Lenel OnGuard Access Control Module (ACM) Integration User Manual v1.0

milestone

Target Audience for this Document

This document is aimed at system users and describes the integration between Lenel OnGuard and Milestone.

Basic knowledge of the Milestone XProtect surveillance software is required.

High knowledge of the Lenel system usage is required.

Contents

Copyright, Trademarks & Disclaimers

Copyright

Trademarks

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

Microsoft and Windows are registered trademarks of Microsoft Corporation.

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

Disclaimer

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

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

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

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

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

Revisions

Date	Version	What was changed	Author
05/11/2016	1.0	Original version	Doug Beyer
04/07/2017	1.0	Added OnGuard versions certified against and updated scability numbers.	Doug Beyer

Scalability Testing

The Lenel ACM integration has been tested against the following. Any customer exceeding the number of devices or using different hardware should contact Milestone to coordinate any additional testing or code changes.

Numbers of devices

Type of Device	Count
Door	1029
Reader	1029
Panel	1900
Alarm Panel	38
Card Holders	10000

Physical hardware

Any other hardware has not been tested:

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

General description

Introduction

This document describes specifics to the Access Control Module (ACM) integration between Milestone XProtect and the Lenel OnGuard access control (AC) system.

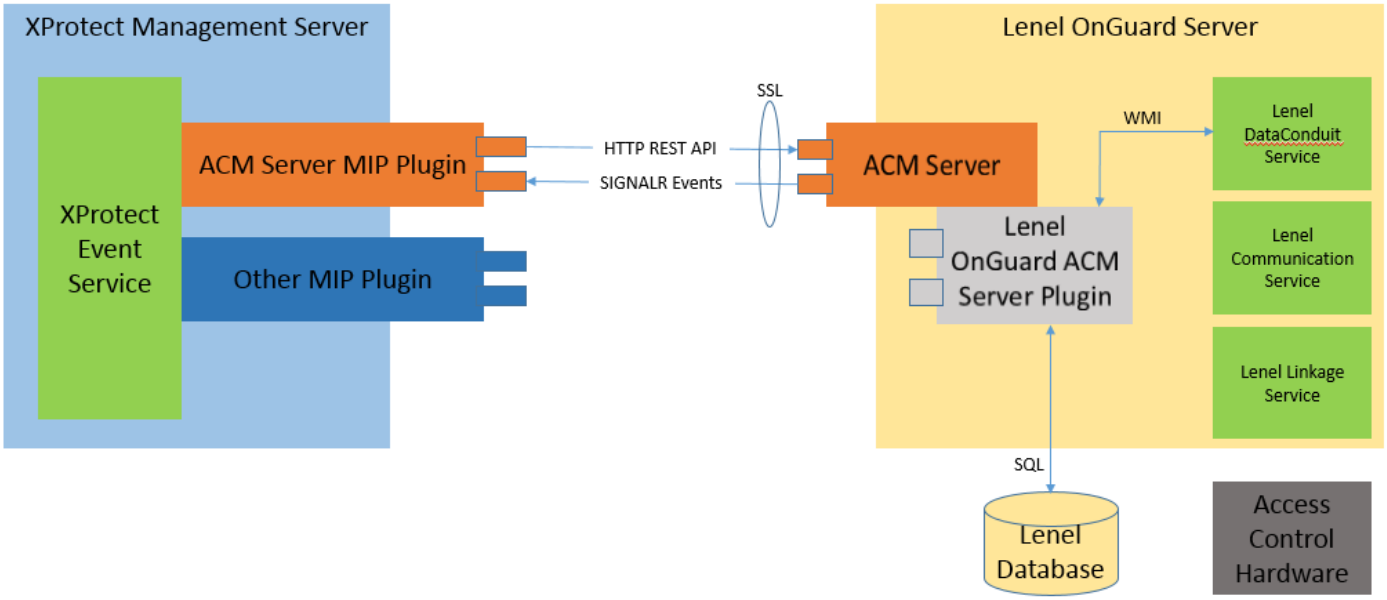
This integration supports the following standard ACM features:

- Retrieve configuration from the Lenel AC system, e.g. doors and event types
- Receive AC event streams and state changes from the Lenel system
- Get/Search cardholder information with picture association (if available through the HR API)
- Add images to cardholders if not available through Lenel
- Create alarms in alarm manager based on AC events - these alarms will be managed only in the XProtect platform. This means that if an alarm is acknowledged in the Milestone Video Management System (VMS), the alarm will still remain open on the Lenel system
- Association of access events to cameras for simultaneous display of events and live video
- Select and categorize the events the user wants to view from the Lenel 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:

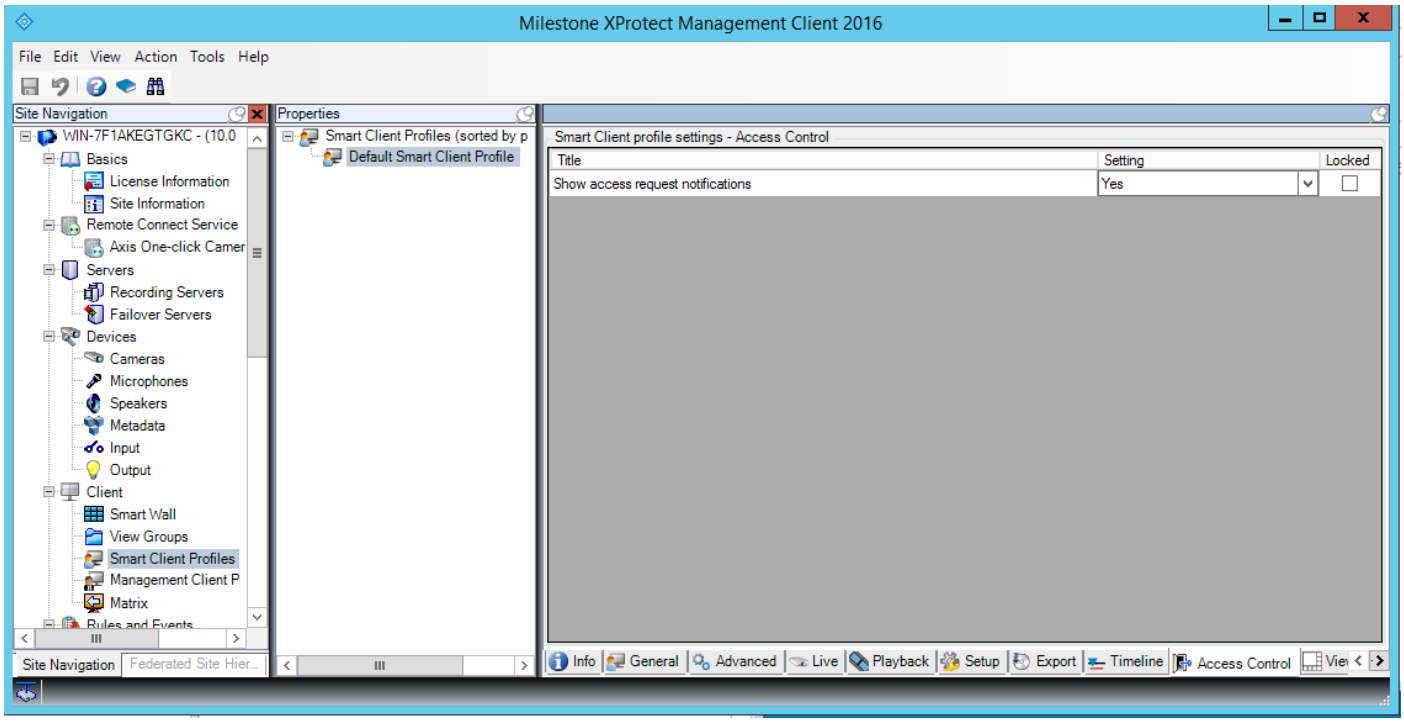
- The ACM Server MIP Plugin that runs in the XProtect Event Server
- The ACM Server that runs on the Lenel server
- The Lenel-OnGuard ACM Server plugin that runs on the Lenel server as well



Prerequisites

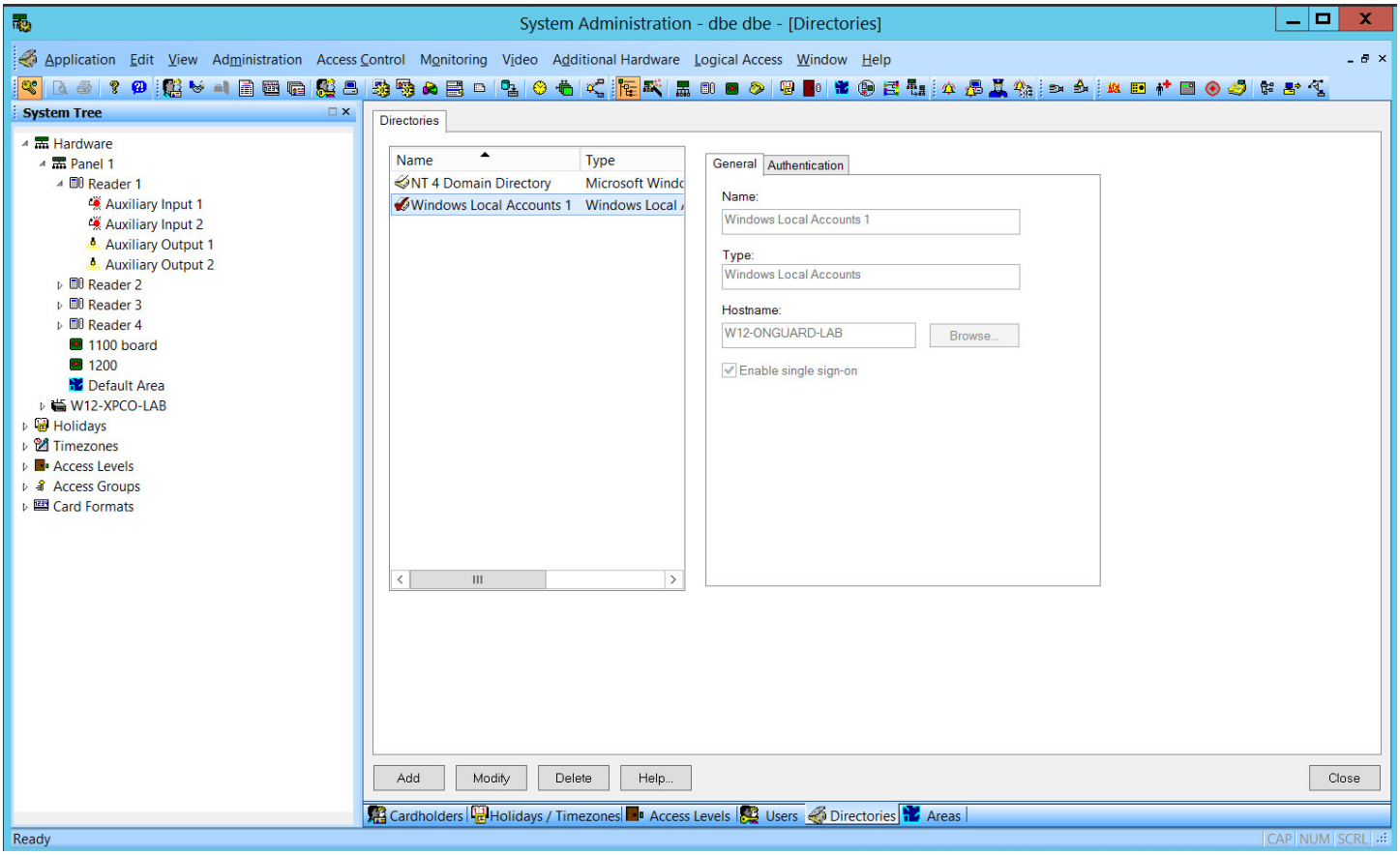
- General
  - .NET Framework 4.5 must be installed on the Lenel server machine (dotnetfx45_full_x86_x64.exe)
  - All servers (i.e. the Lenel and Milestone machines) must be time-synchronized to within a couple of minutes of one another.
  - The customer must have a Milestone license with Access Control enabled and the proper number of doors and cameras allocated.
- The Lenel AC System
  - The supported Lenel versions are 7.0 service pack 2, 7.1 update 1, and 7.2 update 1, 7.3.345 (or later).
  - SQL Server is properly configured. See Configure SQL Server for Connections for suggestions.
  - Lenel is properly configured for its hardware and successfully communicates with its hardware.
  - Lenel is configured for single sign-on (see below for details).
  - Lenel is configured to generate software events (see below for details).
  - The following Windows services are running on the Lenel machine:
    - LS Communication Server – required for the hardware to communicate with the Lenel OnGuard AC system
    - LS DataConduIT Service – required for our integration to use the Lenel DataConduit API
    - LS Linkage Server – required for event handling.
- The Milestone ACM Server
  - Must be run in the context of a Windows admin user that is linked to a Lenel Directory that is marked as single sign-on. See below below for details.
- XProtect Management and Smart Client Applications
  - The machine running the Milestone Event Server must have network name resolution such that it can resolve the computer name of the Lenel Server machine (e.g. DNS, manual host file entry, etc). The Lenel machine must also be able to resolve the Milestone machine.
  - The user that runs the Milestone Management Client application needs to be configured as an administrator within Milestone.
  - The user that runs the Milestone Management Client and Smart Client applications needs to be configured to use the default smart client and management profiles.
    - In the Milestone Management Client, the user should be a member of the **Administrator's Role**
    - The Smart Client user's profile should include **Access Control – Show access request notifications = Yes** (default setting) and any other rights that affect what the user can see/access in Smart Client

    The default Smart Client profile does have these rights as shown below:

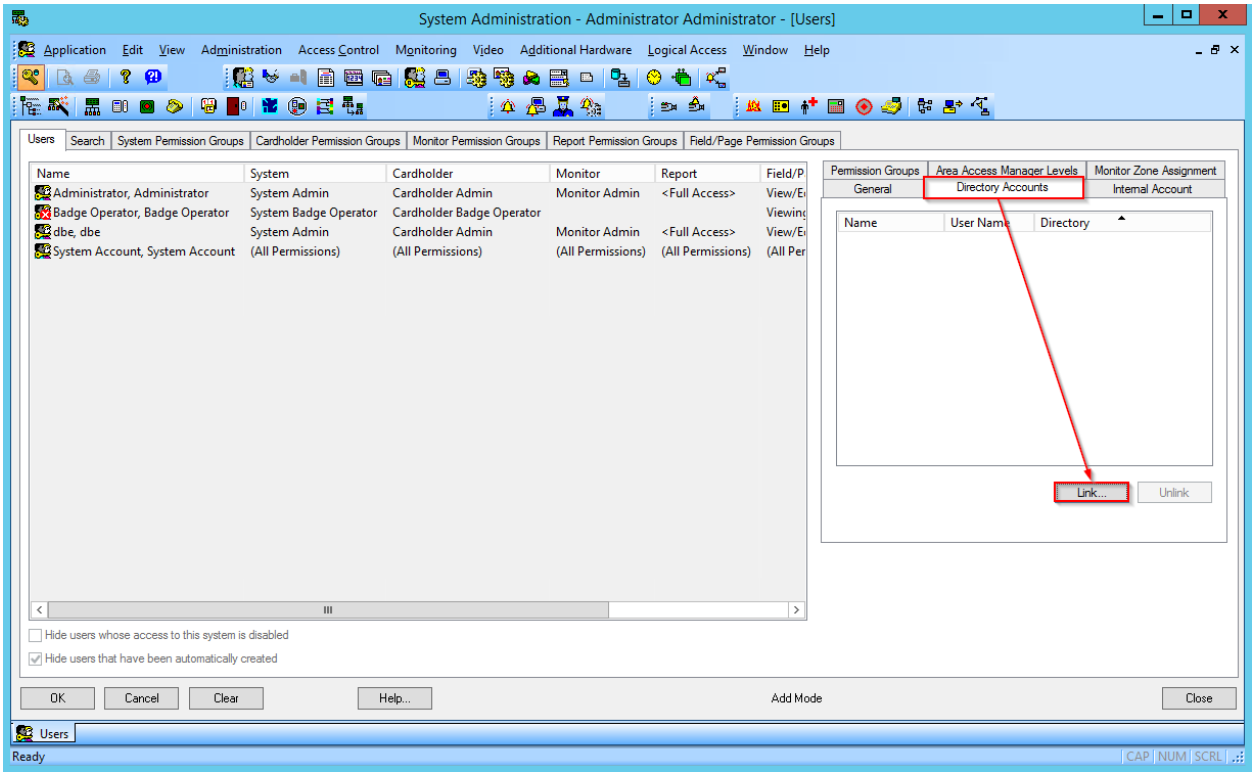


Configure Lenel OnGuard for Single Sign-On

1. Using the Lenel System Administration app:
    a. Click Administration + Directories
        i. Add a “Windows Local Accounts” directory.
            1. Use the machine name for the Hostname field.
            2. Ensure that “Enable single sign-on” is checked.
            3. On the Authentication tab, select “Current Windows Account”.
        ii. Note that if you’re creating a Directory of a type other than “Windows Local Accounts” (e.g. LDAP, Active Directory, NT 4 Domain), then ensure that the user is both a member of the Domain Administrators group and the Local Adminstrators group on the Lenel OnGuard server.

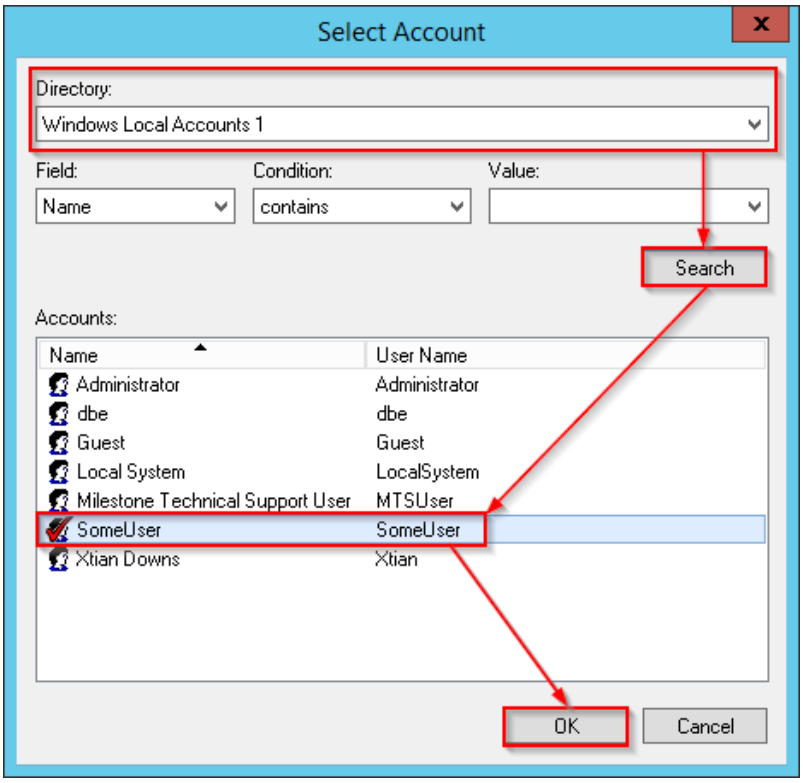


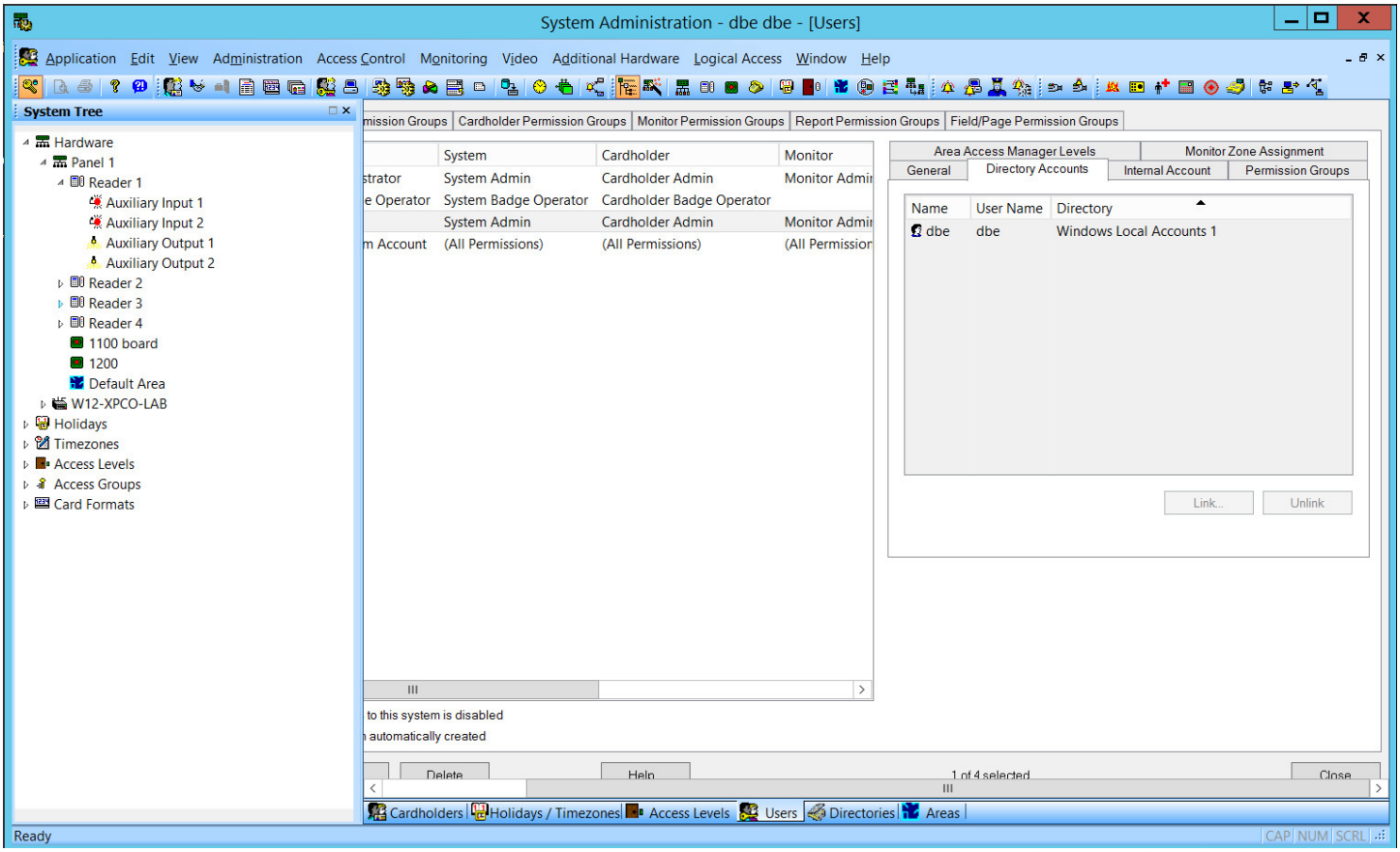
    b. Click Administration + Users
        i. Note that the integration will only discover hardware and get events from Lenel segments that the user is configured for. So if the integration should see all hardware and events, the single signon user must be configured to have access to all segments.
        ii. Add a new user.
            1. General tab
                a. Give the user some name.
                    i. Both first and last names are required but they can be same string if the last name isn’t logically required.
                    ii. I believe the values of the first and last names are immaterial with respect to setting up single sign-on.
                    iii. The first and last names do not have to match an actual Windows user.
                b. Be sure that “Access to this system is disabled” is NOT checked.
            2. Directory Accounts tab
                a. Link the user to the directory you created above.



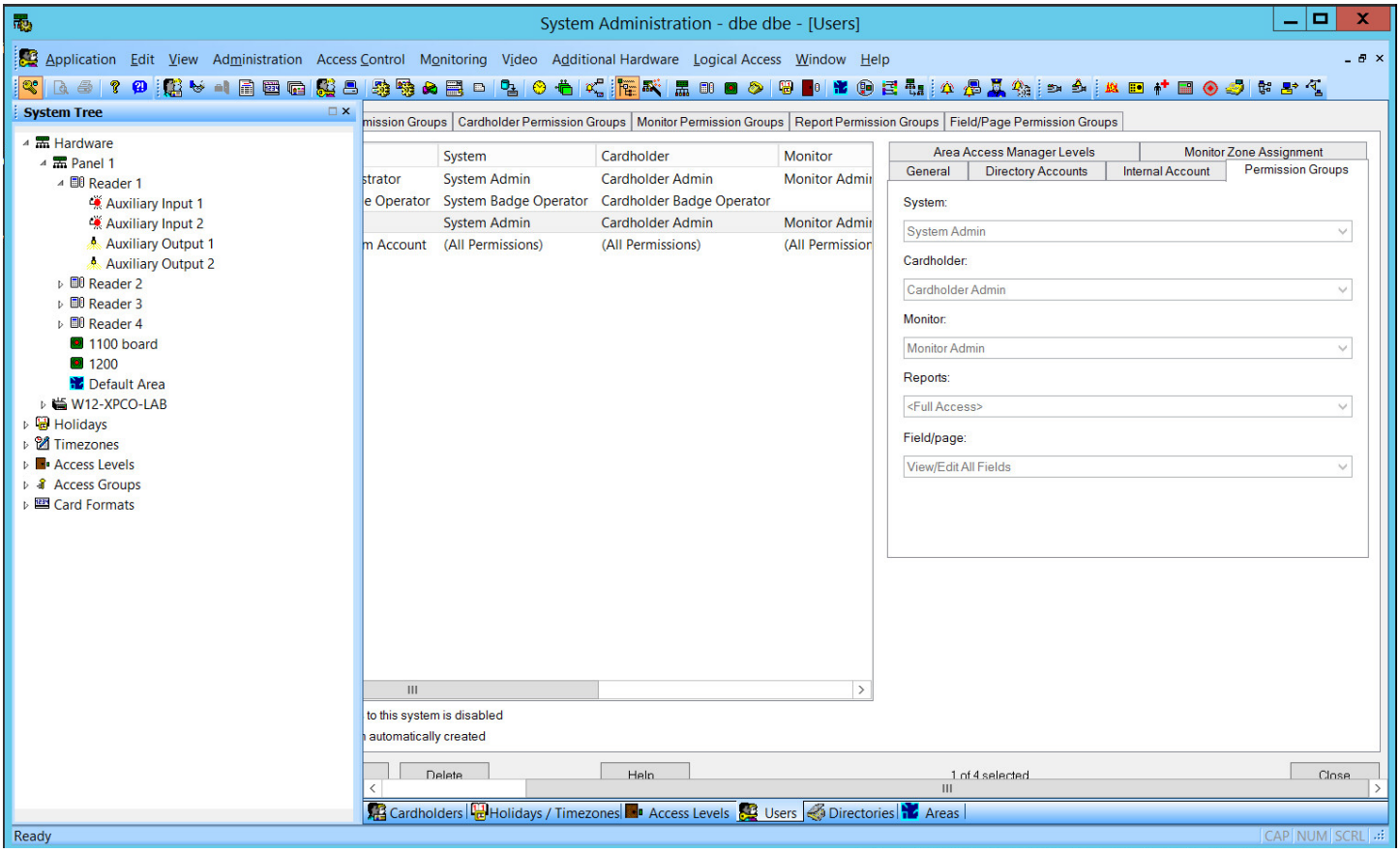
In the **Select Account** dialog, Select **Directory** from drop-down, click **Search**, select a Windows user (must be a member of the machine's local Administrators group) in **Accounts** then click **OK**.

Note that a single Lenel Directory can only be linked to one Windows user. If you attempt to create another Lenel user and try to link that same Lenel Directory to a different Windows user the dialog's Accounts list, it will fail.





3. Internal Account tab
    a. We tested the integration using both vaild and invalid login credentials, and with the "User has internal account" checked and unchecked. None of these settings seem to impact or impair the functionality of the integration in any observable way.
    b. The "User has internal account" checkbox defaults to being checked. It's sufficient to leave it checked.
    c. Enter login credentials.
        i. Login credentials are required by the UI. As stated above, it seems that either valid or invalid credentials are sufficient for our plugin to have access to DataConduit.
4. Permission Group tab
    a. Assign the following permission groups:
        i. System = System Admin
        ii. Cardholder = Cardholder Admin
        iii. Monitor = Monitor Admin
        iv. Reports = Full Access
        v. Field/page = View/Edit All Fields



2. Setting Milestone ACM Server start options
    a. Open Windows Services (Start menu + type “services” (without the quotes) + Run As Administrator).
    b. Locate the Milestone ACM Server service
        i. Right-click and select Properties
        ii. Go to Log On tab, select “This account”, and enter the credentials of a Windows admin user that is linked to a Lenel Directory that is marked for single sign-on.
            1. See the Lenel System Administration application + Users + Directory Accounts tab above where you identified the Lenel Directory that was marked for single sign-on.

Configure Lenel OnGuard to Generate Software Events

1. Under Administration + System Options:
    a. Check the DataConduit Service + Generate Software Events checkbox.
    b. Set the Linkage Server Host to the Lenel server’s machine name.
    c. Set the Message Broker Service Host to the Lenel server’s machine name.

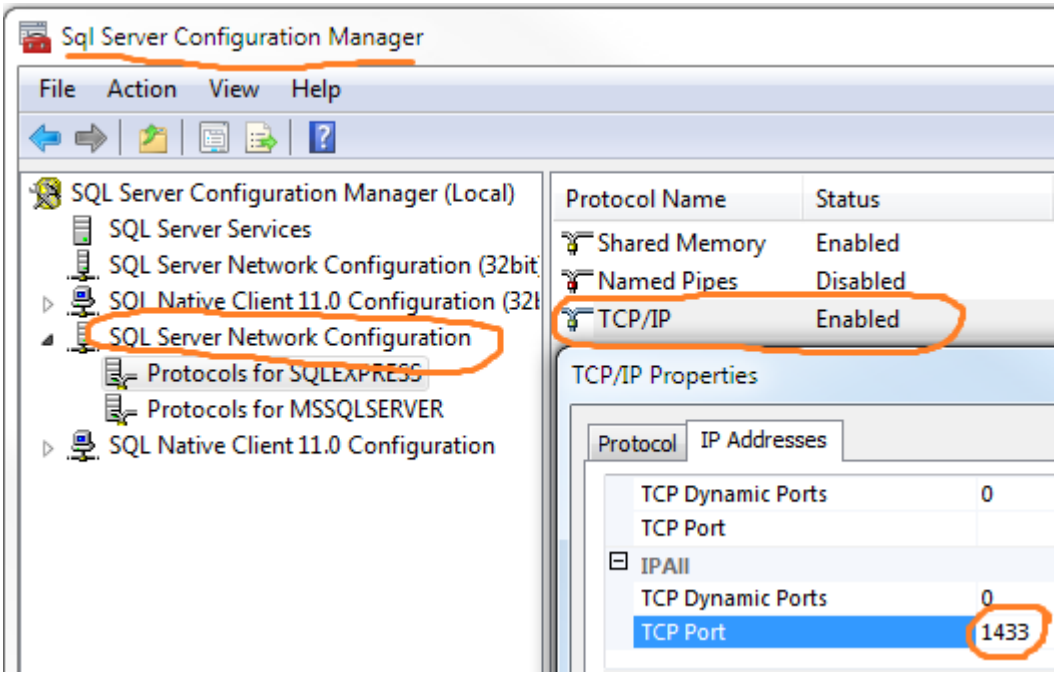
Configure SQL Server for Connections

These instructions are not meant to replace the knowledge of a trained SQL Server administrator. They are here because we’ve seen SQL Server installations not configured this way and the Lenel integration was unable to connect to the database.

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
        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



Installation

The installation package consists of three files which should be installed in the following order:

1) Install the pre-requisites on the Lenel server machine
   a) .NET Framework 4.5
   b) Milestone MIP SDK 2016

2) Milestone.ACMServer.msi: Installer for the ACM Server
   a) Must be installed on the Lenel server machine

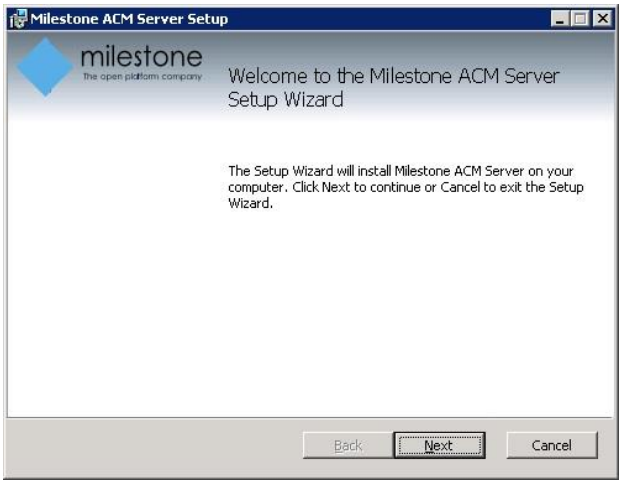
3) Milestone.ACMServer.LenelOnGuard.msi: Installer for the Lenel-OnGuard ACM Server plugin
   a) Must be installed on the Lenel server machine, after the ACMServer.

4) Milestone.ACMServer.MipPlugin.msi: Installer for the XProtect Event Server ACM MIP Plugin
   a) Must be installed on the XProtect Machine that hosts the Event Server Windows service

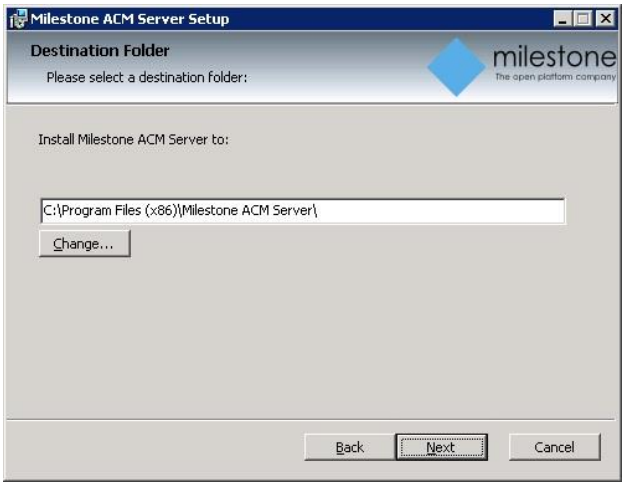
5) Configure the Milestone ACM Server service (see below).

ACM Server

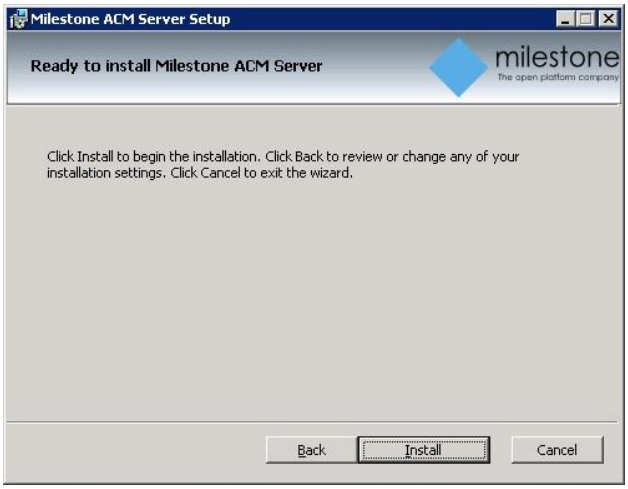
Copy the “Milestone.ACMServer.msi” file to a temporary folder **on the Lenel server** and double-click to install, you should see a screen similar to the following:



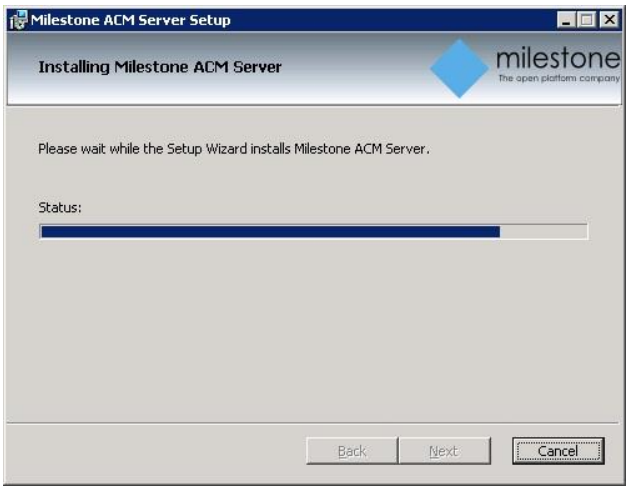
Press next and you will now be able to select the installation path, it is recommended to use the default as displayed:



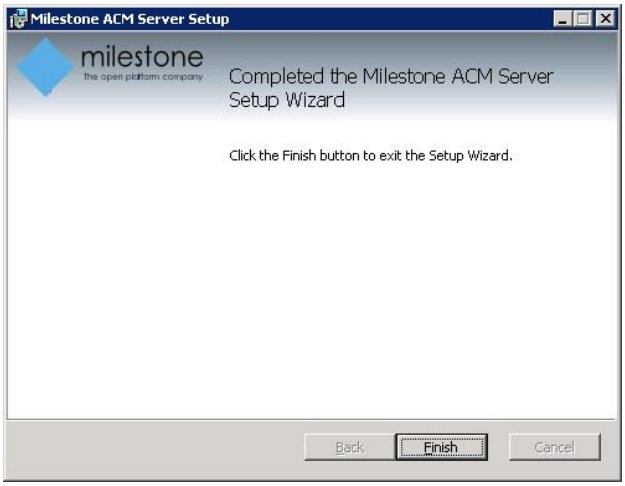
Press next and you are now ready to install, if you are satisfied with the selected options, press install to continue:



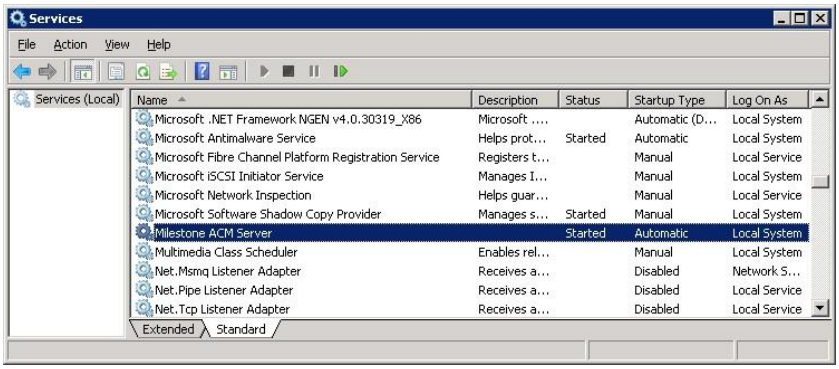
Install progress...



You have successfully installed the ACM Server:

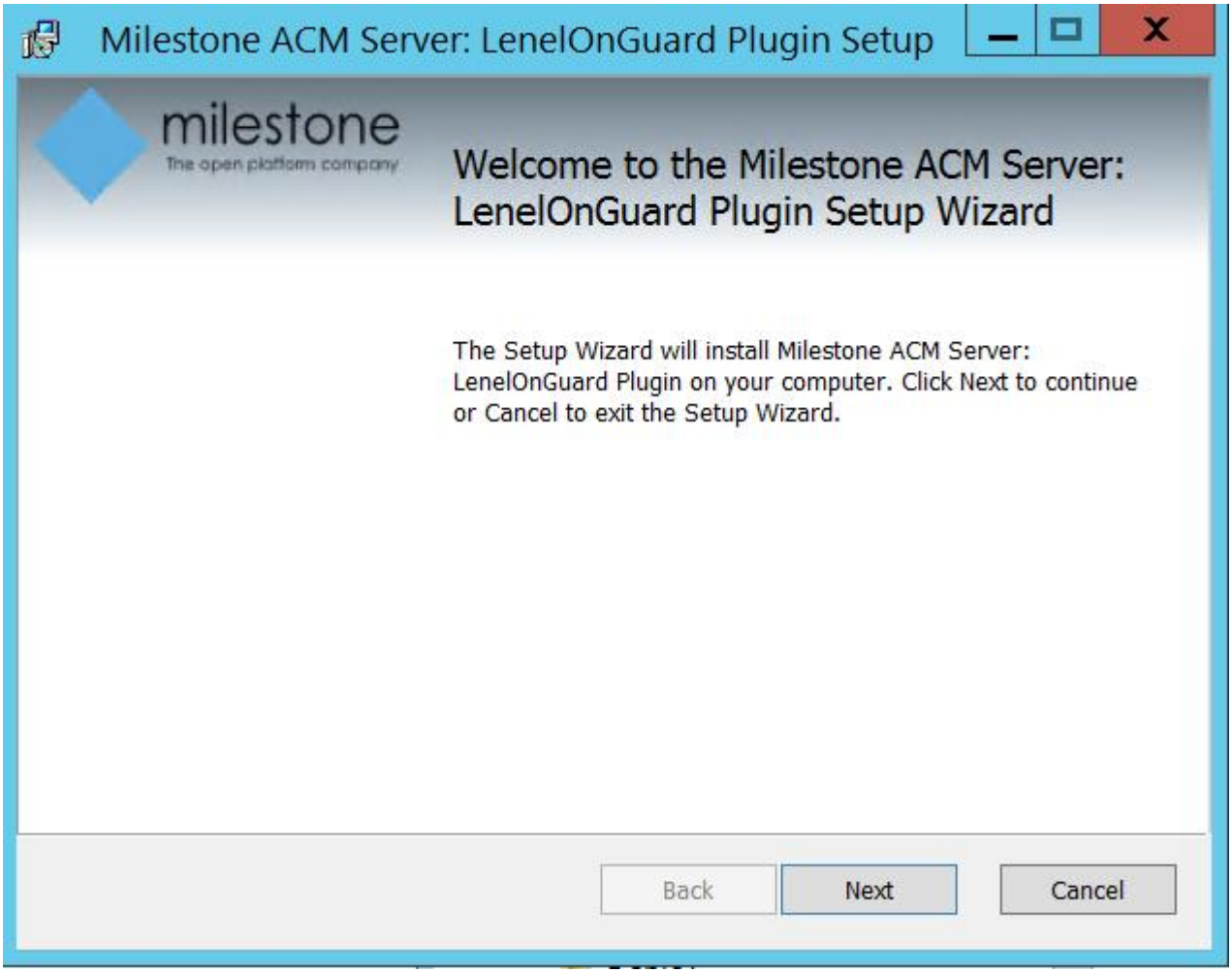


You can verify that the service installed successfully by looking in the Services control panel for a service named Milestone ACM Server.

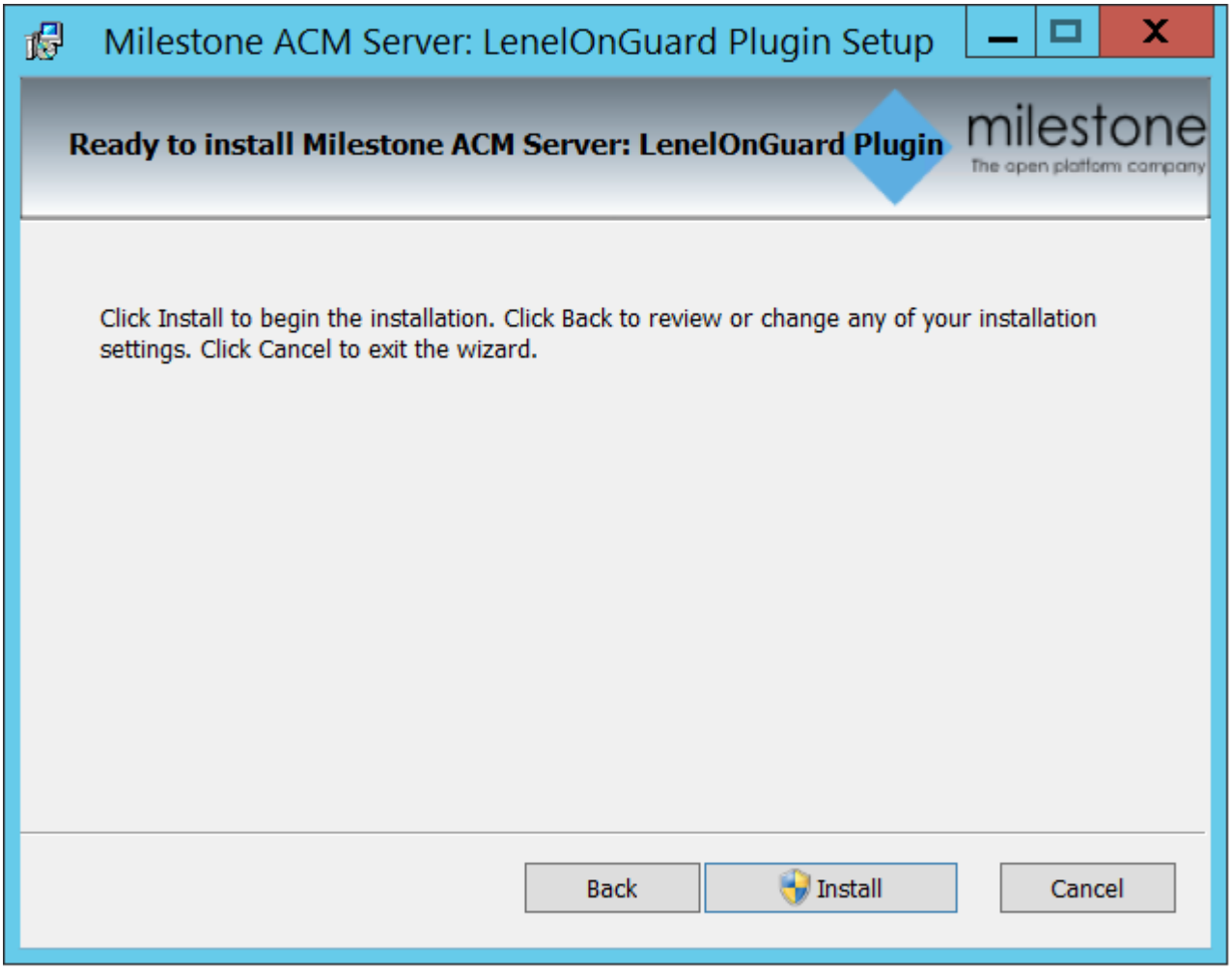


ACM Server: Lenel-OnGuard Plugin

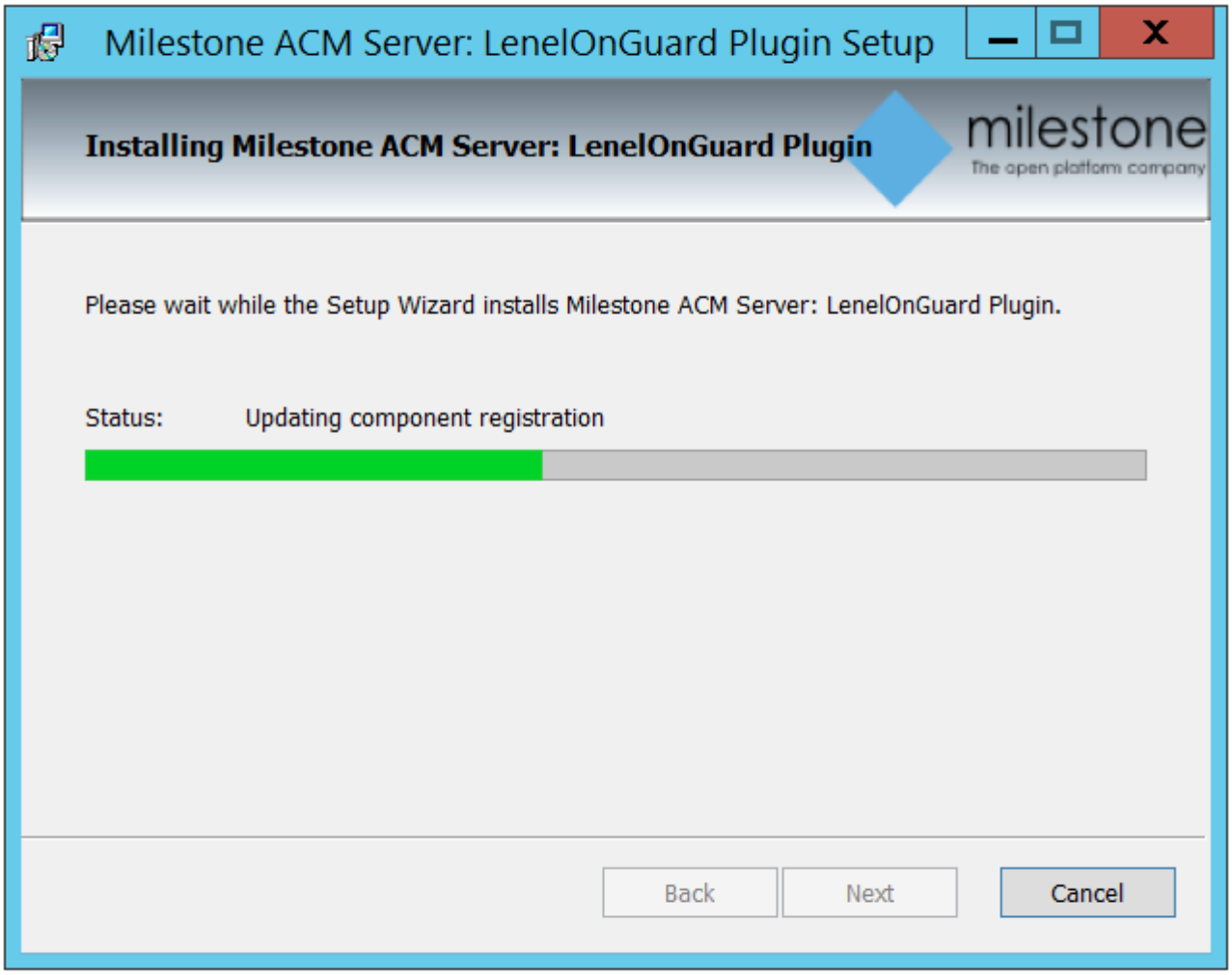
Copy the ” Milestone.ACMServer.LenelOnGuard.msi” file to a temporay folder and double-click to install, you should see a screen similar to the following:



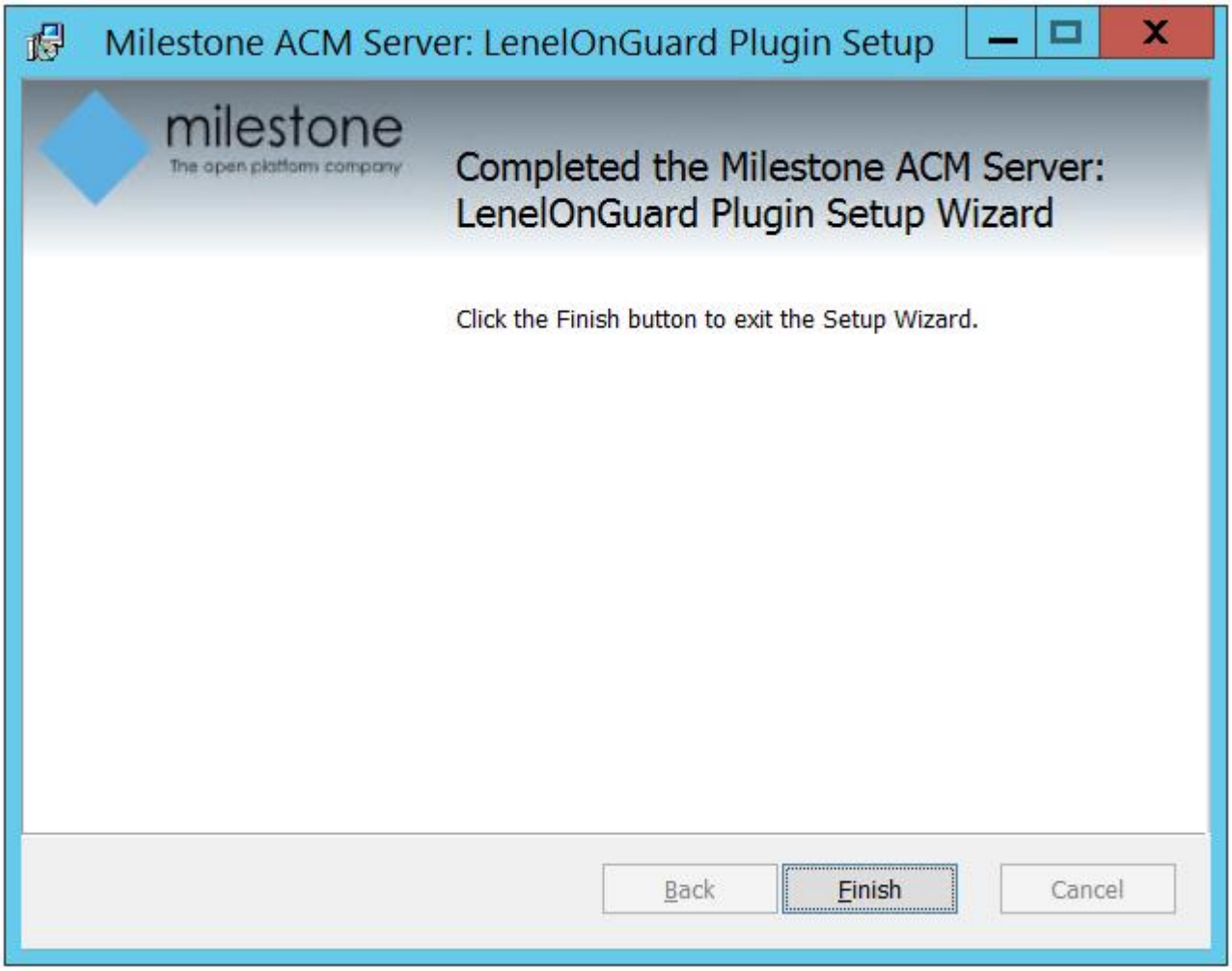
The Lenel-OnGuard plugin automatically detects the presence of both the Lenel server and the pre-installed ACM Server. If either is missing it will refuse to install. There are no options to choose from, when you are ready press install.



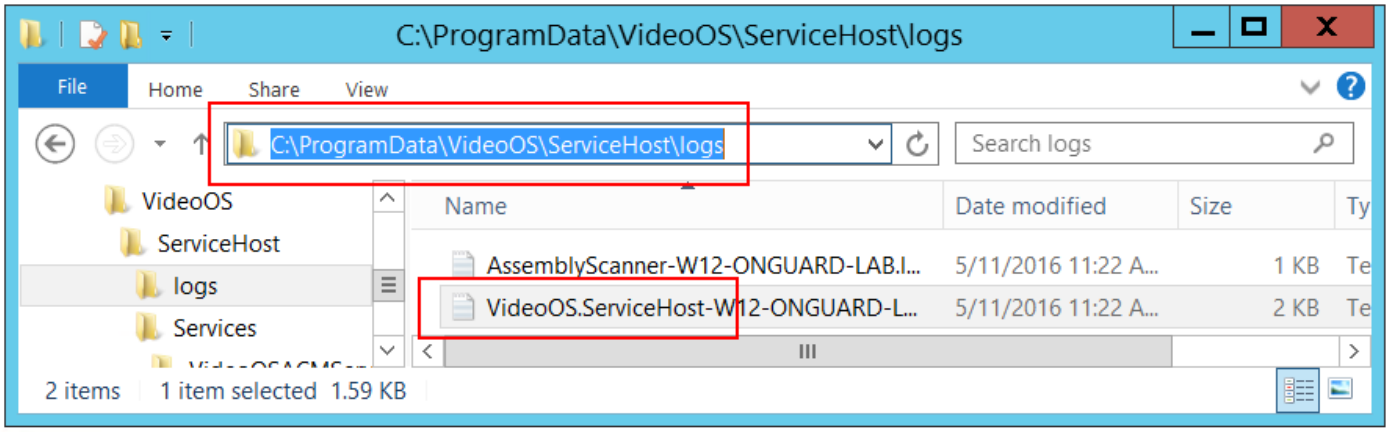
Install progress...

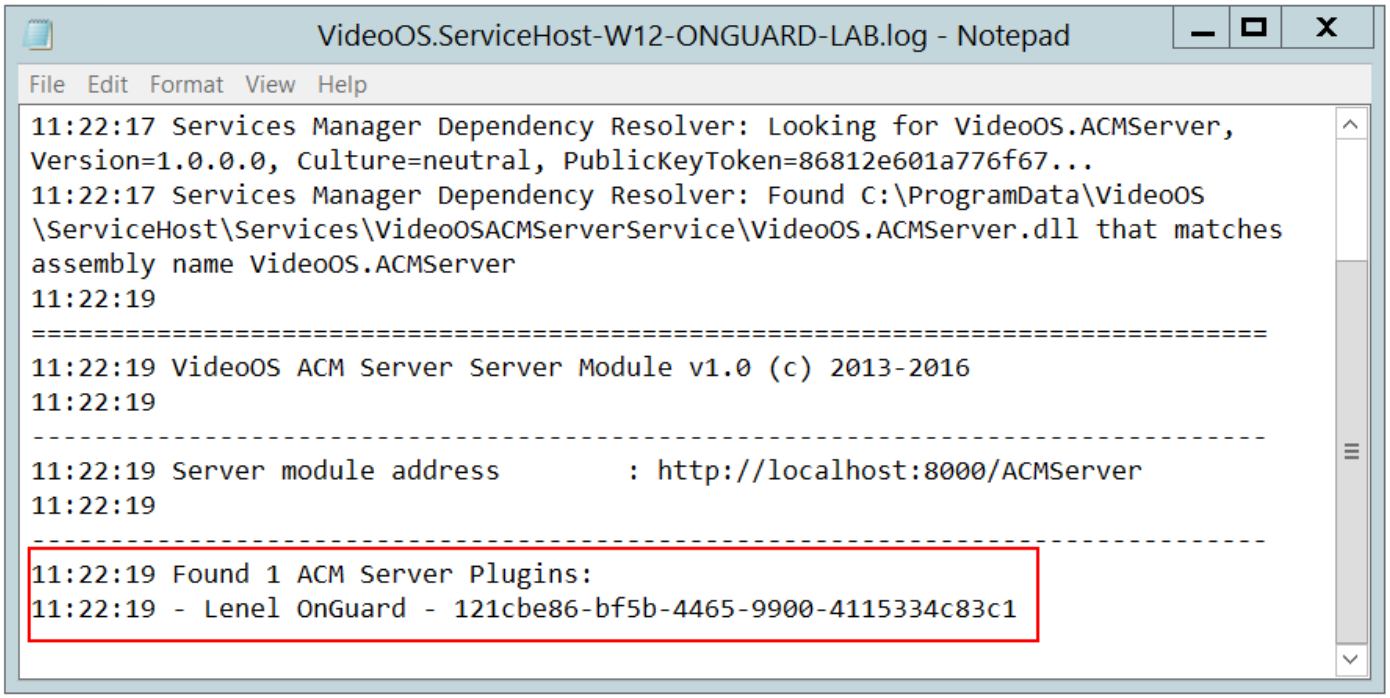


You have successfully installed the Milestone ACM Server Lenel-OnGuard Plugin



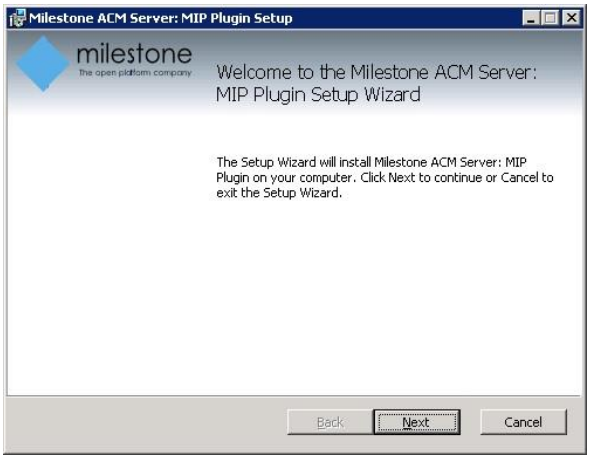
You can verify that the Lenel-OnGuard Plugin is installed and loaded from the logs below:



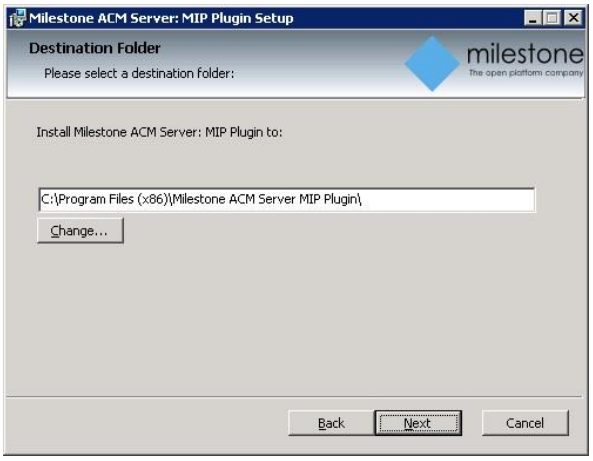


ACM Server: XProtect ACM MIP Plugin

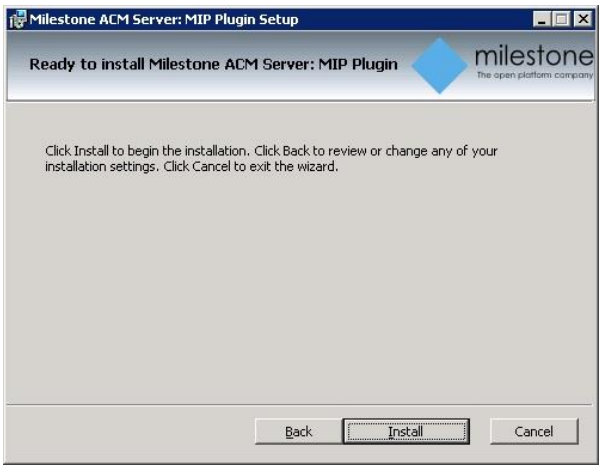
Copy the ”Milestone.ACMServer.MipPlugin.msi” file to a temporay folder on the server where the Xprotect Event Server is installed (in a typical deployment, this is the XProtect Management Server) and double-click to install. You should see a screen similar to the following:



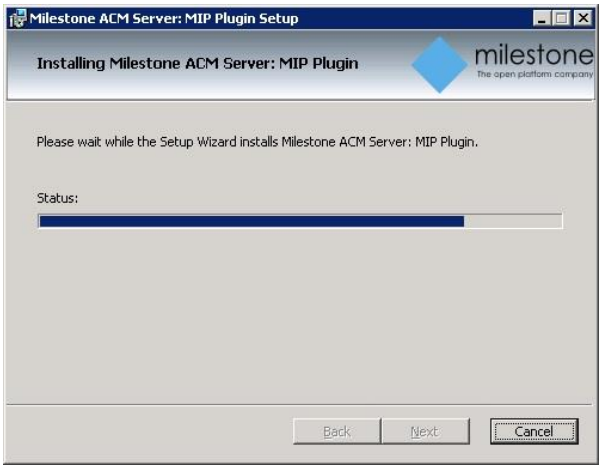
The installer will detect the presence of the XProtect Event Server on the machine and will refuse to install if it cannot be found. It is recommended to leave the default install path as displayed below and press next.



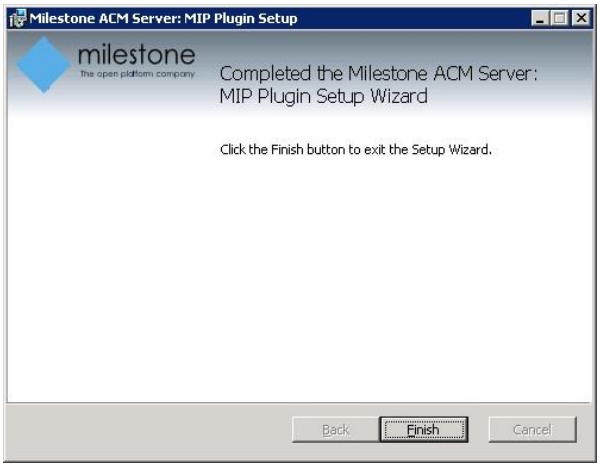
If you are satisfied with the path selection and you are ready to install press ”Install”



Installation progress...



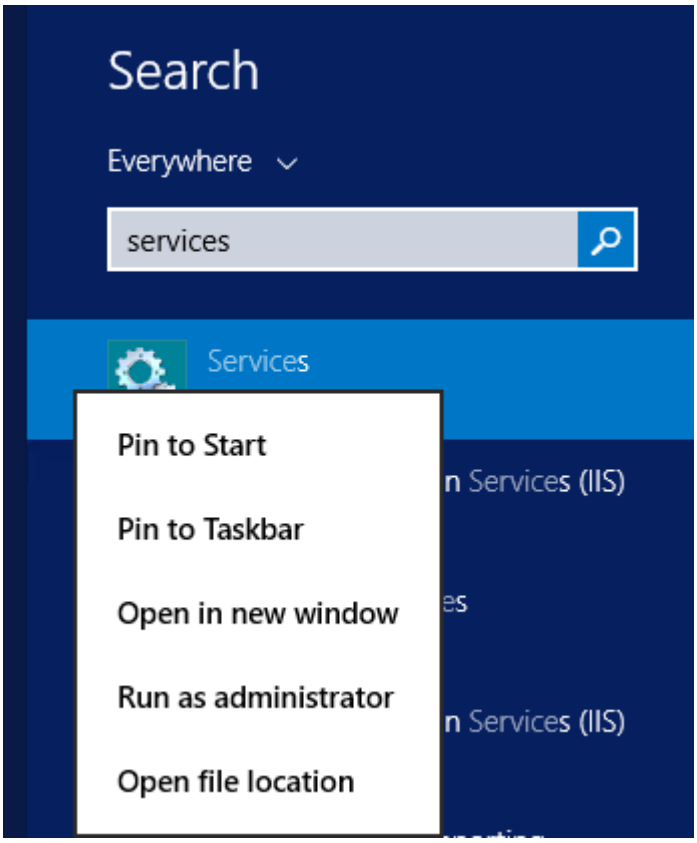
You have successfully installed the ACM MIP Plugin for ACM Server


Milestone ACM Server: MIP Plugin Setup
milestone
The open platform company
Completed the Milestone ACM Server: MIP Plugin Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

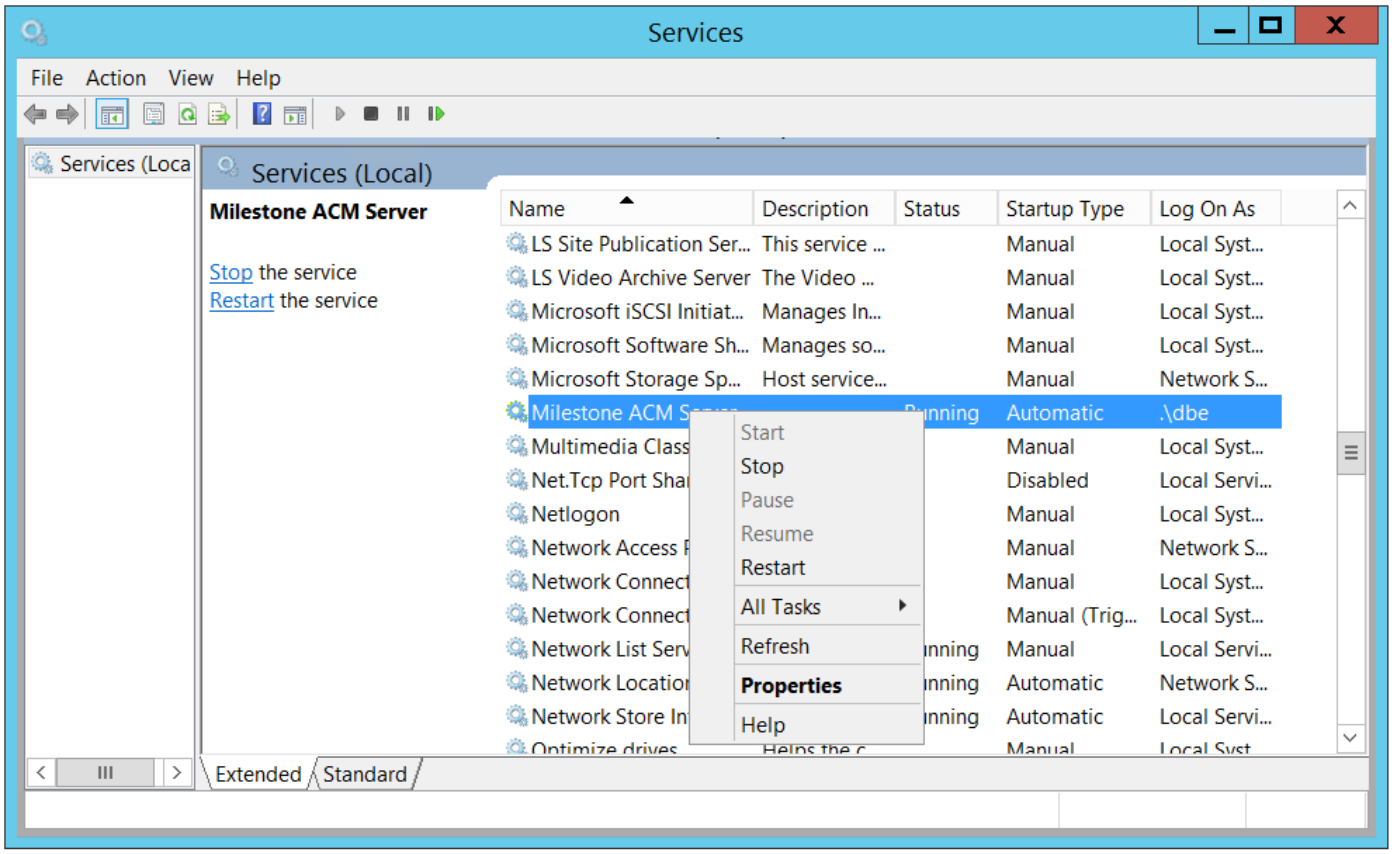
Configuration

ACM Server: Configure to RunAs Lenel Single-Signon Account

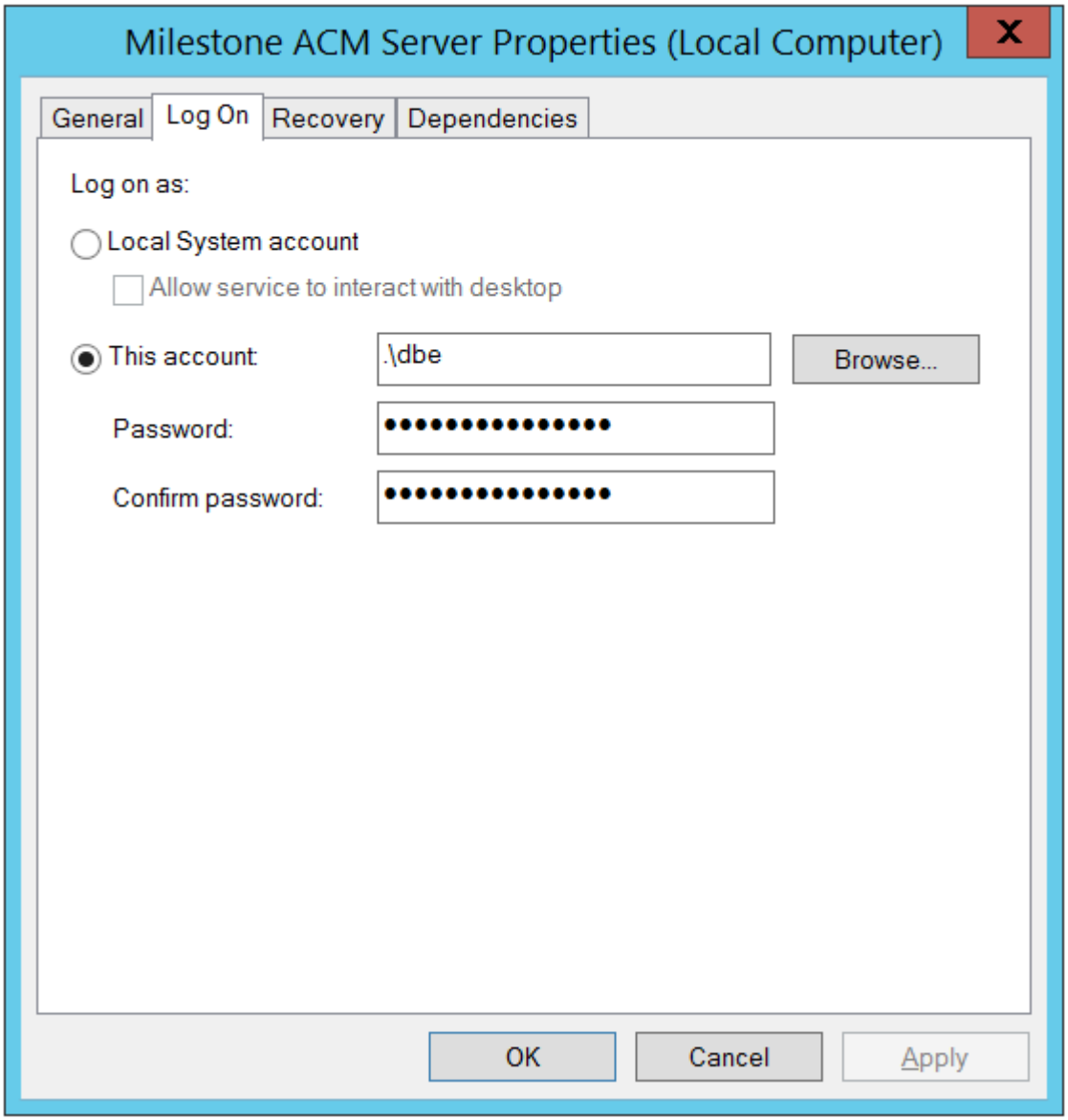
On the Lenel server machine, click the Windows Start menu and type “services”. Right click Services and select “Run as administrator”.



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



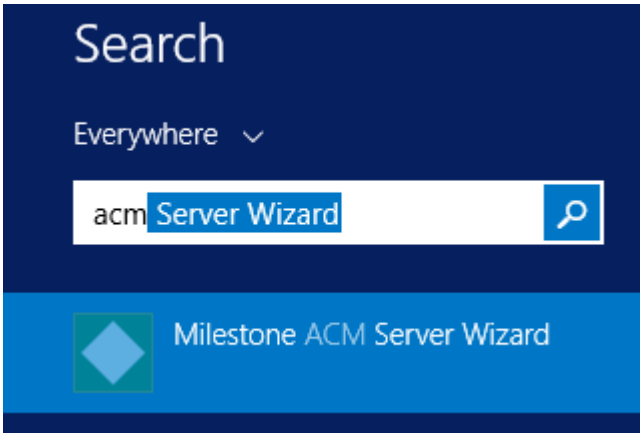
Click the “Log On” tab, select “This account”, and enter the credentials of an admin user on the local machine. Note that this admin user ***must*** be linked to a Lenel Directory that is configured for single signon (see above for configuring single signon).



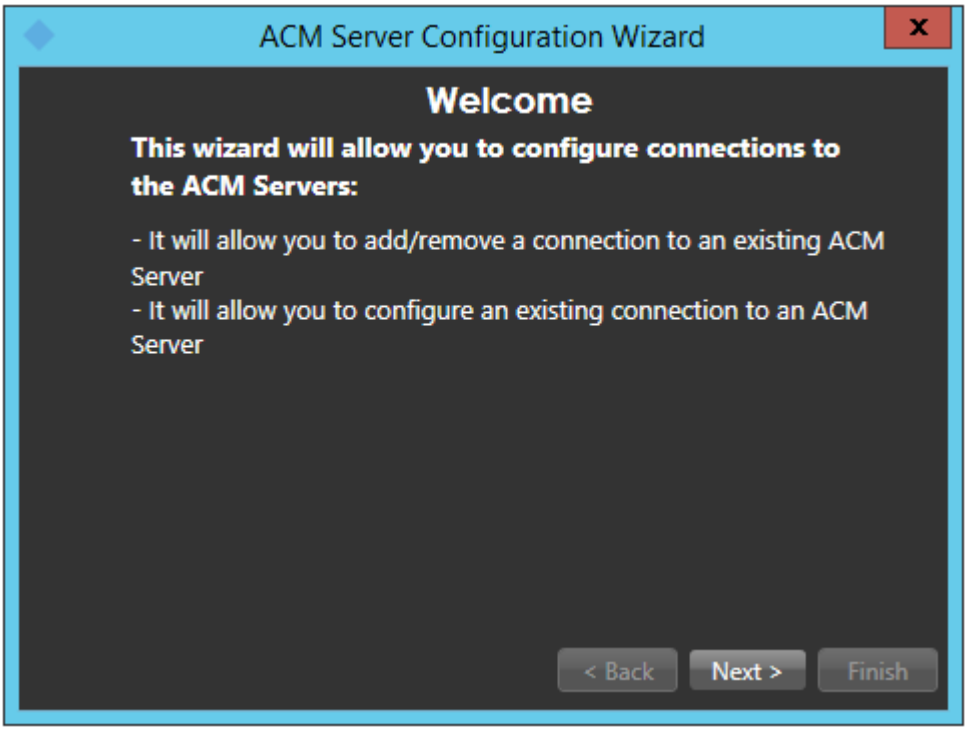
IMPORTANT: Restart the Milestone ACM Server service.

ACM Server: XProtect ACM MIP Plugin

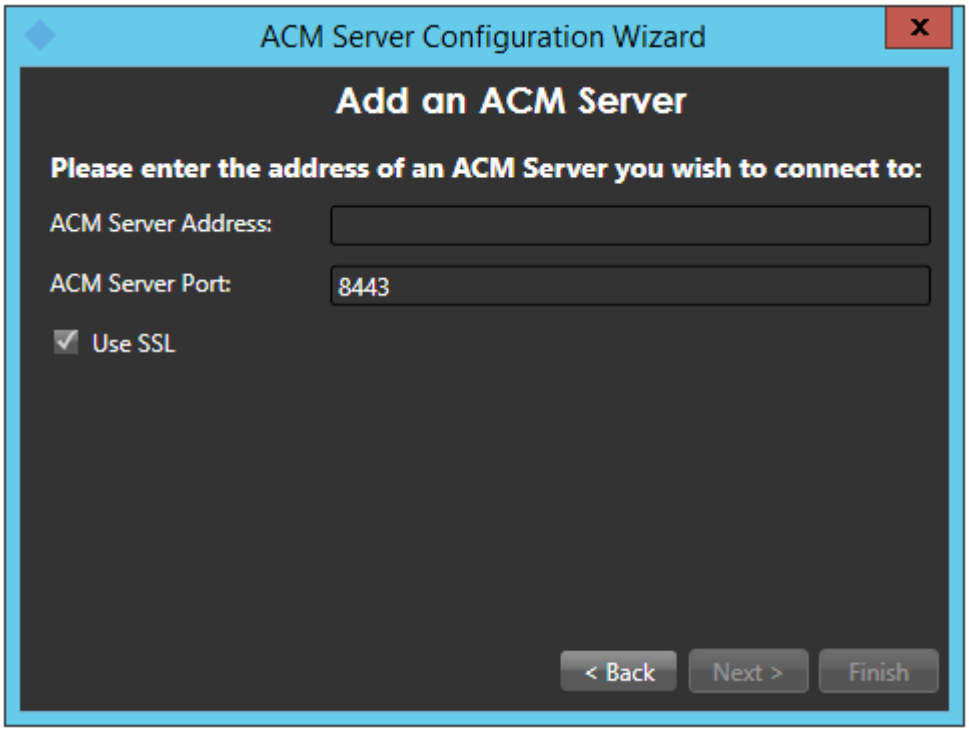
Once all three installers have been setup (see Installation section), it is now time to configure and install the ACM MIP Plugin in the XProtect Event Server. This configuration and deployment is handled by a wizard tool that was installed with the XProtect ACM MIP Plugin package. In the start menu you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



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

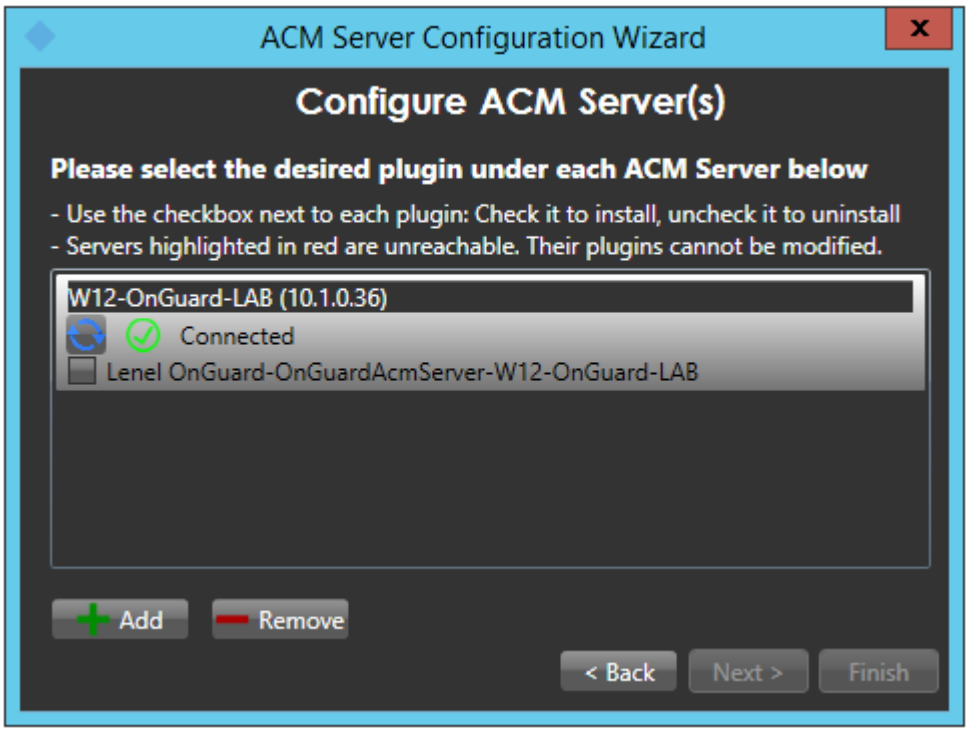


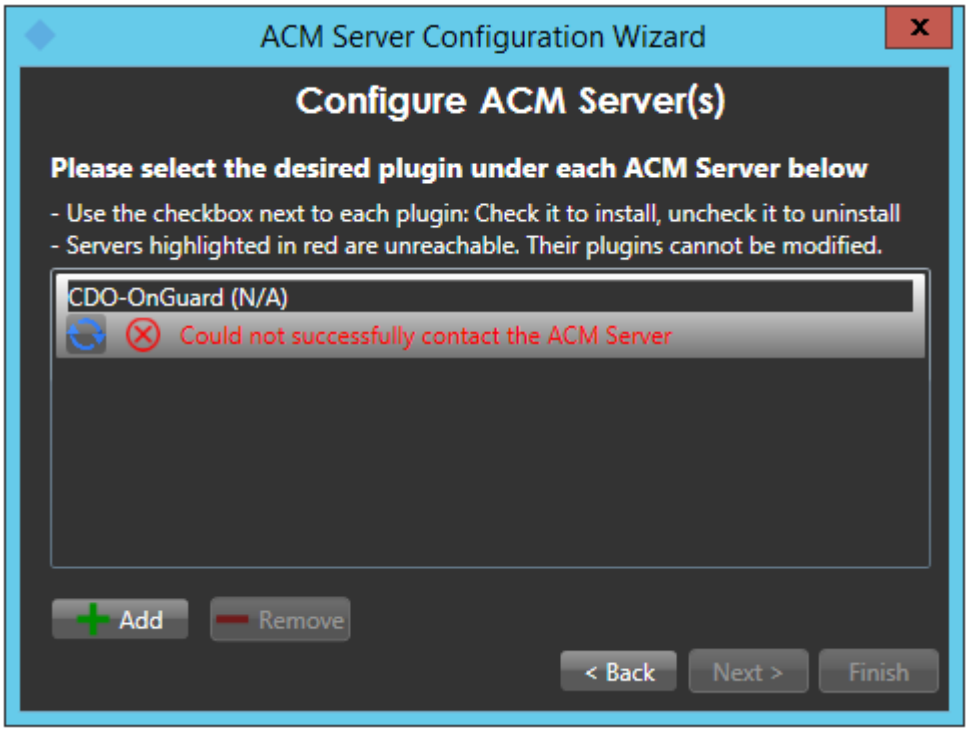
Once you click next, you will have to provide the IP Address / Machine name of the Lenel server on which the ACM Server package was installed.



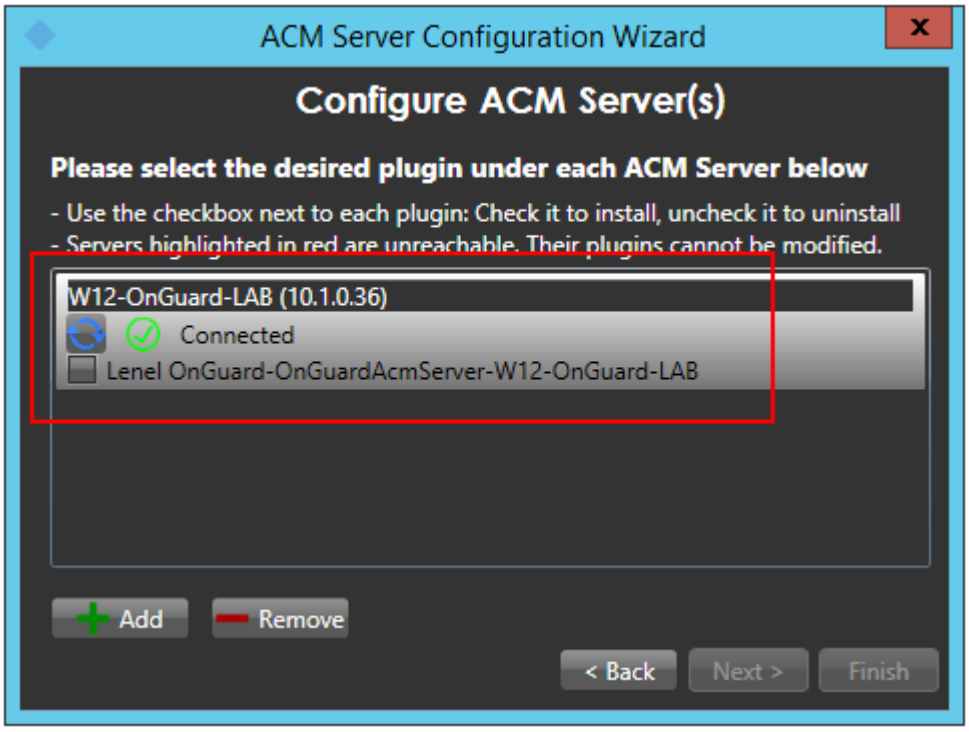
After you have provided the server name/ip address and pressed next, you should get the following screen after the software has validated that there is an ACM Server present at that address. The green checkmark means that it has successfully connected to the provided server name, the red x means that 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 cause of the wizard not being able to connect to the provided server is that the ACM Server on the Lenel machine is not running with sufficient administrative privledges.

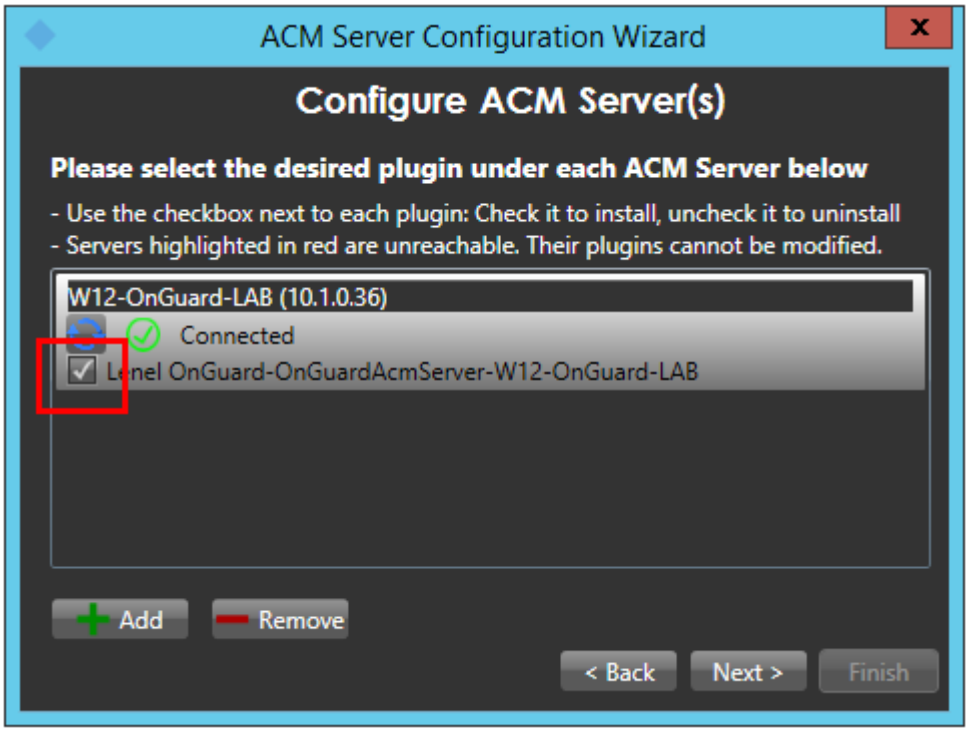




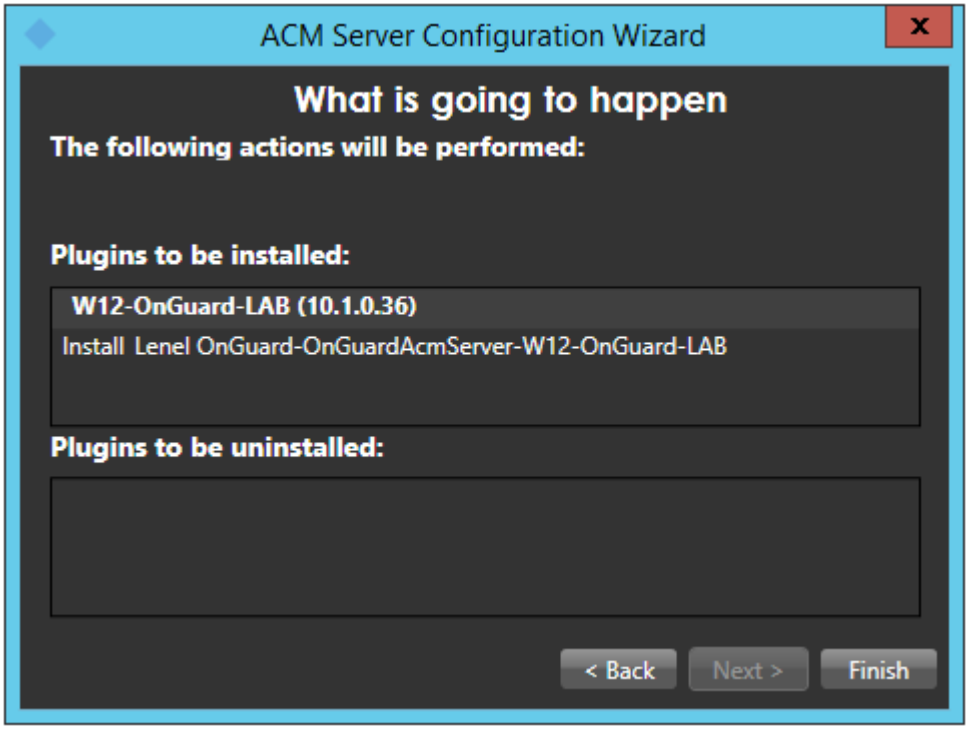
Once you have a successful connection, notice that there is a list of checkboxes under the server heading that represents all detected ACM server plugins installed on that machine. In this case we are looking for Lenel-OnGuard.



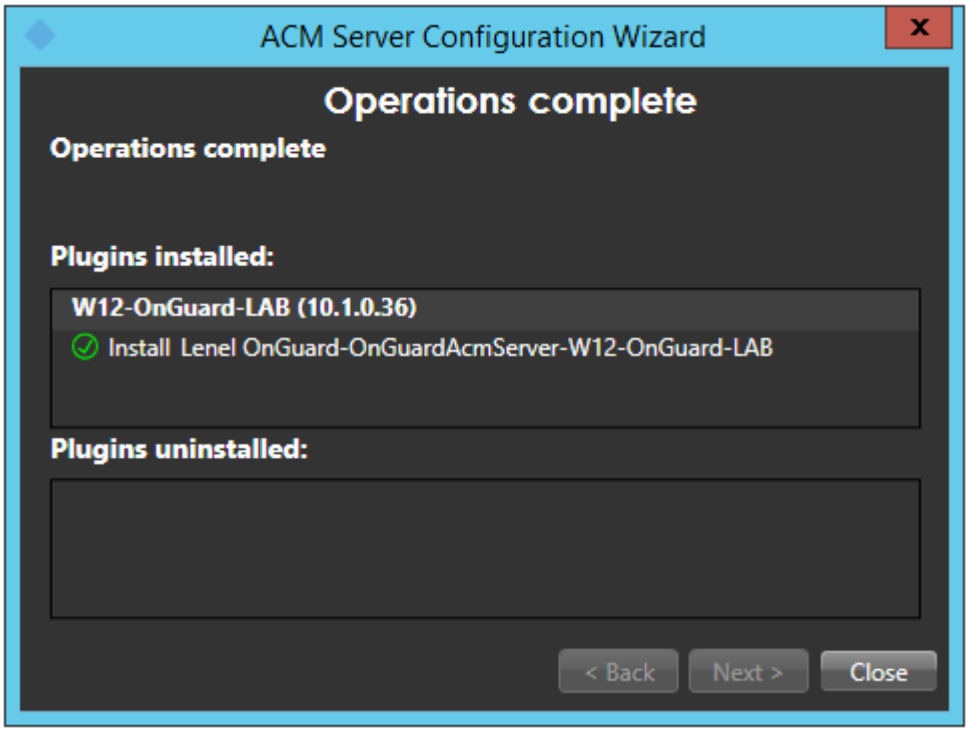
Check the box circled in red below and press next to install a MIP plugin on this host to connect to the Lenel-OnGuard server identified.



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



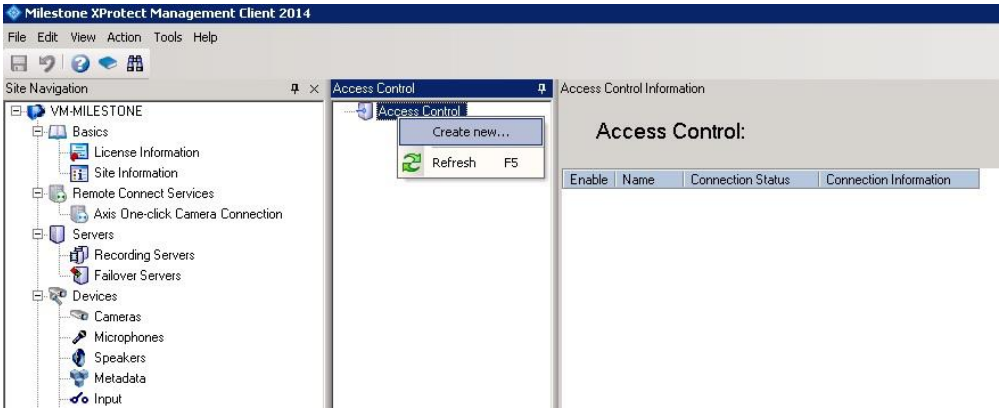
Once the operations are completed, the wizard will display a green checkmark for successful operations and a red x for failed operations.



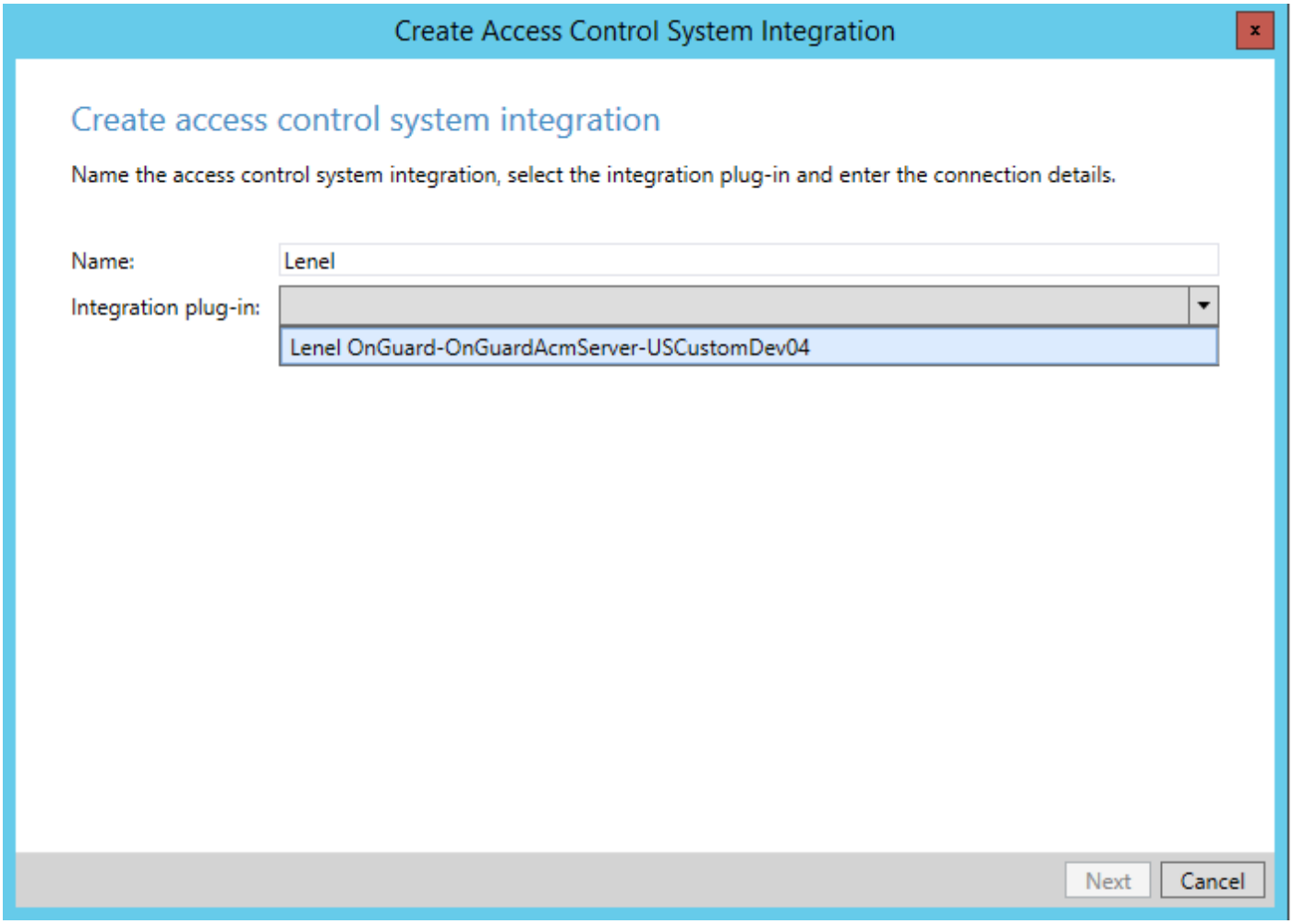
You have successfully installed the ACM Server: XProtect MIP ACM Plugin.

Milestone Management Client Configuration

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.

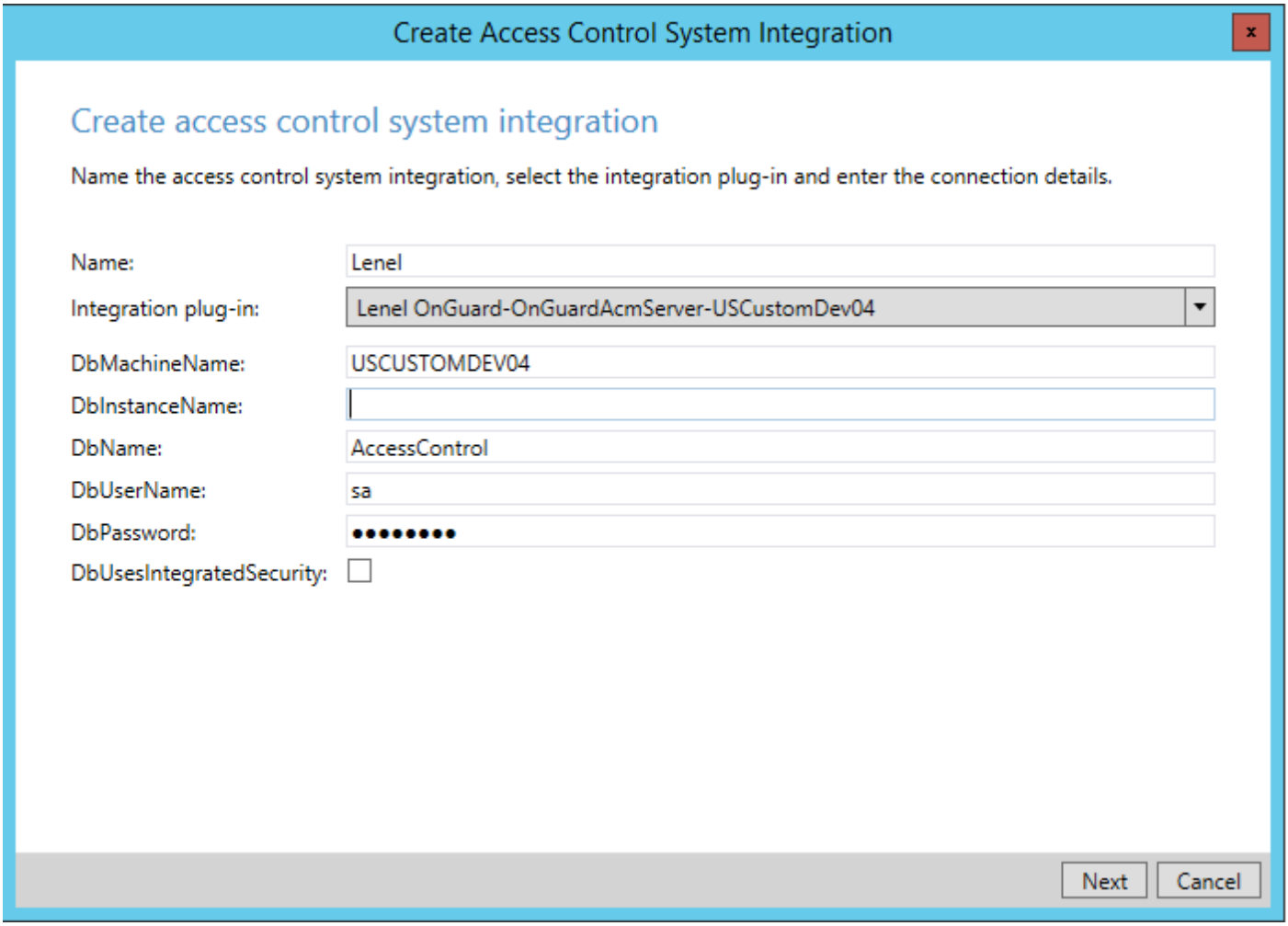


This will popup a wizard to step you through the access control instance creation process. Type a name for the instance of the plugin you wish to create and select from the drop down box the integration plug-in. Note that you will find a plugin named Lenel-OnGuard-OnGuardAcmServer-{ServerName} where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

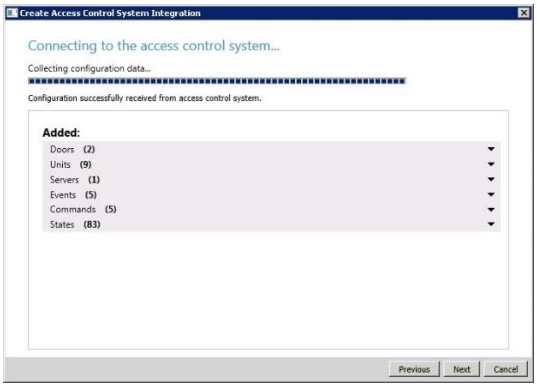


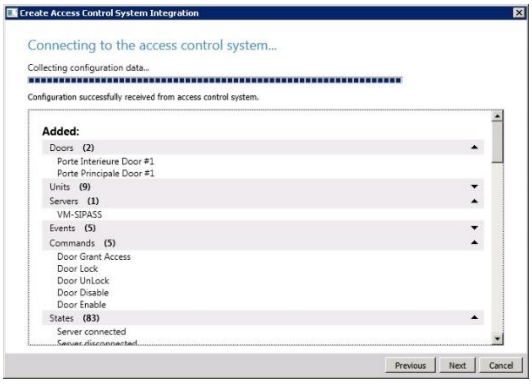
After selecting the plugin, you will have to provide credentials and parameters to configure the connection to the Lenel database server.

IMPORTANT – Leave DbInstanceName blank to connect to the default SQL Server instance.

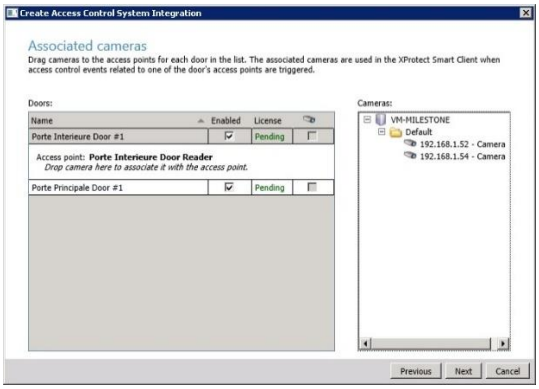


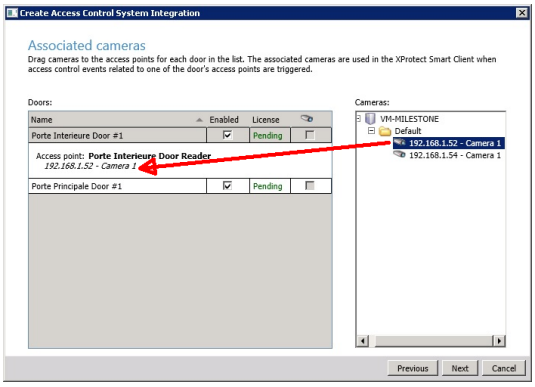
The wizard will now fetch the configuration of the Lenel AC system into Milestone. The screen below is a resume of the configuration found on the server:



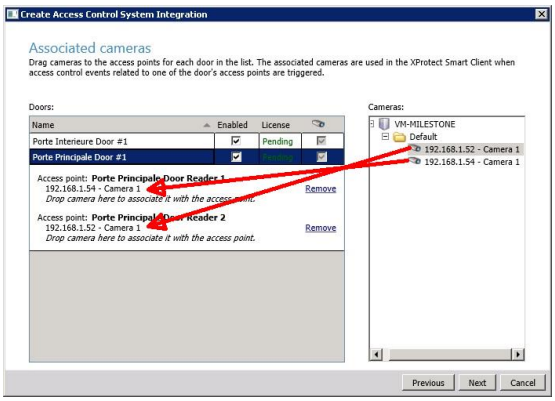


On this screen an association has to be created between each access point of a door and cameras in the Milestone system. This is done so that the system will know which cameras to display on door alarms. For each access point of each door drag a camera from the right tree and place it under the desired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

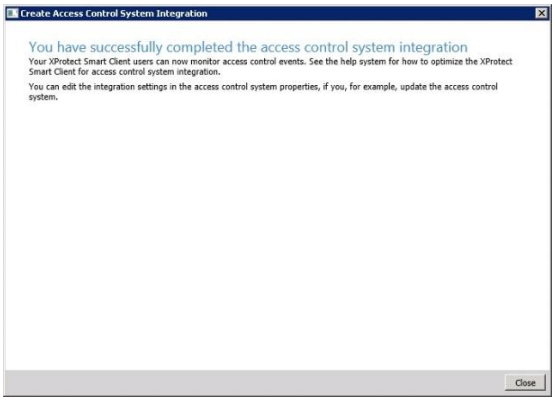




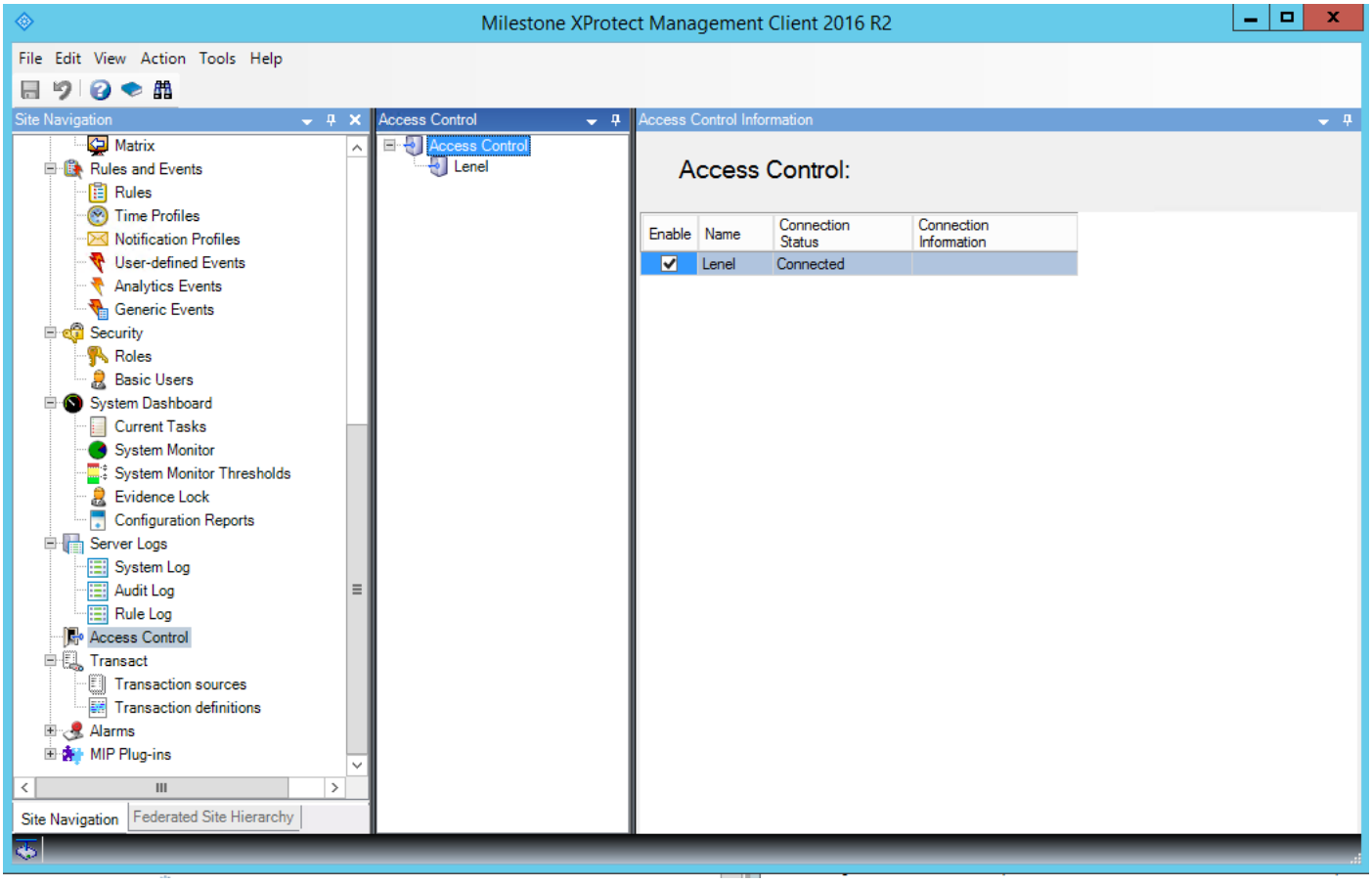
When there is more than one access point per door, you can select the different cameras for the different angles. You can also select more than one camera per access point:



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



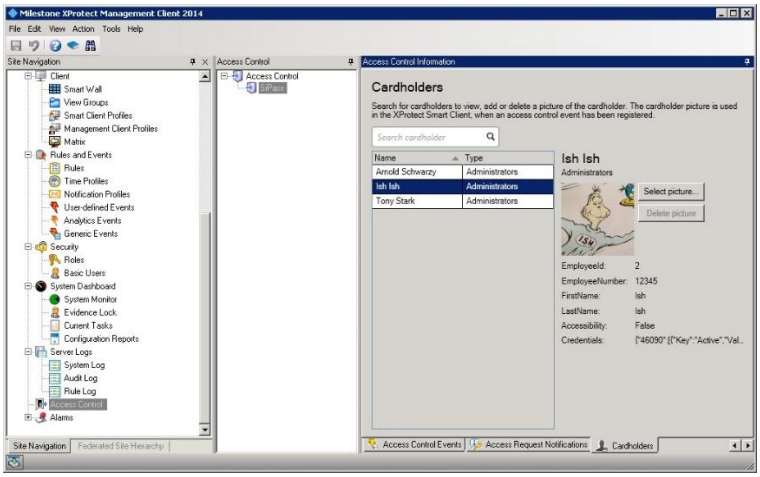
You can verify the that integration module is now connected by looking at the Access control tree.


Milestone XProtect Management Client 2016 R2
File Edit View Action Tools Help
Site Navigation
Matrix
Rules and Events
Rules
Time Profiles
Notification Profiles
User-defined Events
Analytics Events
Generic Events
Security
Roles
Basic Users
System Dashboard
Current Tasks
System Monitor
System Monitor Thresholds
Evidence Lock
Configuration Reports
Server Logs
System Log
Audit Log
Rule Log
Access Control
Transact
Transaction sources
Transaction definitions
Alarms
MIP Plug-ins
Site Navigation
Federated Site Hierarchy
Access Control
Access Control
Lenel
Access Control Information
Access Control:
Enable
Name
Connection Status
Connection Information
Lenel
Connected

Operations

Searching for cardholders

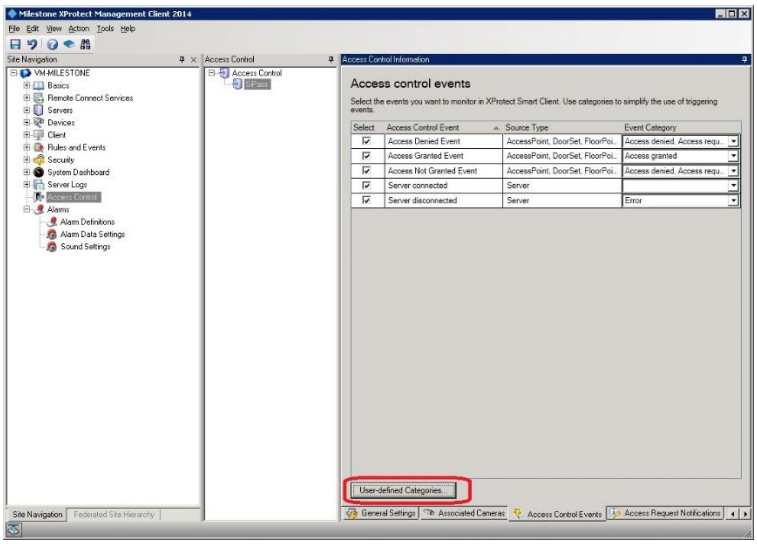
The user can search for existing cardholders in the Lenel system through the management client interface:



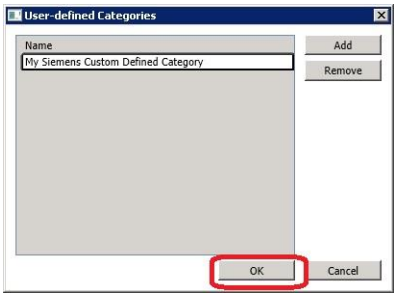
The cardholder picture and detailed information are downloaded from the Lenel server. The search can be made by first name, last name, card number and employee id. Enter the search string in the search cardholder text box.

Defining Alarms based on Lenel events

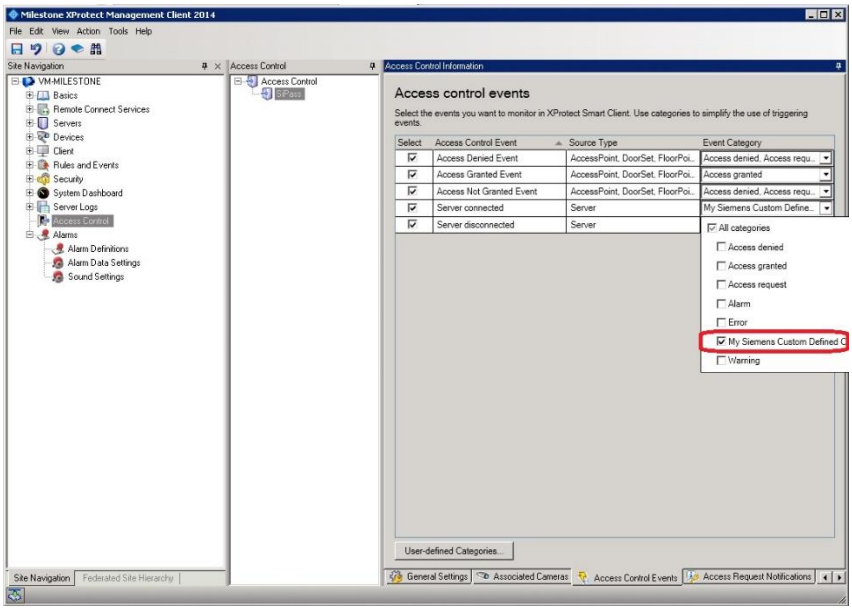
To define alarms based on Lenel events, the events must be part of an event category. The category can be one of the pre-defined Access Control Event categories such as (Access Granted, Access Request, Access Denied, Alarm, Error, Warning) or a user-defined category. Here is how to create an alarm based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



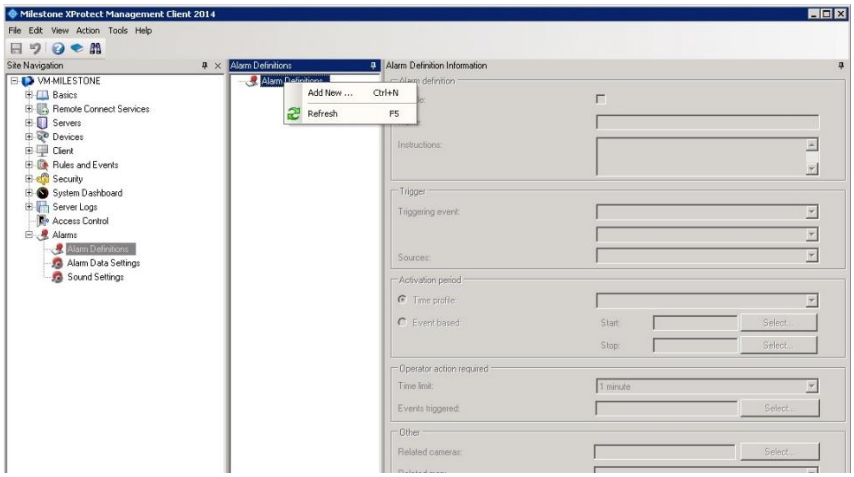
Name the category a pertinent name which represents the group of events and press OK



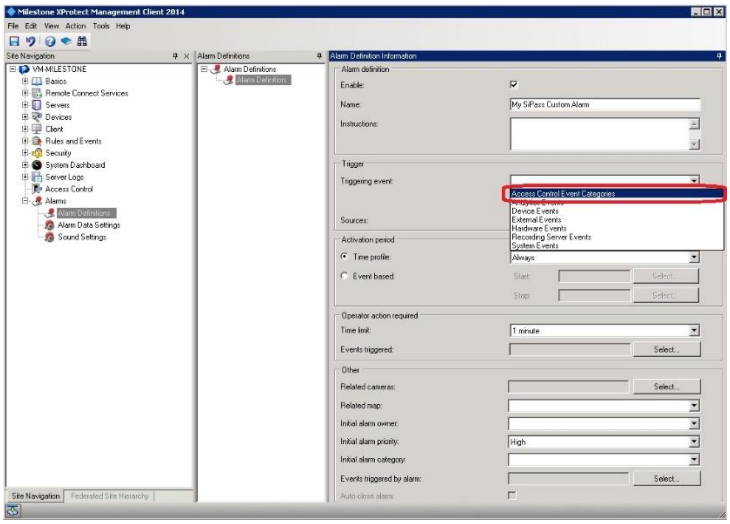
Associate the category with one of the Lenel AC events:



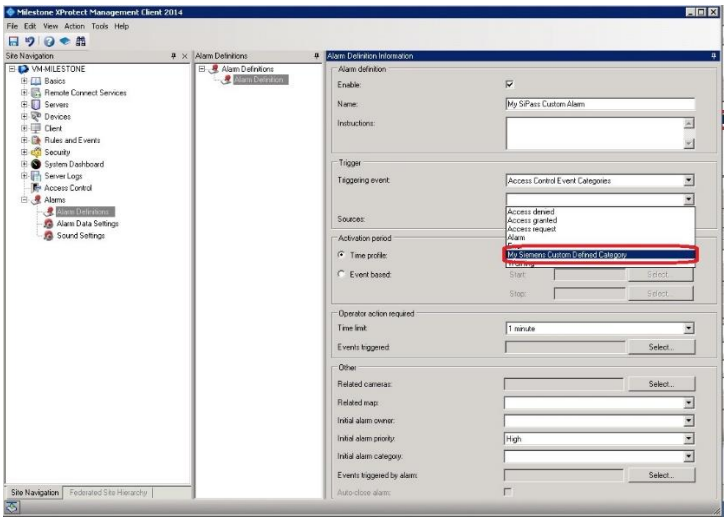
Save your changes and move to the Alarm Definitions section to create an alarm based on that user-defined event category.



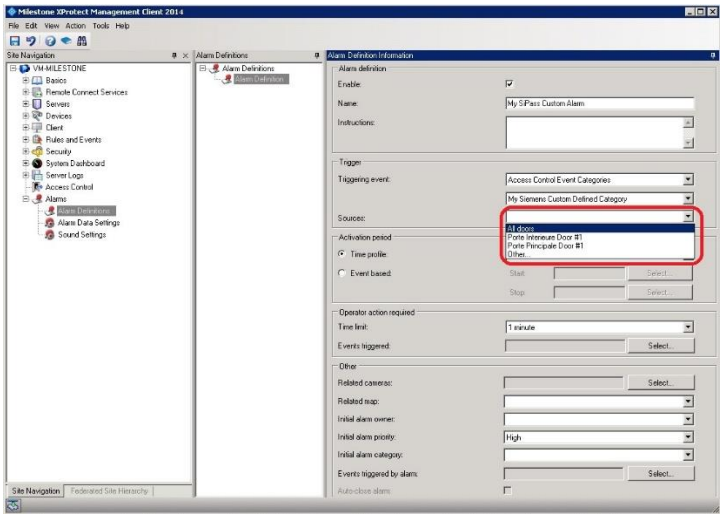
Name the alarm a pertinent name and select Access Control Event Categories in the Triggering event dropdown:



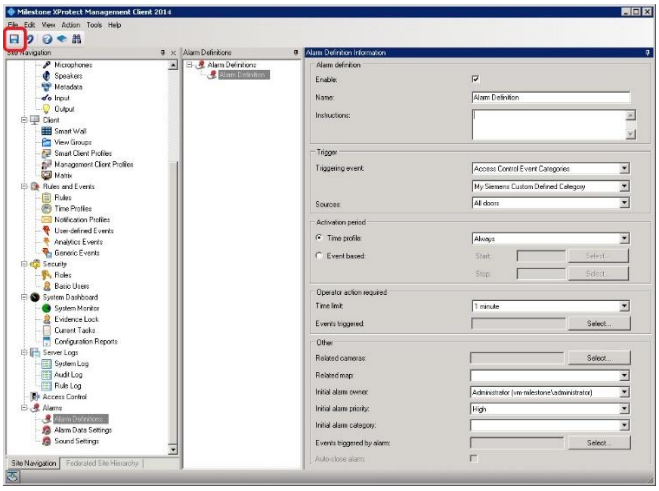
Select the new user-defined event category that was defined earlier:



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



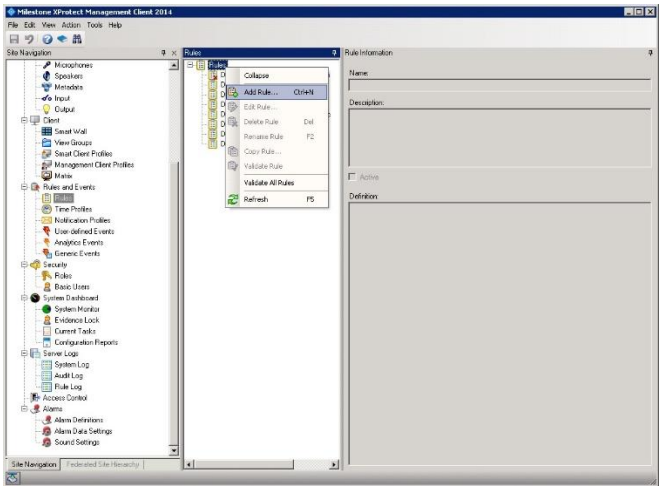
Select all the other alarm parameters and save:



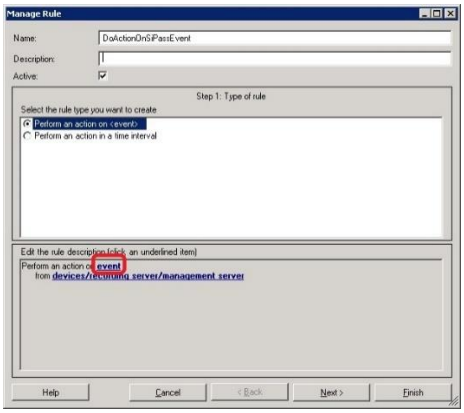
Alarms acknowledged in Milestone are not acknowledged in Lenel as there is no direct correspondence between them.

Defining Rules based on Lenel events

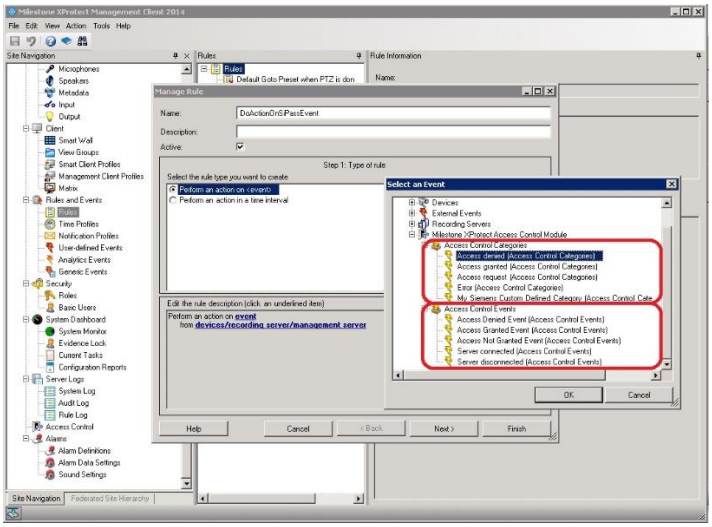
To define rules in Milestone based on Lenel events, create a rule in the Rules tab:



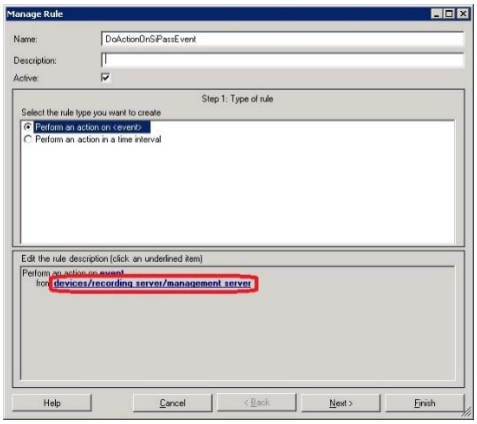
Select the event hyperlink:

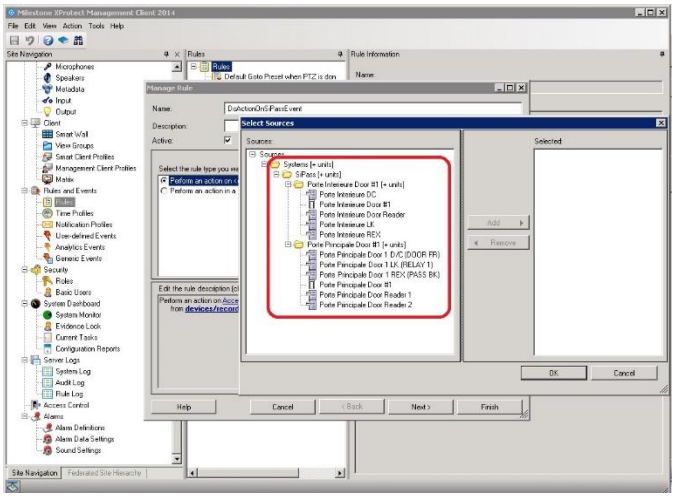


Select an event category or event from the Select an Event dialog:

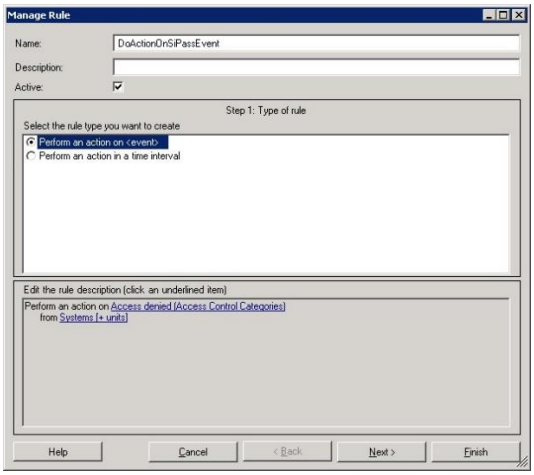


Select the devices/recording server/management server hyperlink and select the event source. To select any source select the System (+units) node.

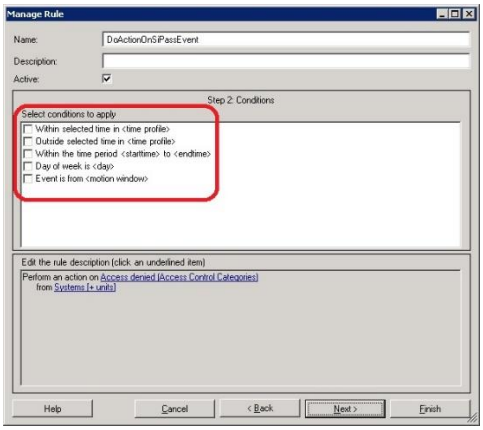




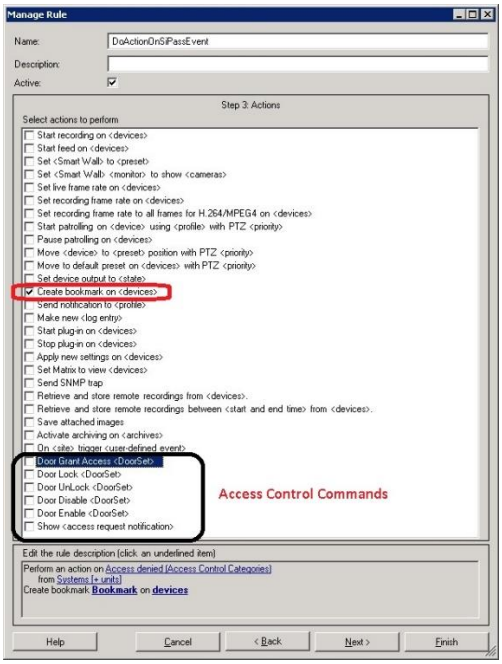
The wizard will look like this after selecting the “Access Denied” event and System (+ units) source:



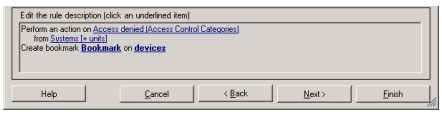
Press next and select the optional time frame when the action will take place. In this example no time frame has been selected, this means it will always execute.

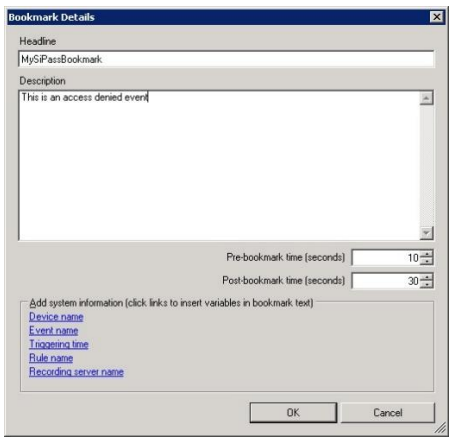


Select the action that will be executed when the Lenel event occurs. Notice that AC commands can be used as actions based on any events that come into Milestone:

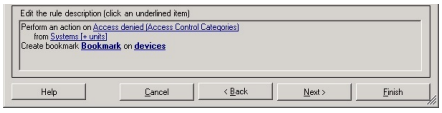


In this example “create bookmark on <device>” will be selected, click the Bookmark hyperlink and the following dialog will be displayed to setup the bookmark action:

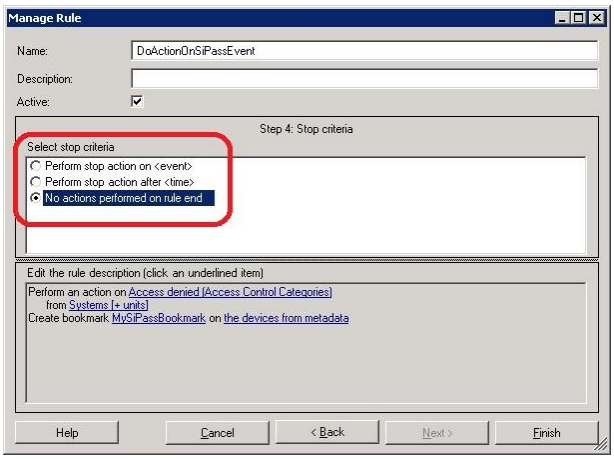




Click the devices hyperlink and select the device on which the bookmark will be applied:



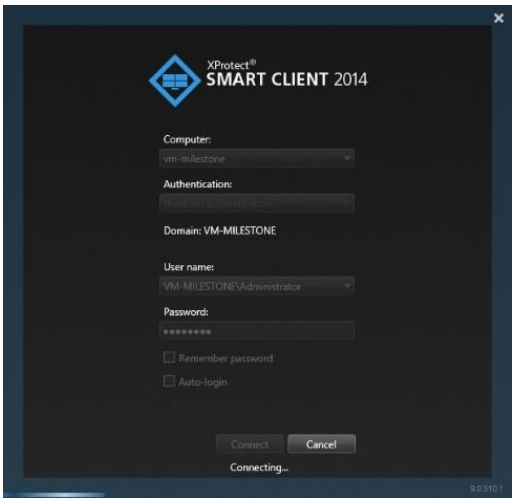
Click next on the rule wizard and select an optional stop criteria, in this example there is no stop criteria.

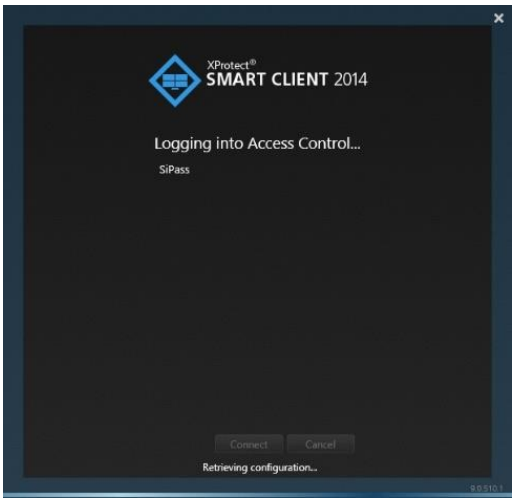


Click finish and the rule is set.

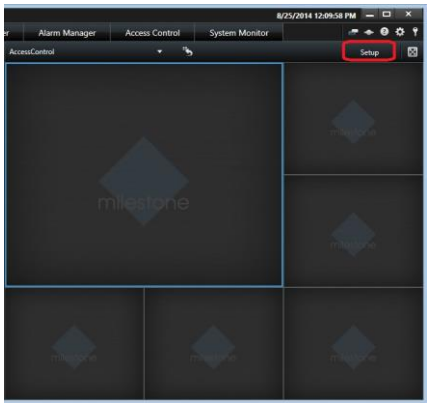
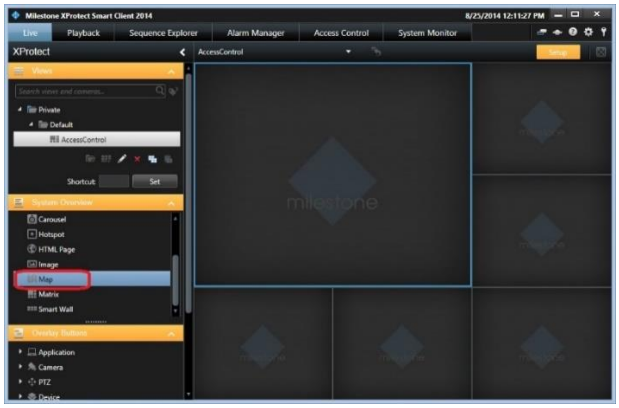
Smart Client Maps

It is possible to put doors and Lenel 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:

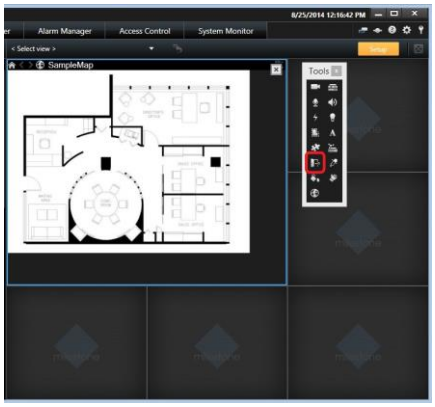
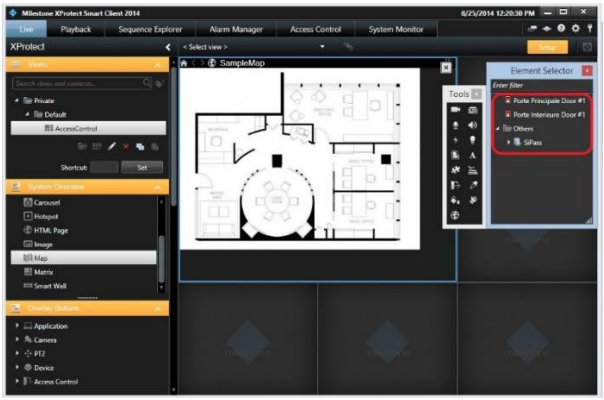




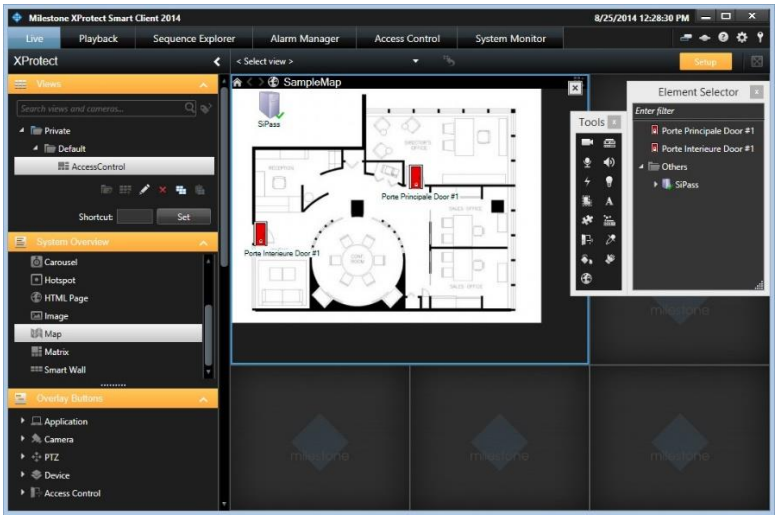
Use an existing view, go into setup mode by pressing the setup button in red below and create a map by dragging it onto a tile once in setup mode.

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

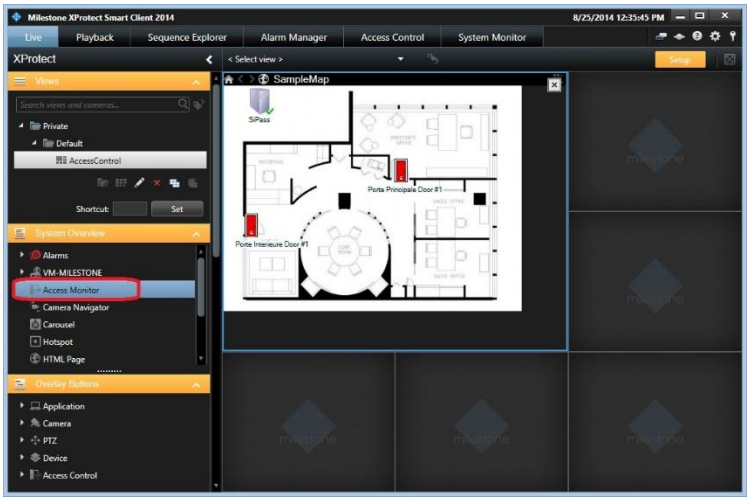



The finalized map with the doors and server added in this example will look like this:



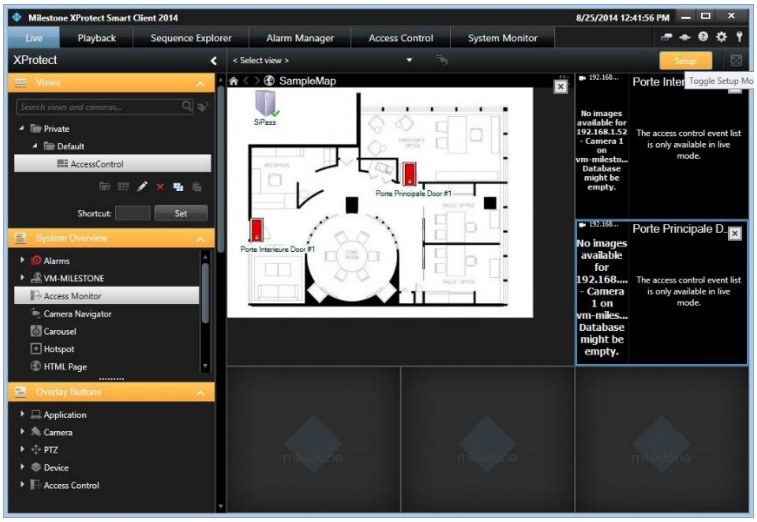
Access Monitor Tiles

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:



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 LS Communication Server service is not running (or needs to be restarted).

Failure of the ACM plugin to communicate with Windows 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 Directory that is configured for single signon. See Configure Lenel OnGuard for Single Sign-On and ACM Server: Configure to RunAs Lenel Single-Signon 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 to the ACM Server

When the system is properly running, the Milestone Event Server MIP plugin “pings” the Lenel 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 installation.

Not seeing hardware or events from a segment

If not seeing some hardware or events from some segment, ensure the single signon user is configured in Lenel to have access to the necessary segments.

Logging

By default the debug logs are enabled on both the milestone event server plugin and the Lenel 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\ACMServerPlugin**, 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 Server side

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

1. On the Lenel 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 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.
    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

Known issues

- Alarm acknowledgement from XProtect to Lenel is not implemented.
- This ACM integration was only tested against the MIP SDK 2016.
- The ACM integration is currently coded to only work with a Lenel 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.

Milestone Systems offices are located across the world. For details about office addresses, phone and fax numbers, visit www.milestonesys.com.

milestone

The Open Platform Company