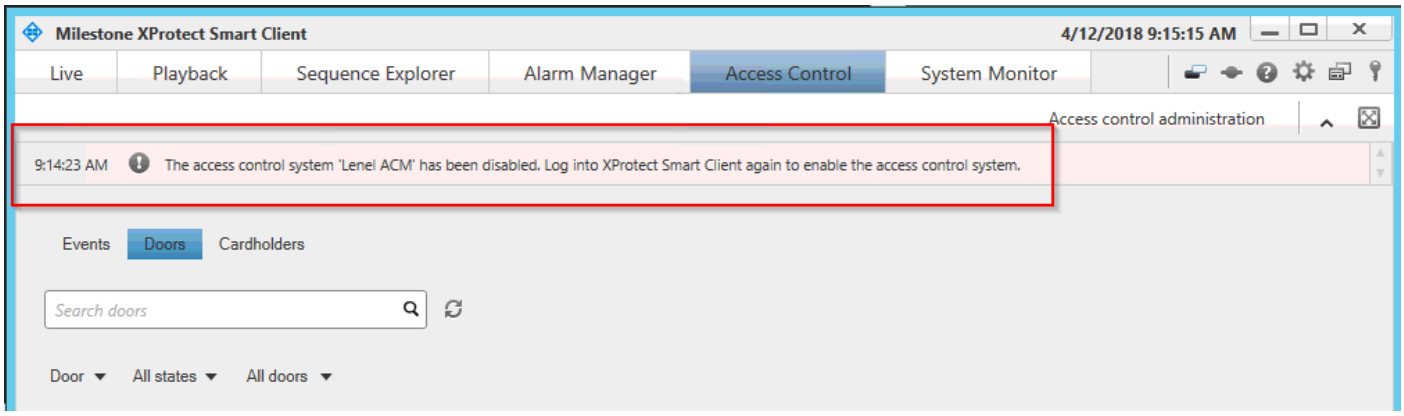
XProtect Personalized Login doesn't specifically include personalized alarm acknowledgment. Rather, as with non-personalized login, any user can acknowledge any alarm that is visible in the Smart Client. Since alarms

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.
Lenel 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 Lenel OnGuard Event Types

The Lenel OnGuard event types are originally read from the Lenel 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 Lenel 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_fcnoentrymade,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 Lenel 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.

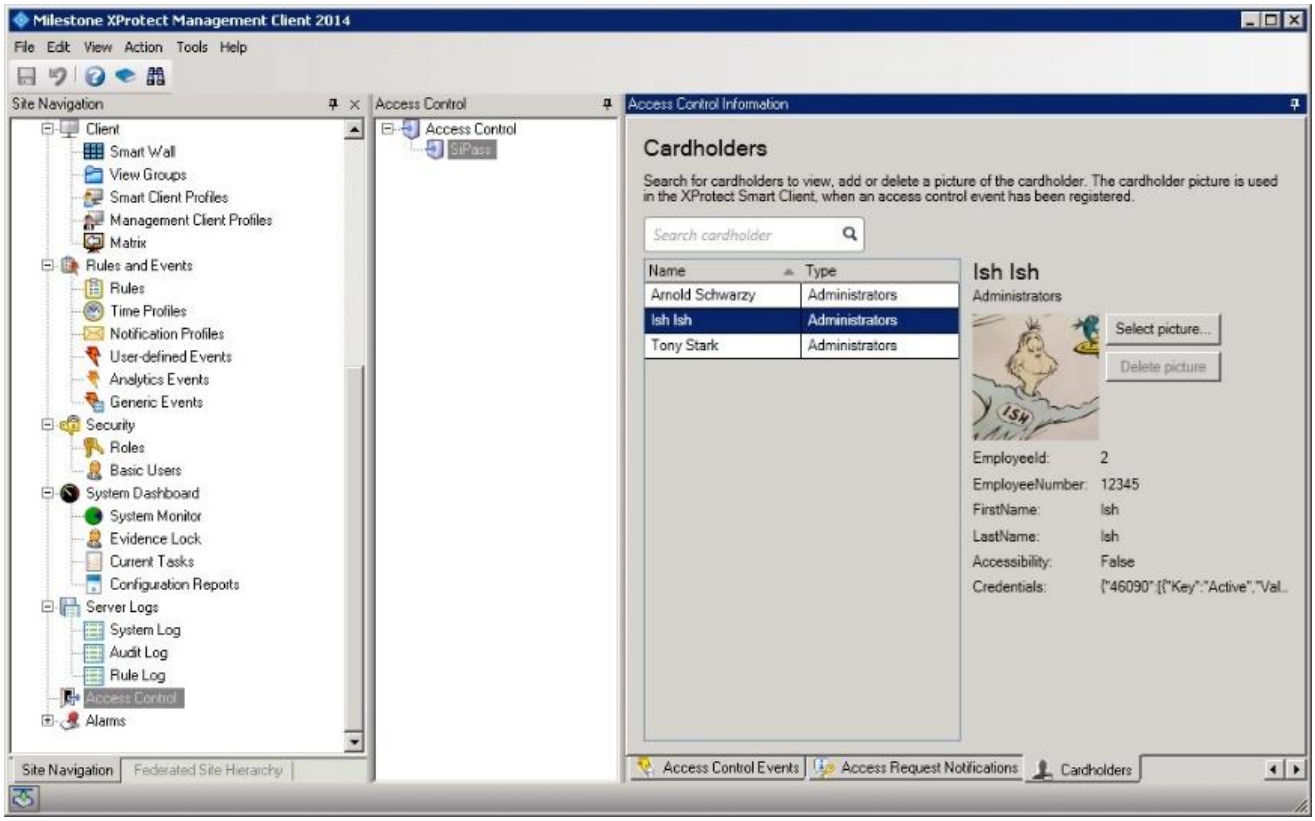
After making and saving changes to the event type file, the administrator should do the following:

1. On the Lenel 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 Lenel 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.

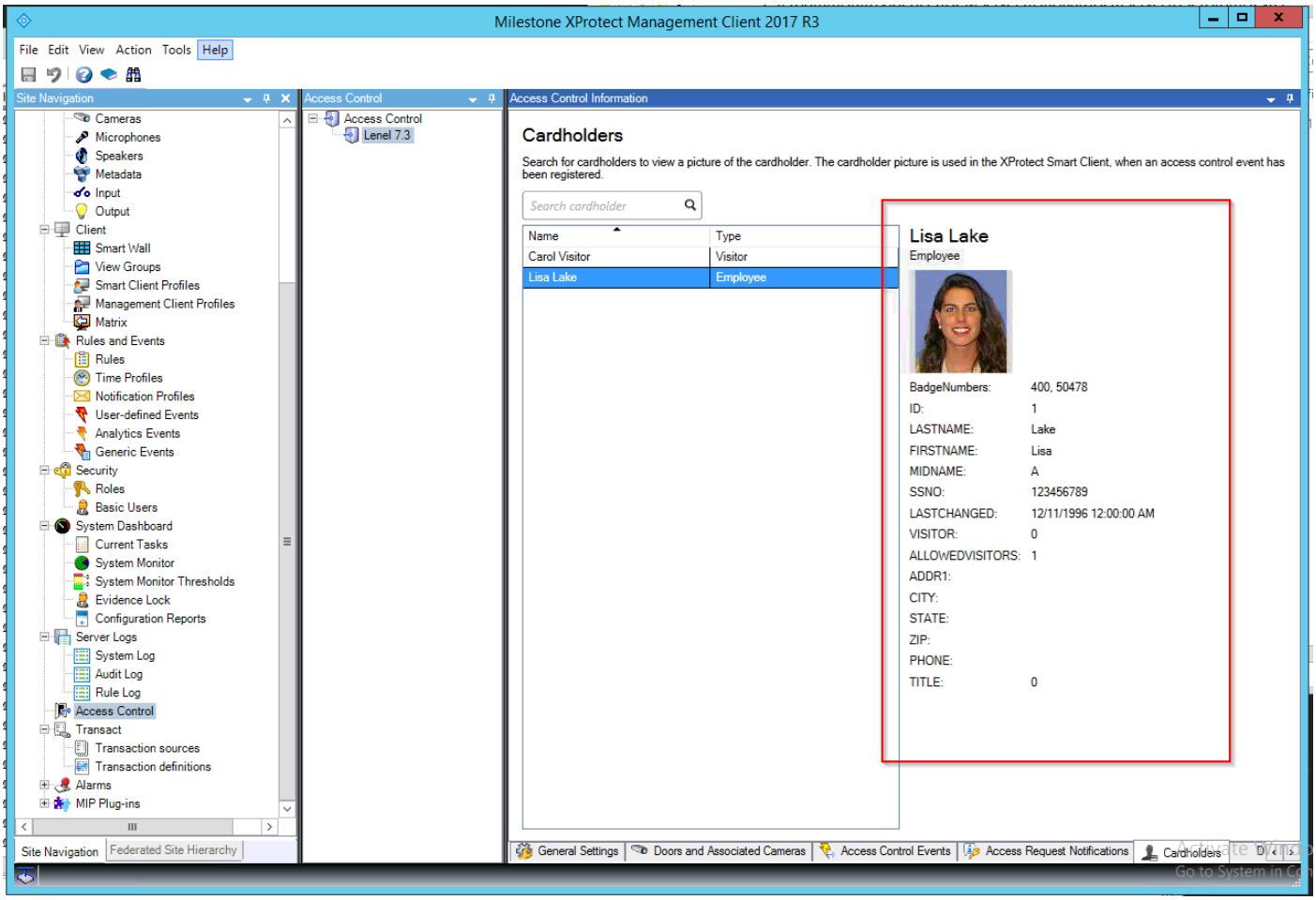
The user can search for existing cardholders in the Lenel OnGuard system through the management client interface:



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.



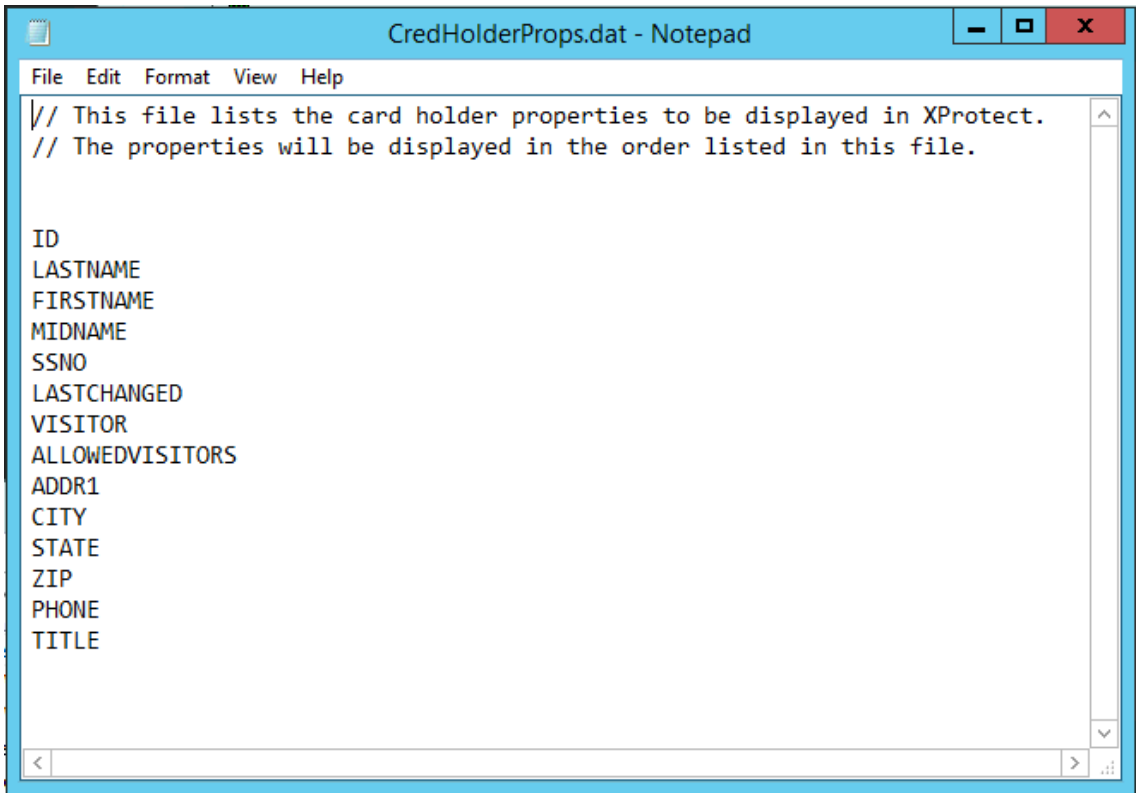
Lenel OnGuard allows customization of the Cardholder UI in their System Administration application. It's easy for a customer to define enough custom fields to extend beyond the visible region shown above for the XProtect Management Client.

The Lenel 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 Lenel 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.

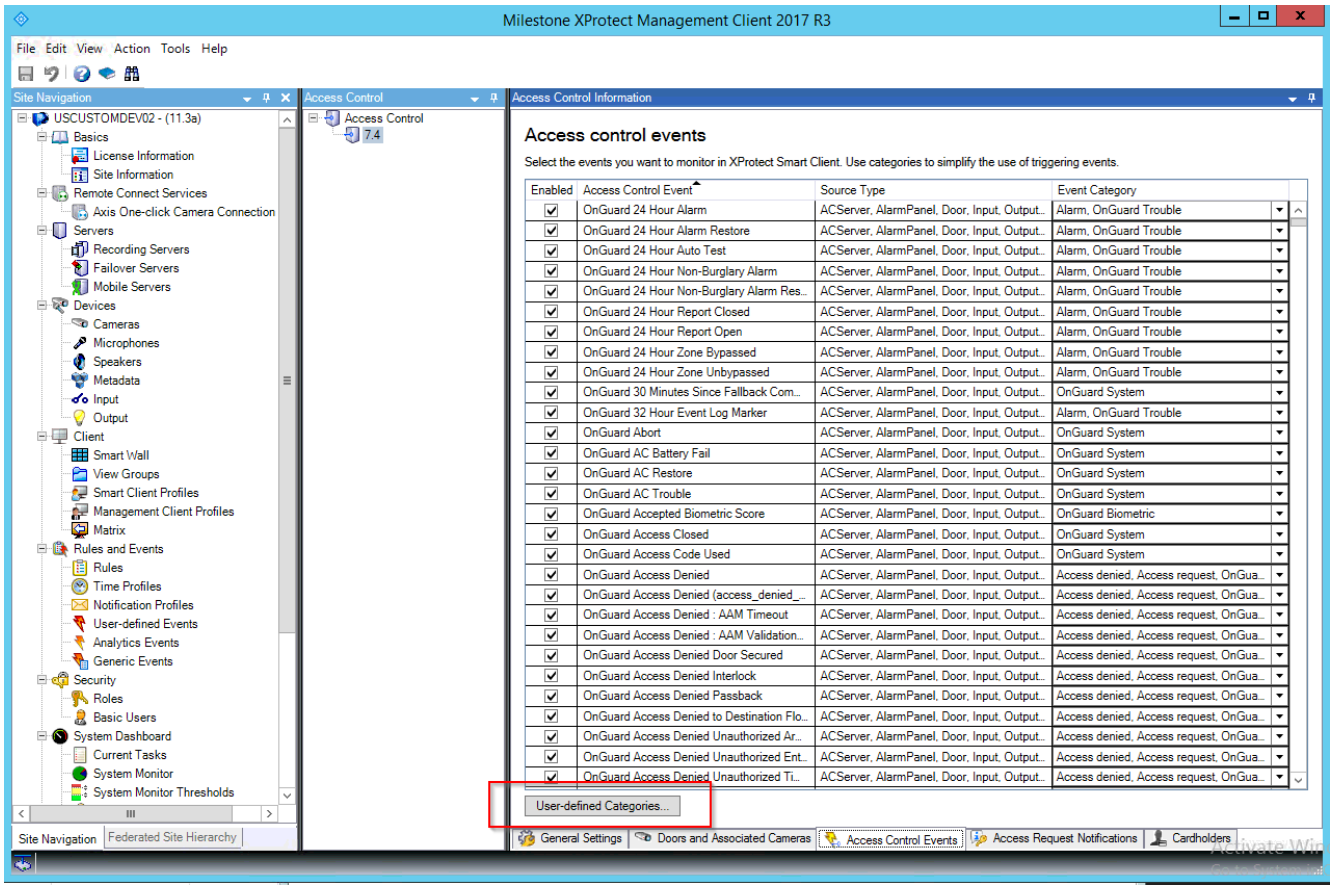
Note that the cardholder's badge numbers are always displayed as the first property.

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.

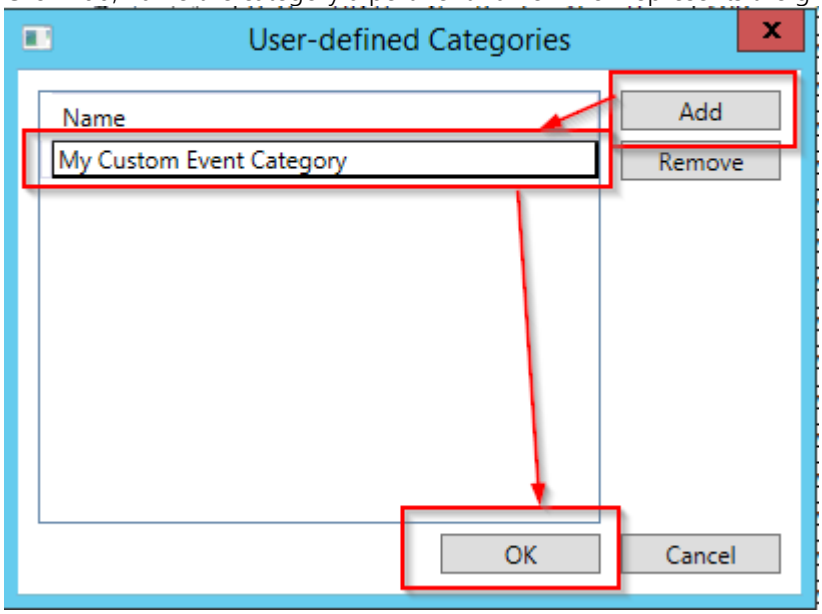


Defining alarms based on Lenel OnGuard events

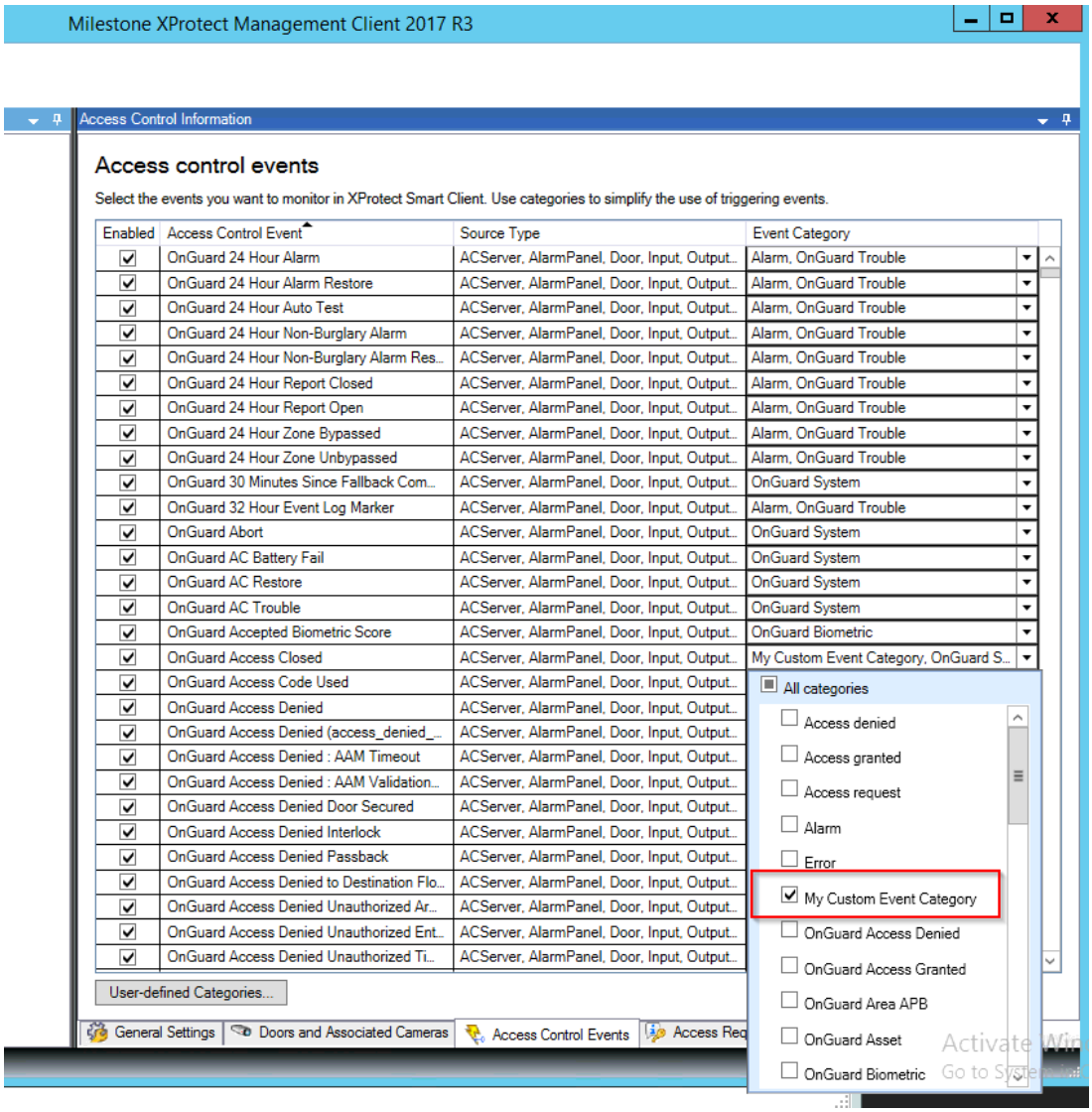
To define alarms based on Lenel OnGuard events, the events must be part of an event category. The category can be one of the pre-defined Access Control Event categories such as (Access Granted, Access Request, Access Denied, Alarm, Error, and Warning) or a user-defined category. Here is how to create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



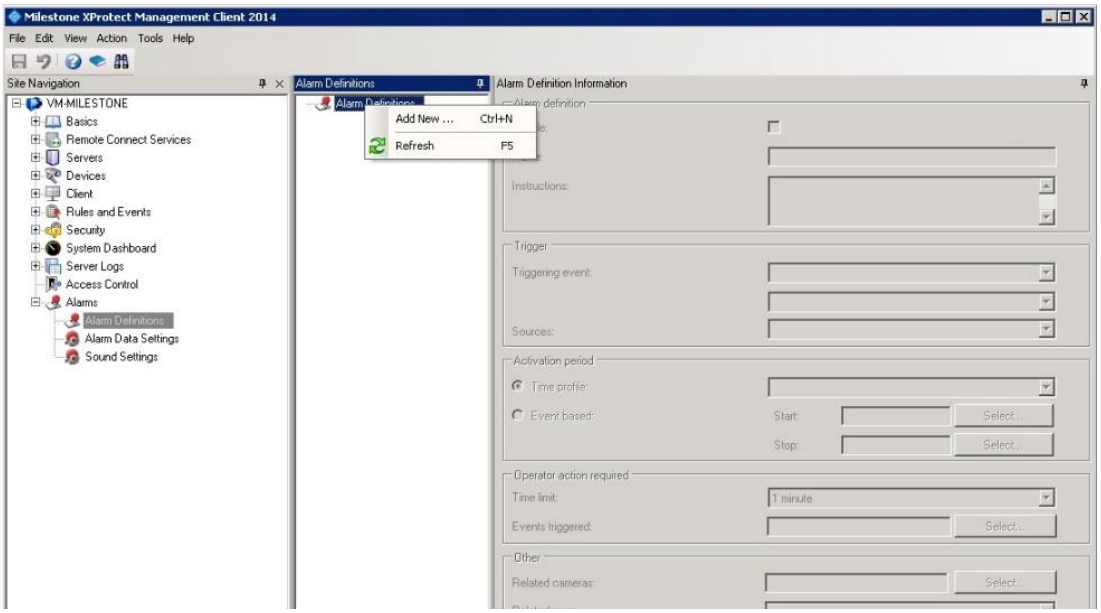
Click Add, name the category a pertinent name which represents the group of events, and press OK.



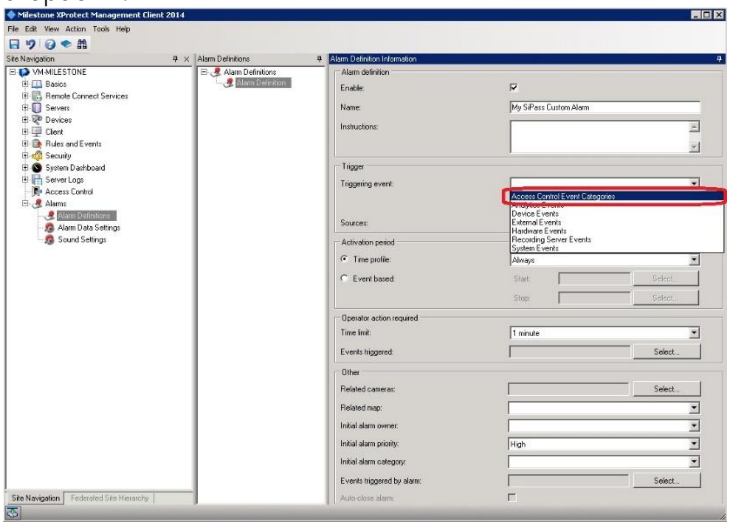
Associate the category with one of the Lenel OnGuard AC events:



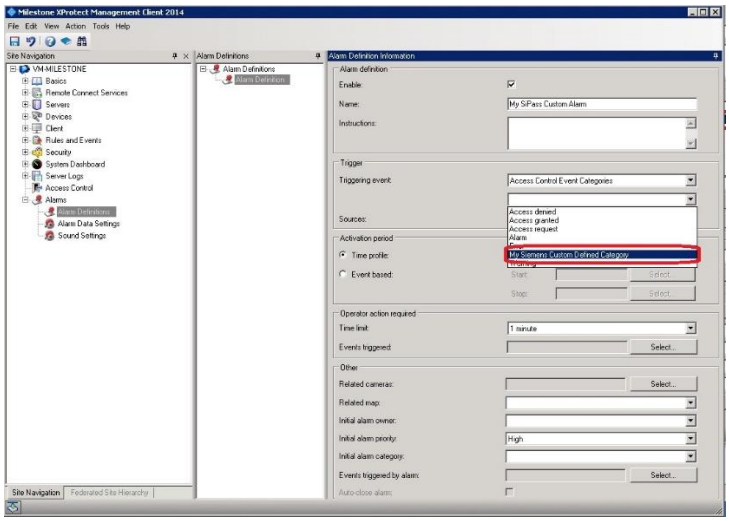
Save your changes and move to the Alarm Definitions section to create an alarm based on that user-defined event category.



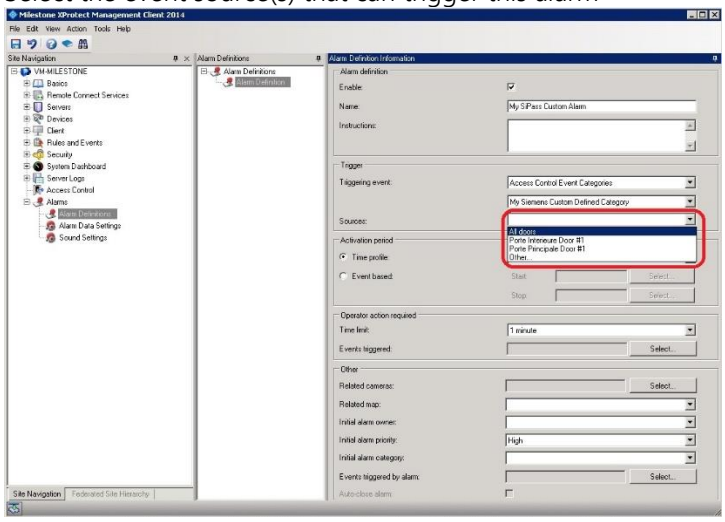
Name the alarm a pertinent name and select Access Control Event Categories in the Triggering event dropdown:



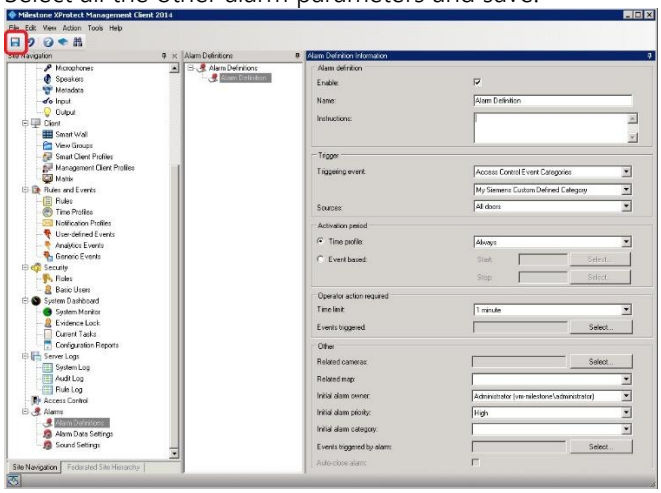
Select the new user-defined event category that was defined earlier:



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



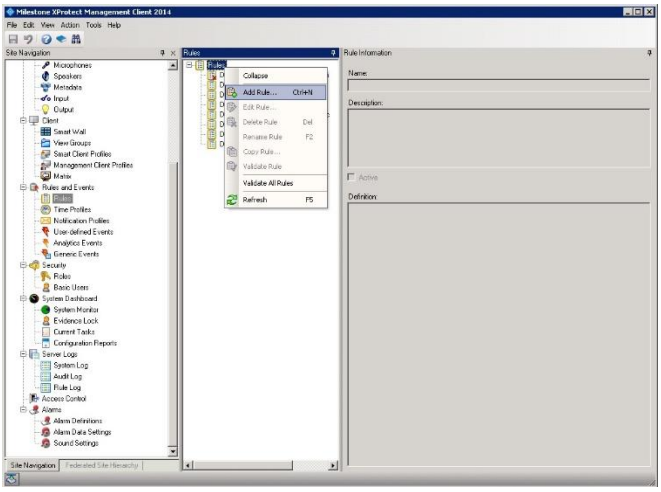
Select all the other alarm parameters and save:



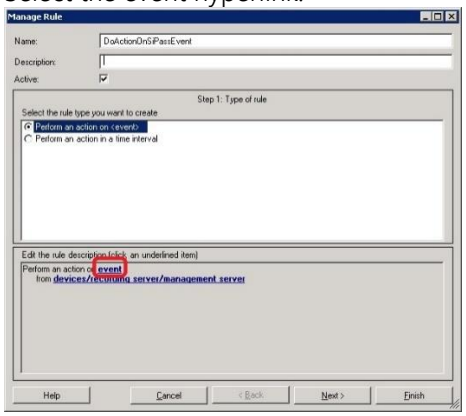
Alarms acknowledged in Milestone are acknowledged in Lenel OnGuard.

Defining rules based on Lenel OnGuard events

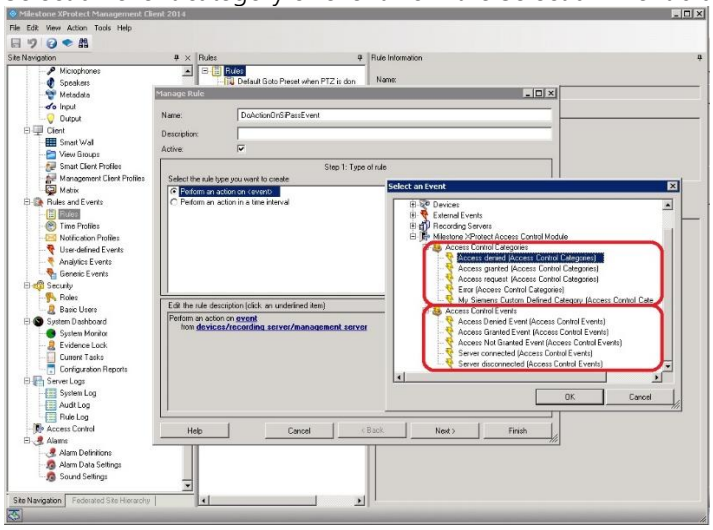
To define rules in Milestone based on Lenel OnGuard events, create a rule in the Rules tab:



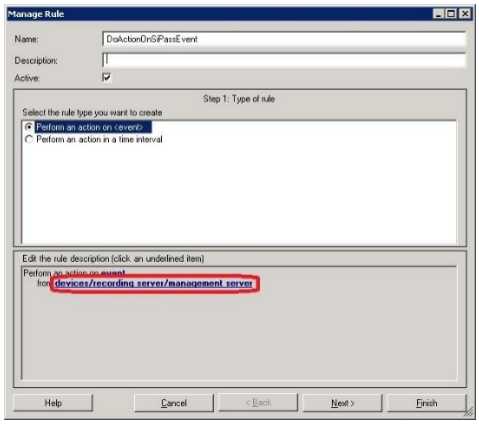
Select the event hyperlink:

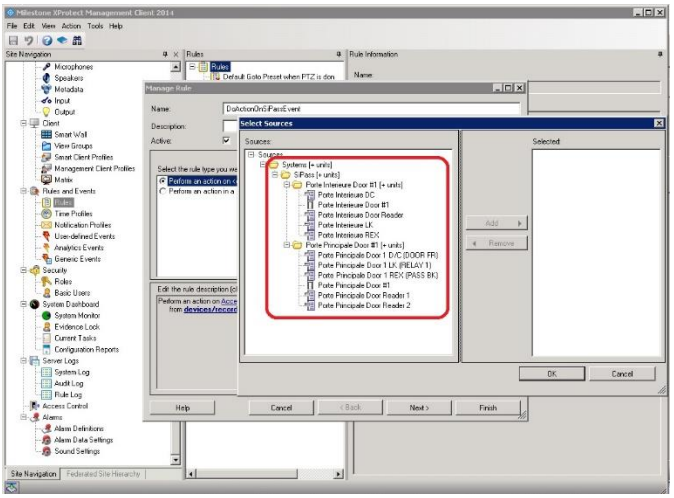


Select an event category or event from the Select an Event dialog:

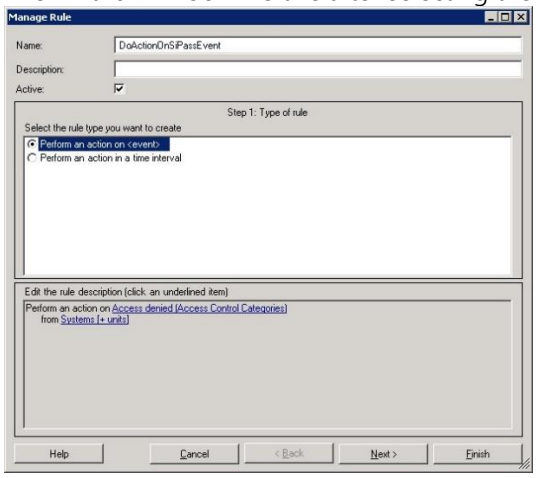


Select the devices/recording server/management server hyperlink and select the event source. To select any source select the System (+units) node.

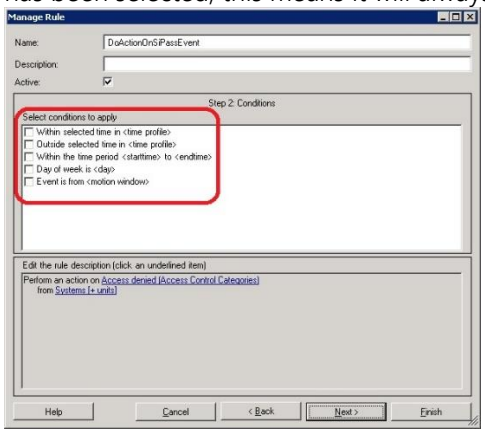




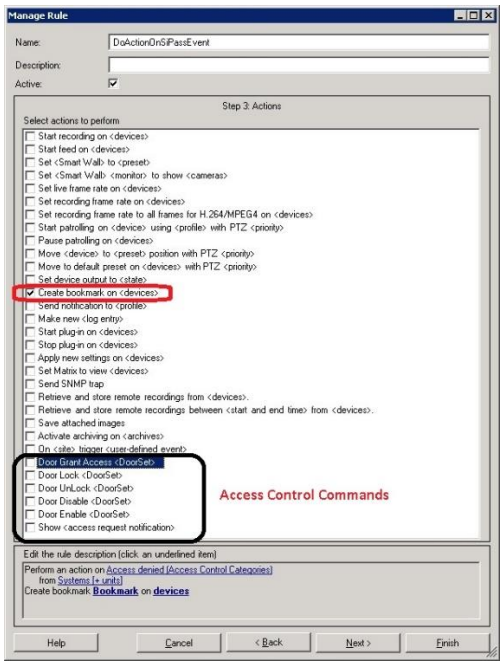
The wizard will look like this after selecting the "Access Denied" event and System (+ units) source:



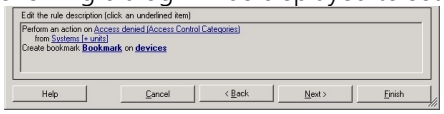
Press next and select the optional time frame when the action will take place. In this example no time frame has been selected, this means it will always execute.

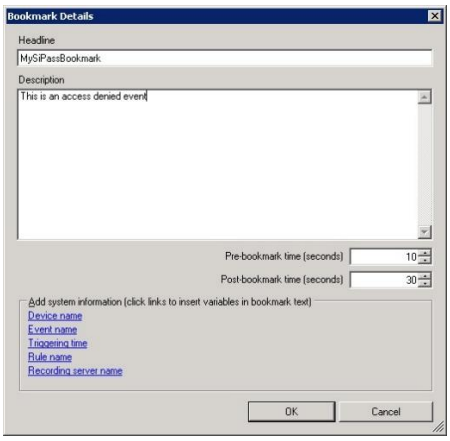


Select the action that will be executed when the Lenel OnGuard event occurs. Notice that AC commands can be used as actions based on any events that come into Milestone:

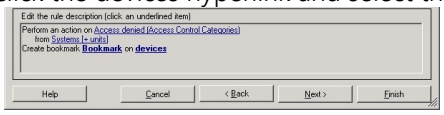


In this example "create bookmark on <device>" will be selected, click the Bookmark hyperlink and the following dialog will be displayed to setup the bookmark action:

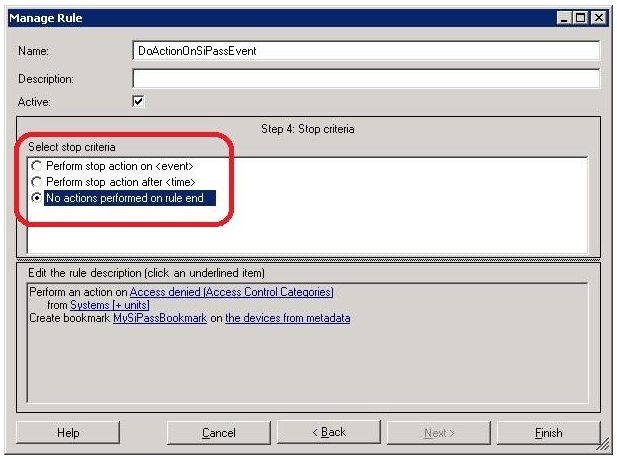




Click the devices hyperlink and select the device on which the bookmark will be applied:



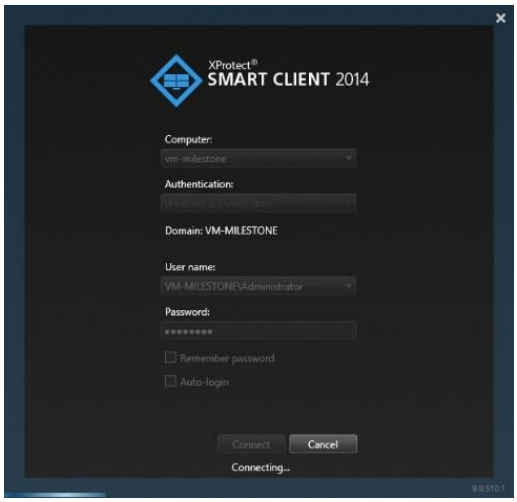
Click next on the rule wizard and select an optional stop criteria, in this example there is no stop criteria.

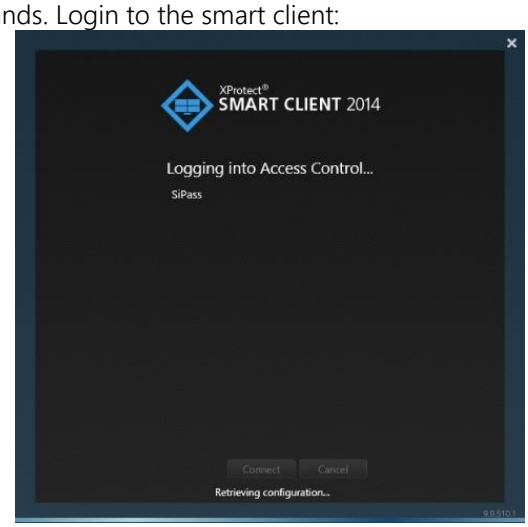


Click finish and the rule is set.

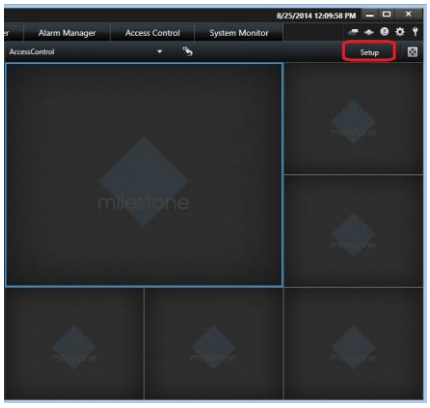
XProtect® Smart Client Maps

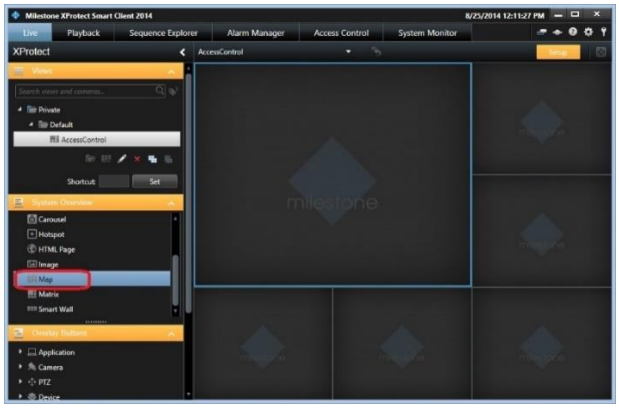
It is possible to put doors and Lenel OnGuard server(s) on an existing Smart Client Map to display door and server status as well as execute manual commands. Login to the smart client:



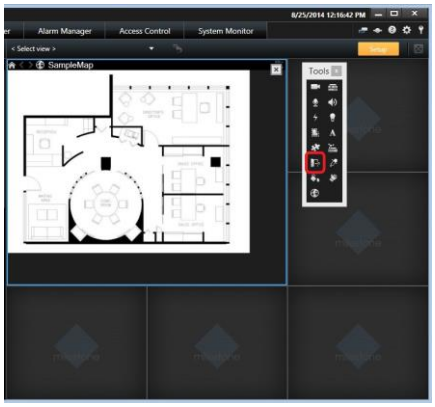


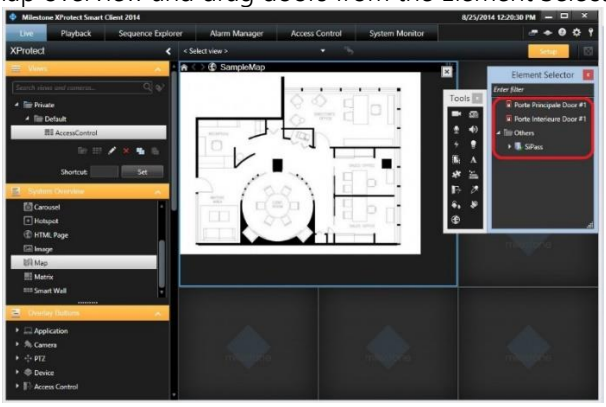
Use an existing view, go into setup mode by pressing the setup button in red below and create a map by dragging it onto a tile once in setup mode.



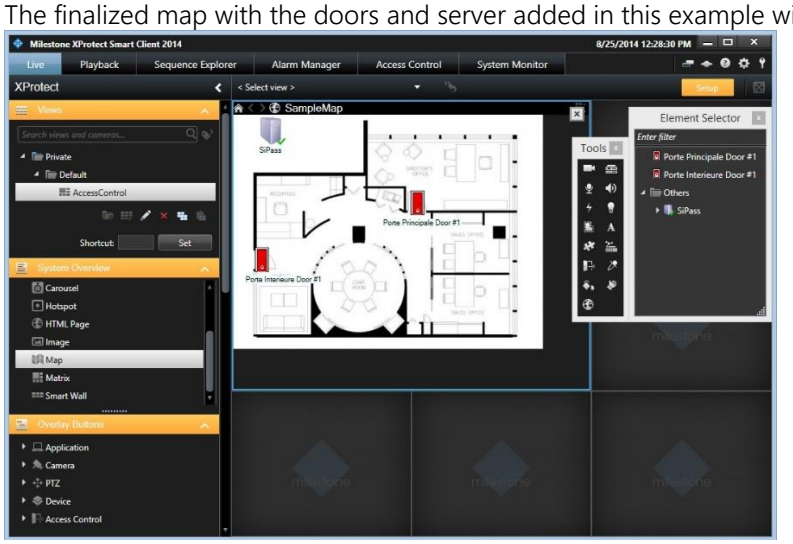


Select the access control button on the map overview and drag doors from the Element Selector to the map



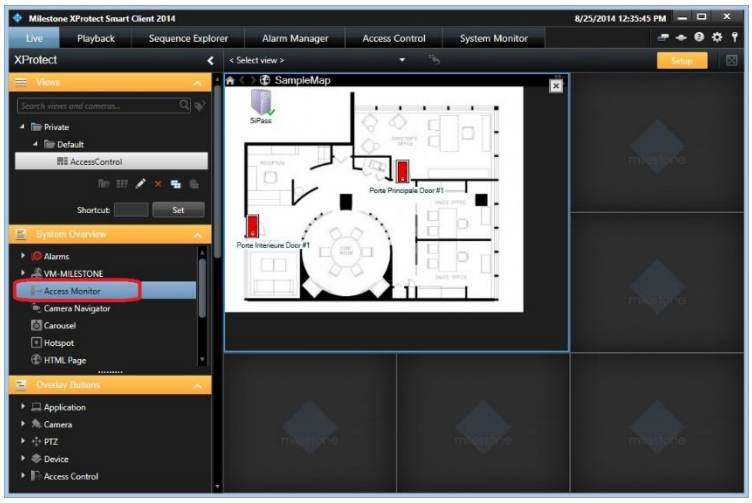


The finalized map with the doors and server added in this example will look like this:



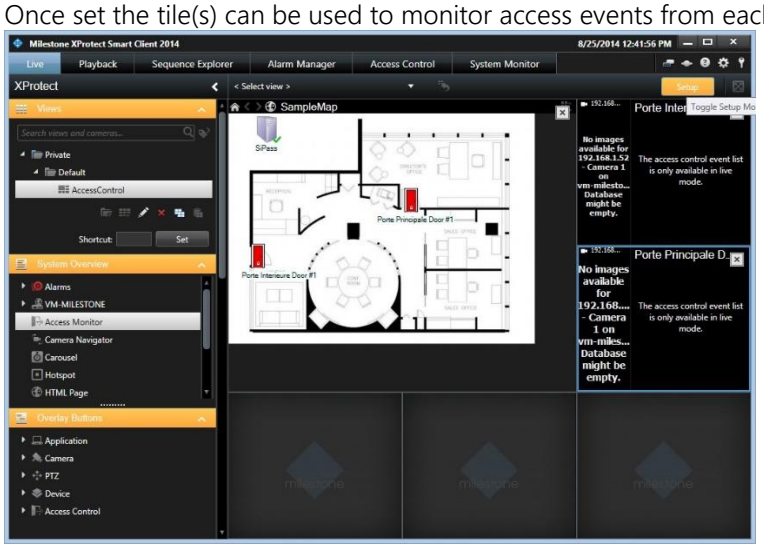
XProtect® Access Monitor tiles

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:

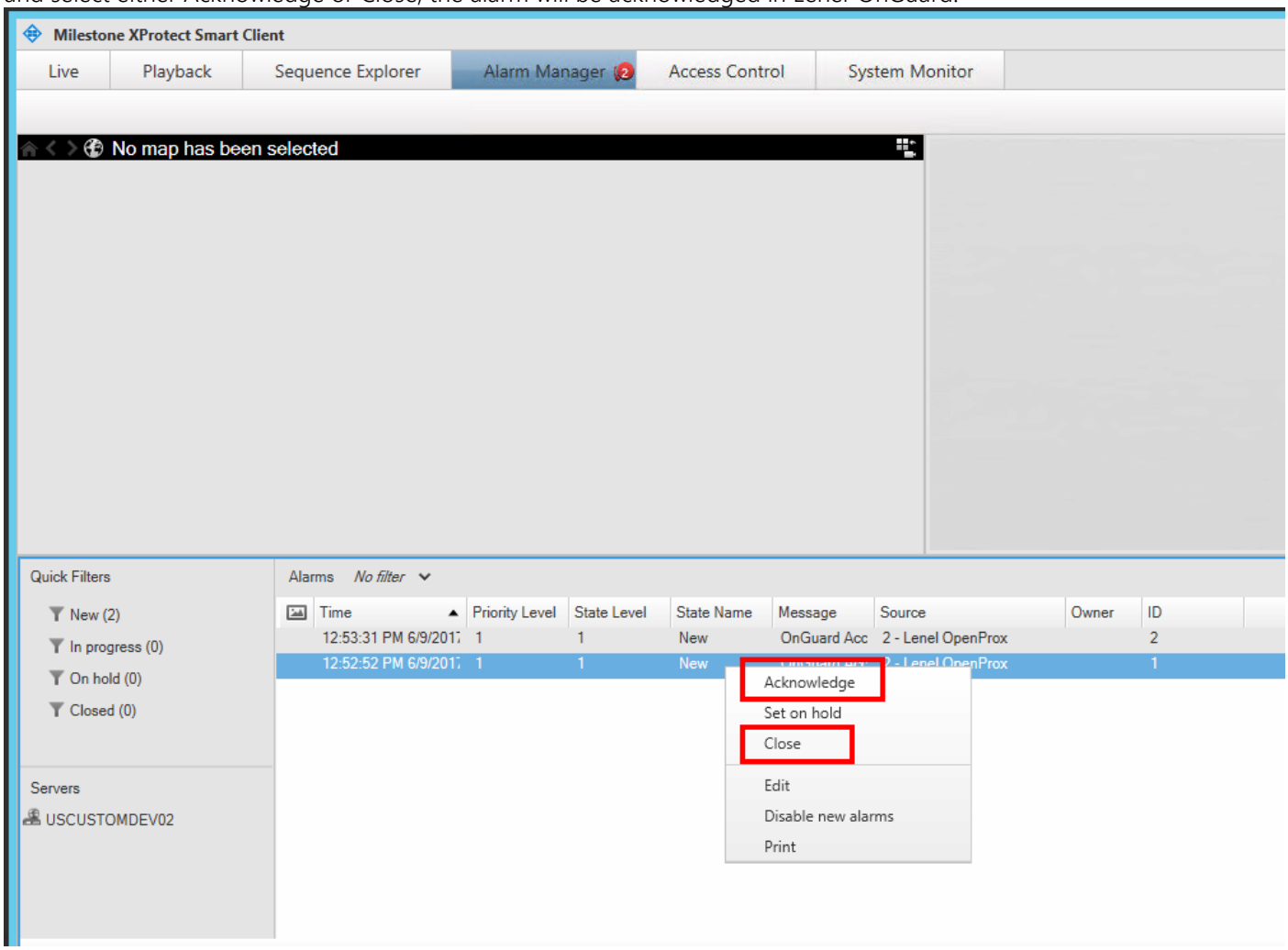
Once set the tile(s) can be used to monitor access events from each door configured above:



Alarm Acknowledgment

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

Alarm acknowledgment from Lenel OnGuard to XProtect is not implemented due to the lack of such functionality in Lenel OnGuard.
Alarm acknowledgment is done in the XProtect Smart Client's Alarm Manager tab. If you right-click an alarm, and select either Acknowledge or Close, the alarm will be acknowledged in Lenel OnGuard.



NOTE – As mentioned above, selecting either Acknowledge or Close will cause the alarm to be acknowledged in Lenel OnGuard and removed from Lenel OnGuard's active alarm list. But, selecting Acknowledge above does not remove the alarm from XProtect's Alarm Manager list. XProtect considers acknowledgment and closing the alarm to be different steps. The result of all this is that, if you first acknowledge and then close the alarm in XProtect, you will see an error in the debug log about failure to acknowledge the alarm in Lenel OnGuard. The reason is simple – the alarm was removed from Lenel OnGuard's active alarm list when you did the acknowledgment; therefore it didn't exist when you did the close. This does not cause problems; just noise in the debug logs.

Fetching Lenel OnGuard event types

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

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

This application must be run on the Lenel OnGuard machine where the Lenel 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, Lenel 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 Lenel 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 Lenel 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. Restart the Milestone ACM Server. Then, restart the Milestone Event Server for the changes to take effect.

Logging

By default the debug logs are enabled on both the milestone event server plugin and the Lenel 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

Lenel OnGuard Server side

5. On the machine running the Lenel OnGuard server go to X:\ProgramData\VideoOS\Service-Host\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 Lenel OnGuard server go to X:\ProgramData\VideoOS\Service-Host\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 MilestoneACMServerServ-iceLogs.zip
9. On the machine running the Lenel OnGuard server go to: X:\ProgramData\VideoOS\Service-Host\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\logs
10. Create a zip file of the contents of that whole folder and name it LenelOnGuardAcmServer-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.

Lenel OnGuard Server side

1. On the Lenel 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 Lenel 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

Lenel OnGuard loses communication with the access control hardware

Communication can be lost for the following reasons:

1) Firewall blocking the traffic
2) The Lenel OnGuard LS Communication Server service is not running (or needs to be restarted).
3) The Lenel 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 Lenel 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 Lenel OnGuard Directory that is configured for single sign-on. See Configure Lenel OnGuard for Single Sign-On and ACM Server: Configure to RunAs Lenel OnGuard Single-Sign-on Account above for details.

If the ACM Server is not running in the required security context, the Lenel 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 Lenel OnGuard ACM plugin about every 5 seconds. At a log level setting of Trace, you'll see lines like the following in the Lenel 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 Lenel 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

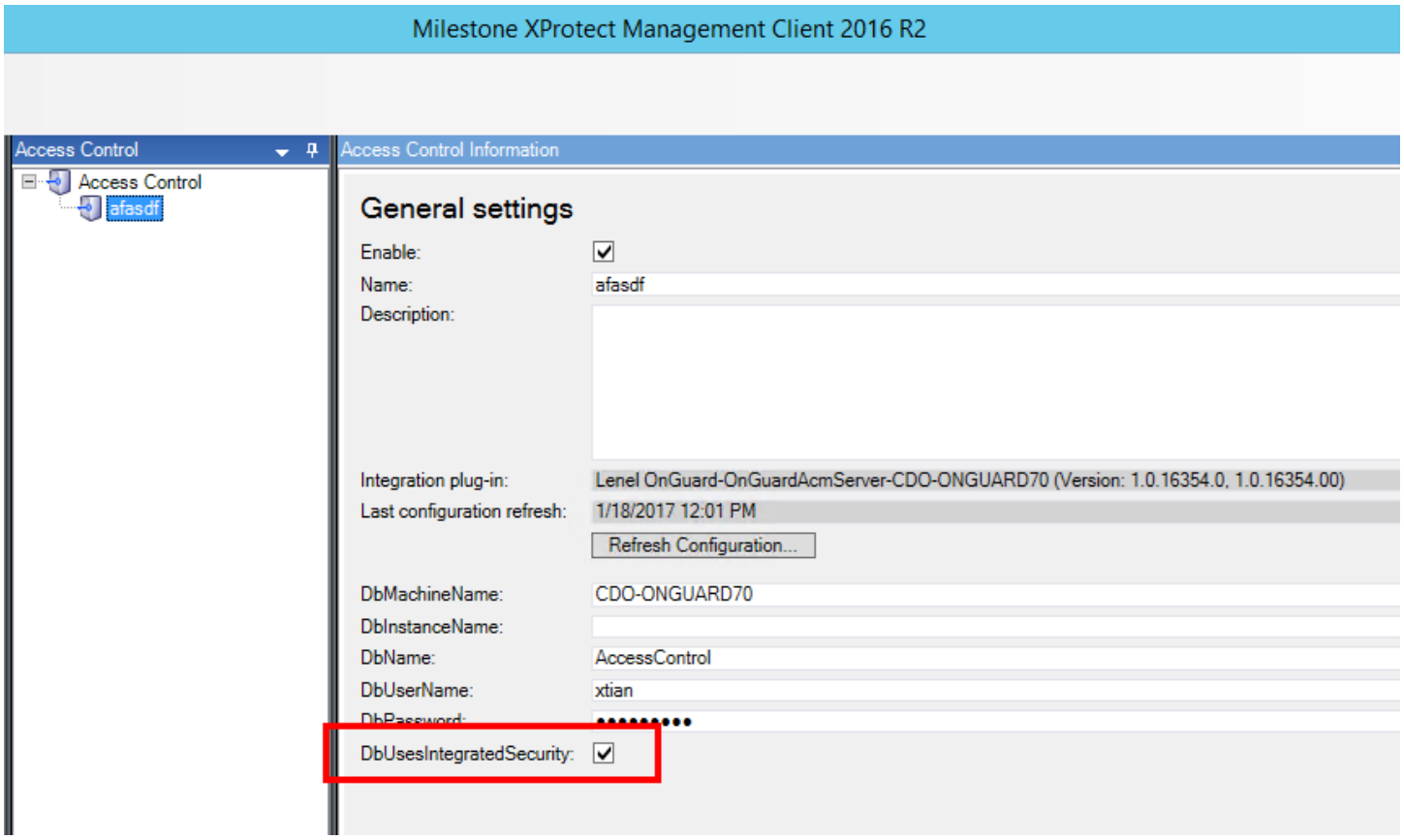
If the debug log shows an error similar to:

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 Lenel 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 Lenel 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 Lenel 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 Lenel 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 Lenel 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 Lenel OnGuard will be processed. But the system will not even attempt to create state change events related to the Lenel OnGuard events.

No matter what settings you adjust, all raw events received from Lenel OnGuard get sent to XProtect.
If DoProcessStateChanges is enabled, for every raw event received from Lenel OnGuard, the Lenel 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 Lenel 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 Lenel 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)

Use the LenelEventCntr.exe utility included in the distributed zip file to count events processed and provide some metrics (e.g. events per second, etc).

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 Lenel OnGuard.

The Lenel OnGuard ACM integration downloads cardholders from Lenel 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 Lenel OnGuard ACM log files, they're typically due to the Lenel 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 Lenel OnGuard SSO user to the built-in "System Account" user. This built-in user has all possible permissions within Lenel OnGuard.

Steps:

1. Log into Lenel OnGuard's System Administration application as the Lenel 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 Lenel OnGuard ACM logs to see if the errors went away.

Lenel OnGuard OpenAccess connectivity

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

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

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

The Lenel 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.

Lenel OnGuard ACM integration flooding user transaction report

Milestone's XProtect system requests the current states of Lenel OnGuard hardware at various times throughout the life of the application. As prescribed by the Lenel 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 Lenel OnGuard for the single sign-on (SSO) user. Per Lenel OnGuard, there is nothing the Lenel OnGuard ACM integration can do to prevent these transactions from being entered into Lenel OnGuard.

Customers making use of Lenel OnGuard's built-in "User Transaction" report from Lenel OnGuard's Sys Admin + Reports will see these *many* transactions from the Lenel OnGuard ACM integration under the SSO user in the report. Because there's so many of these transactions, some customers feel that the Lenel OnGuard ACM integration makes this report useless. Per Lenel 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, Lenel OnGuard Technical Support, OAAP, etc will not support these custom reports.

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

Lenel OnGuard ACM instance is not displayed in the XProtect® Management Client

If XProtect is unable to communicate with the Lenel 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 Lenel OnGuard is running successfully. This may require restarting the DataConduIT or OpenAccess 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 Lenel 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 Lenel 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

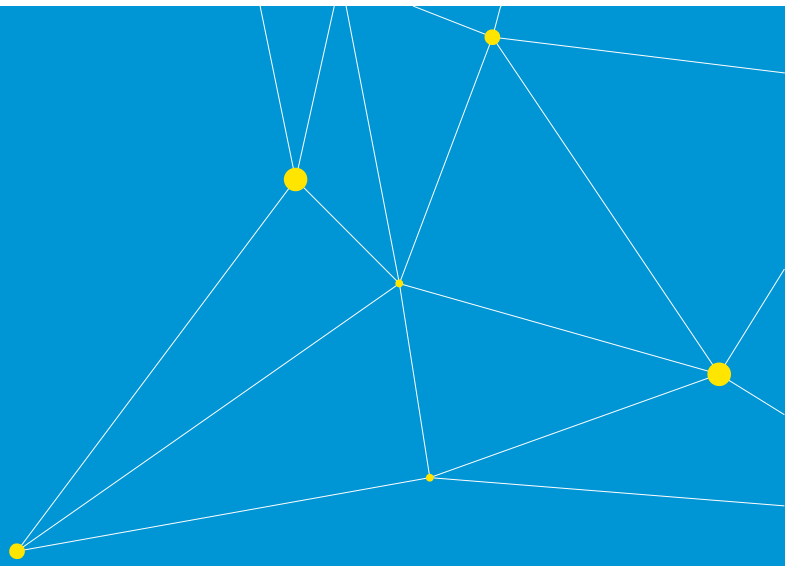
This is a known issue with Lenel OnGuard 7.4 Update 1 (7.4.457.69) running in an Enterprise configuration where devices do not send events through OpenAccess to the Milestone ACM Server integration.
For questions and information concerning a fix for this issue, please contact Lenel support for information 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 Lenel OnGuard and Milestone systems on Windows Server 2012 R2 and Windows Server 2016.
- This ACM integration is currently coded to only work with a Lenel OnGuard system using SQL Server as its database. Oracle integration has not been implemented yet.
- Only United States English installers are available.
- Lenel OnGuard doesn't model doors; they work only with readers. But Milestone ACM requires doors to be modelled. Therefore, the Lenel 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 Lenel 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.