



Lenel OnGuard Access Control Module (ACM) Integration User Manual V2.0



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

TARGET AUDIENCE FOR THIS DOCUMENT	2
CONTENTS	3
COPYRIGHT, TRADEMARKS & DISCLAIMERS	5
REVISIONS	6
SCALABILITY TESTING	7
NUMBERS OF DEVICES	7
PHYSICAL HARDWARE	7
SOFTWARE TESTED AGAINST	7
EVENTS HANDLED	7
GENERAL DESCRIPTION	9
INTRODUCTION	9
SOLUTION OVERVIEW	9
TERMINOLOGY	9
PREREQUISITES	10
CONFIGURE LENEL ONGUARD FOR SINGLE SIGN-ON	11
CONFIGURE LENEL ONGUARD TO GENERATE SOFTWARE EVENTS	15
CONFIGURE SQL SERVER FOR CONNECTIONS	15
INSTALLATION	17
ACM SERVER	17
ACM SERVER: LENEL-ONGUARD PLUGIN	20
ACM SERVER: XPROTECT ACM MIP PLUGIN	25
MIP PLUGIN UPGRADES	27
CONFIGURATION	29
ACM SERVER: CONFIGURE TO RUN AS LENEL SINGLE-SIGNON ACCOUNT	29
REDUCING PERMISSIONS	31
ACM SERVER: XPROTECT ACM MIP PLUGIN	31
INSTALLING AN ACM SERVER	32
UNINSTALLING AN ACM SERVER	36
MILESTONE MANAGEMENT CLIENT CONFIGURATION	37
REDUCING PERMISSIONS	41
EDITING LENEL EVENT TYPES	41

OPERATIONS	43
SEARCHING FOR CARDHOLDERS	43
DEFINING ALARMS BASED ON LENEL EVENTS	43
DEFINING RULES BASED ON LENEL EVENTS	46
SMART CLIENT MAPS	49
ACCESS MONITOR TILES	50
ALARM ACKNOWLEDGMENT	51
TROUBLESHOOTING GUIDE	53
LENEL ONGUARD LOSES COMMUNICATION WITH THE ACCESS CONTROL HARDWARE	53
FAILURE OF THE ACM PLUGIN TO COMMUNICATE WITH WINDOWS MANAGEMENT INTERFACE (WMI)	53
MILESTONE EVENT SERVER MIP PLUGIN CANNOT COMMUNICATE TO THE ACM SERVER	53
DEBUG LOG SHOWS SQLACCESS.CONNECT() FAILED.	53
FAILURE TO CONNECT TO SQL SERVER	54
NOT RECEIVING CARD HOLDER OR BADGE CHANGES	54
OPTIMIZING EVENT PROCESSING PERFORMANCE	54
LOGGING	55
GATHERING THE LOGS	55
CHANGING LOGGING LEVEL	55
KNOWN ISSUES	57
EVENTS HANDLED	58
LENELFETCHEVENTTYPES UTILITY	58
EXAMPLE EVENT LIST	58

Copyright, Trademarks & Disclaimers

Copyright

© 2017 Milestone Systems A/S.

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
05/17/2017	2.0	Prerequisites, scalability, and troubleshooting sections updated. Some images updated.	Doug Beyer

Scalability Testing

The Lenel ACM integration has been tested against the following. Any customer exceeding the number of devices, using different hardware, or using different software versions 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

Software Tested Against

- The following XProtect versions are supported –
 - XProtect 2016 (all releases)
 - 2017 R2 (11.2a)
- The following minimum Lenel OnGuard versions are supported –
 - OnGuard 7.0 (7.0.1107)
 - OnGuard 7.1 (7.1.481.74)
 - OnGuard 7.2 (7.2.269.67)
 - OnGuard 7.3 (7.3.345).

Events Handled

See the [Events Handled](#) section.

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.

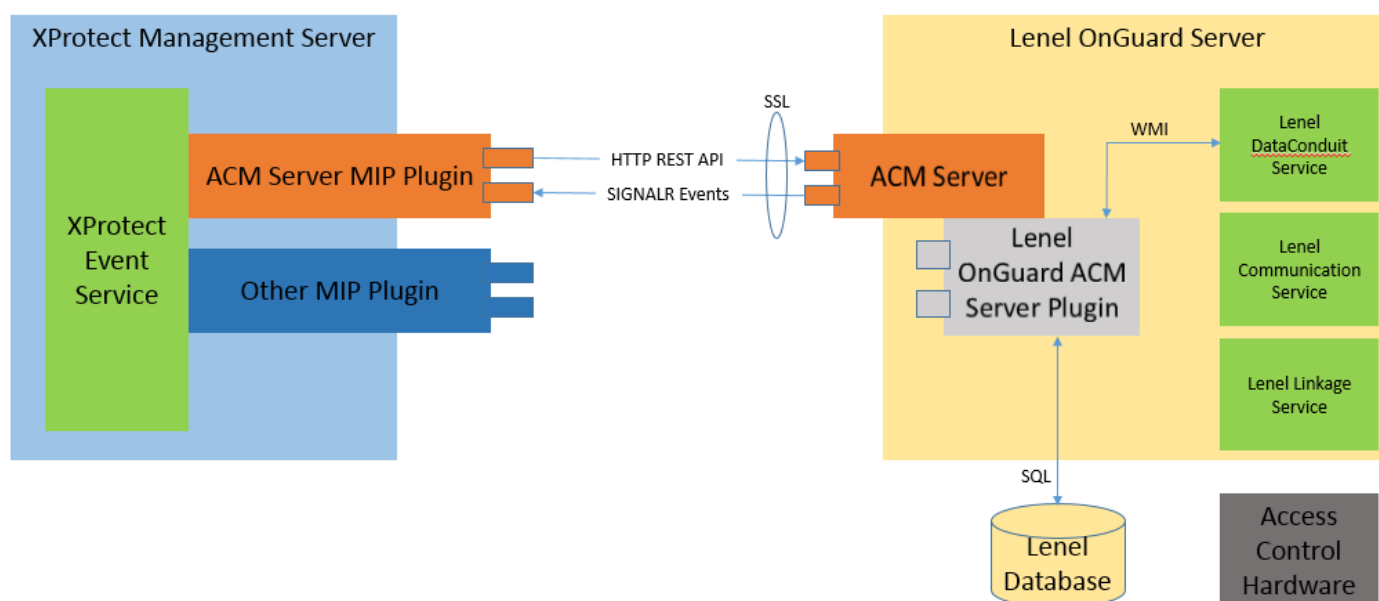
This integration supports the following standard ACM features:

- 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)
- Create alarms in alarm manager based on AC events.
- Alarm acknowledgment from XProtect (2016 R3 or greater) to Lenel. Alarm acknowledgment from Lenel to XProtect is not implemented due to the lack of such functionality in Lenel.
- 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



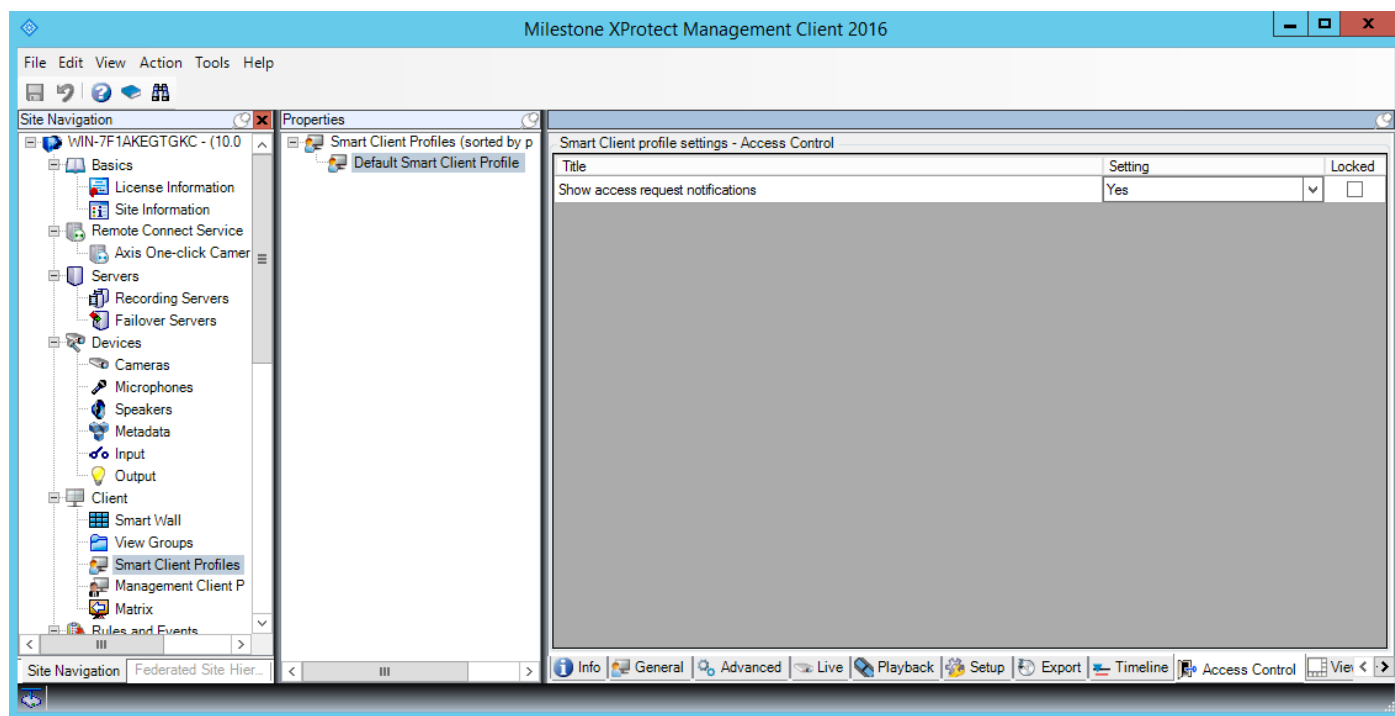
Terminology

- Legacy plugin – Refers to Lenel OnGuard plugins with version numbers <= 1.0.16354, dated approximately 12/19/2016.

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.
 - It is *essential* that the same version of the Lenel ACM integration be installed on both the XProtect and Lenel machines.
- The Lenel AC System
 - 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.
 - The following minimum Lenel OnGuard versions are supported - OnGuard 7.0 (7.0.1107), OnGuard 7.1 (7.1.481.74), OnGuard 7.2 (7.2.269.67), and OnGuard 7.3 (7.3.345).
 - 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](#) 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

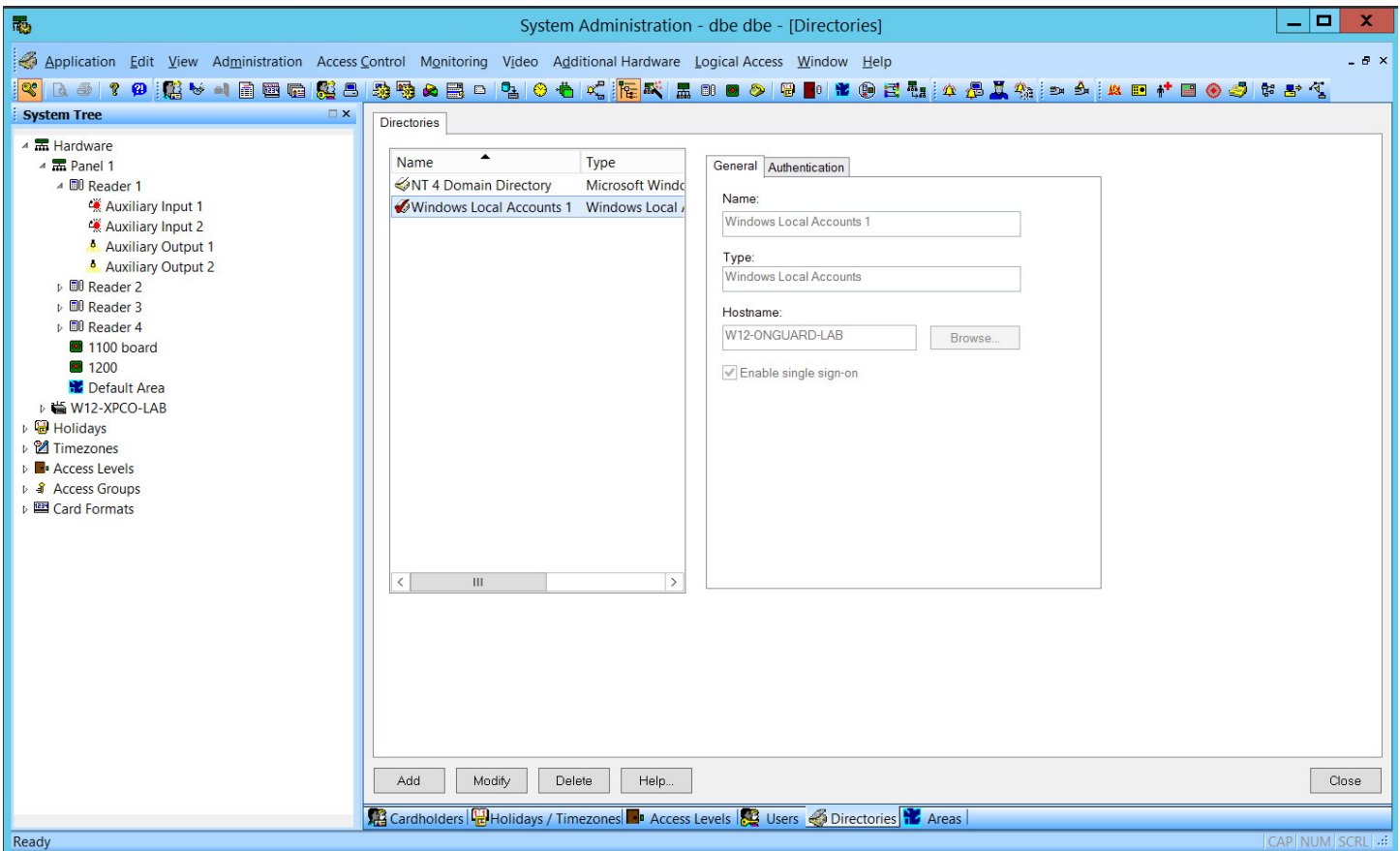
The default Smart Client profile does have these rights as shown below:



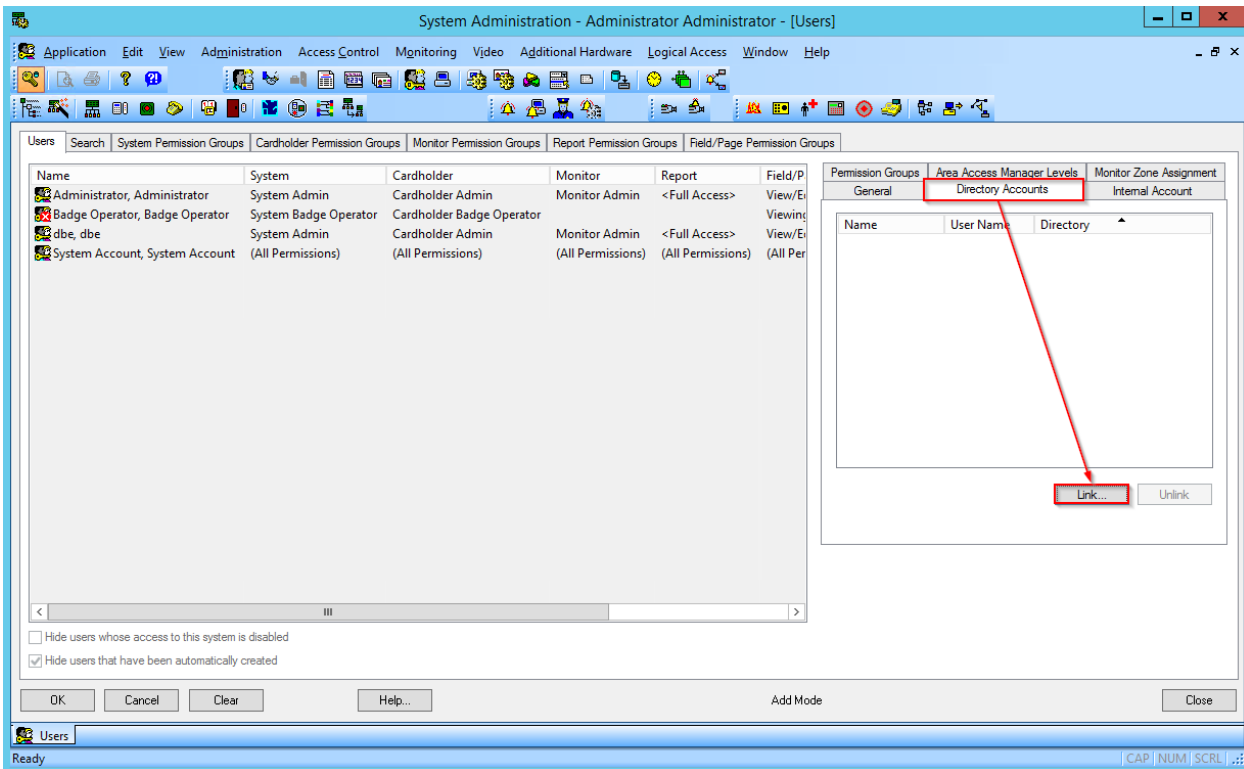
Configure Lenel OnGuard for Single Sign-On

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

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), then ensure that the user is a member of the Local Administrators group on the Lenel OnGuard server.

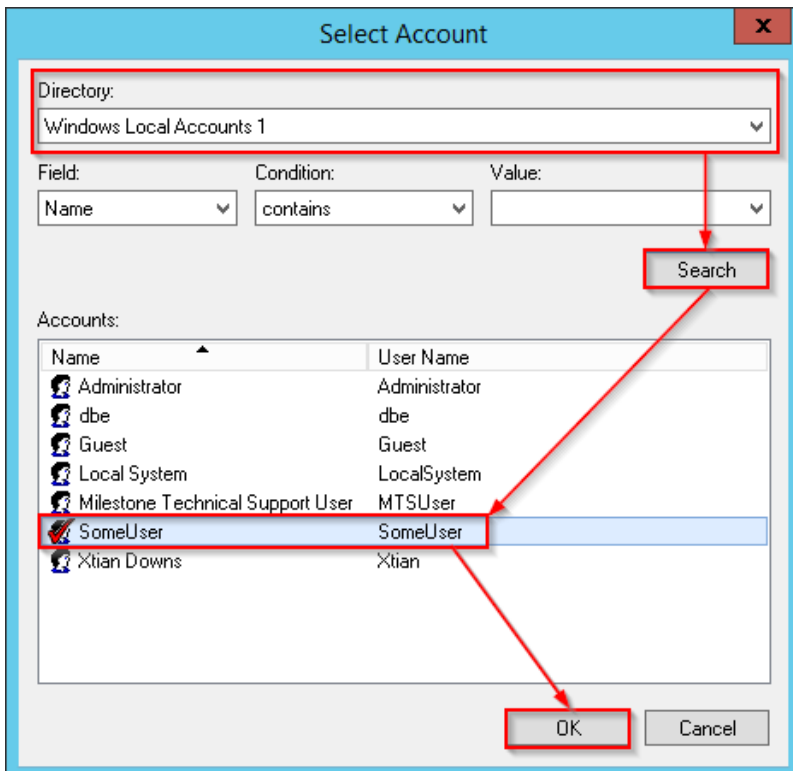


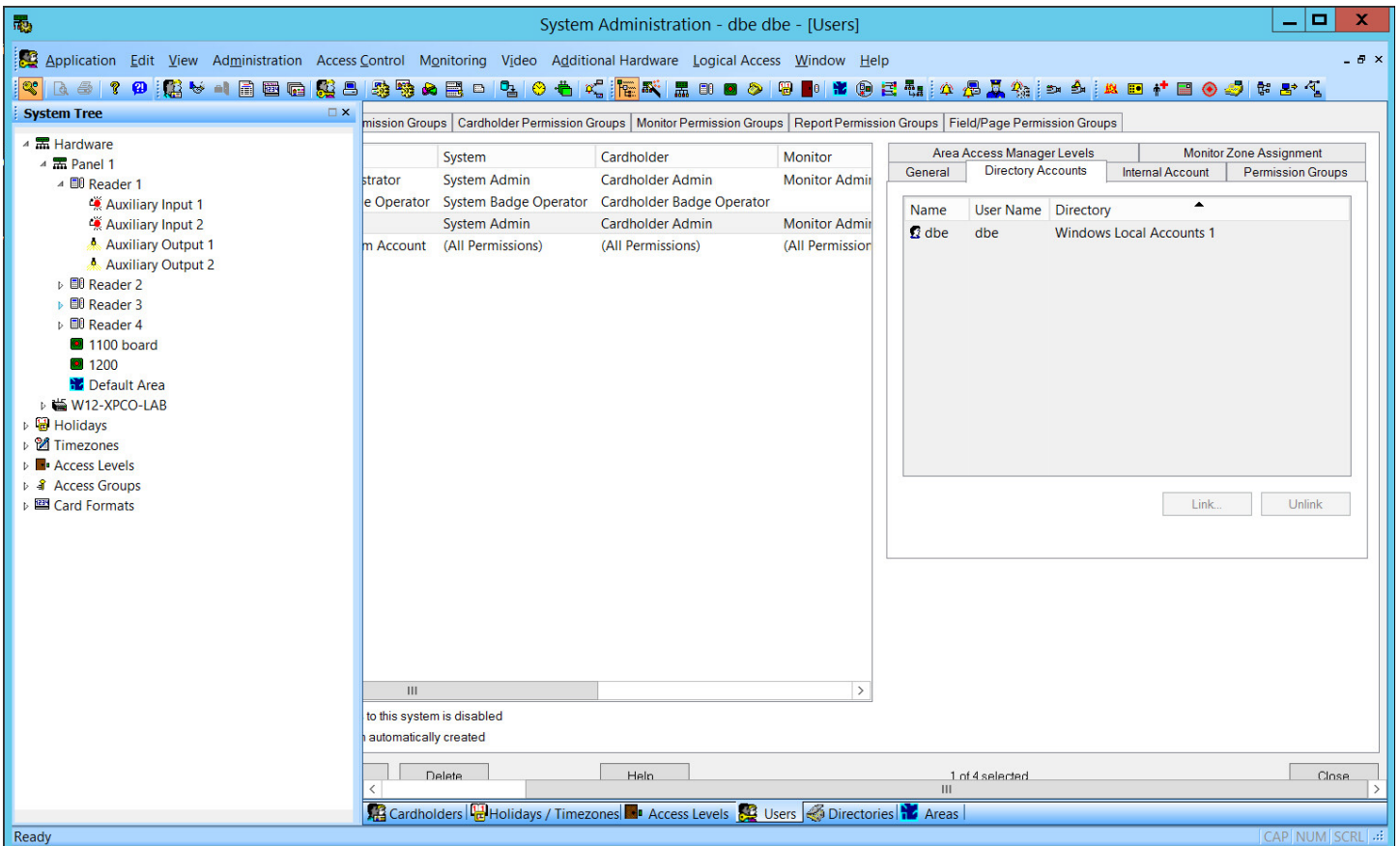
- b. Click Administration + Users
 - i. Add a new user.
 1. General tab
 - a. Give the user some name.
 - i. Both first and last names are required but they can be same string if the last name isn't logically required.
 - ii. I believe the values of the first and last names are immaterial with respect 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.



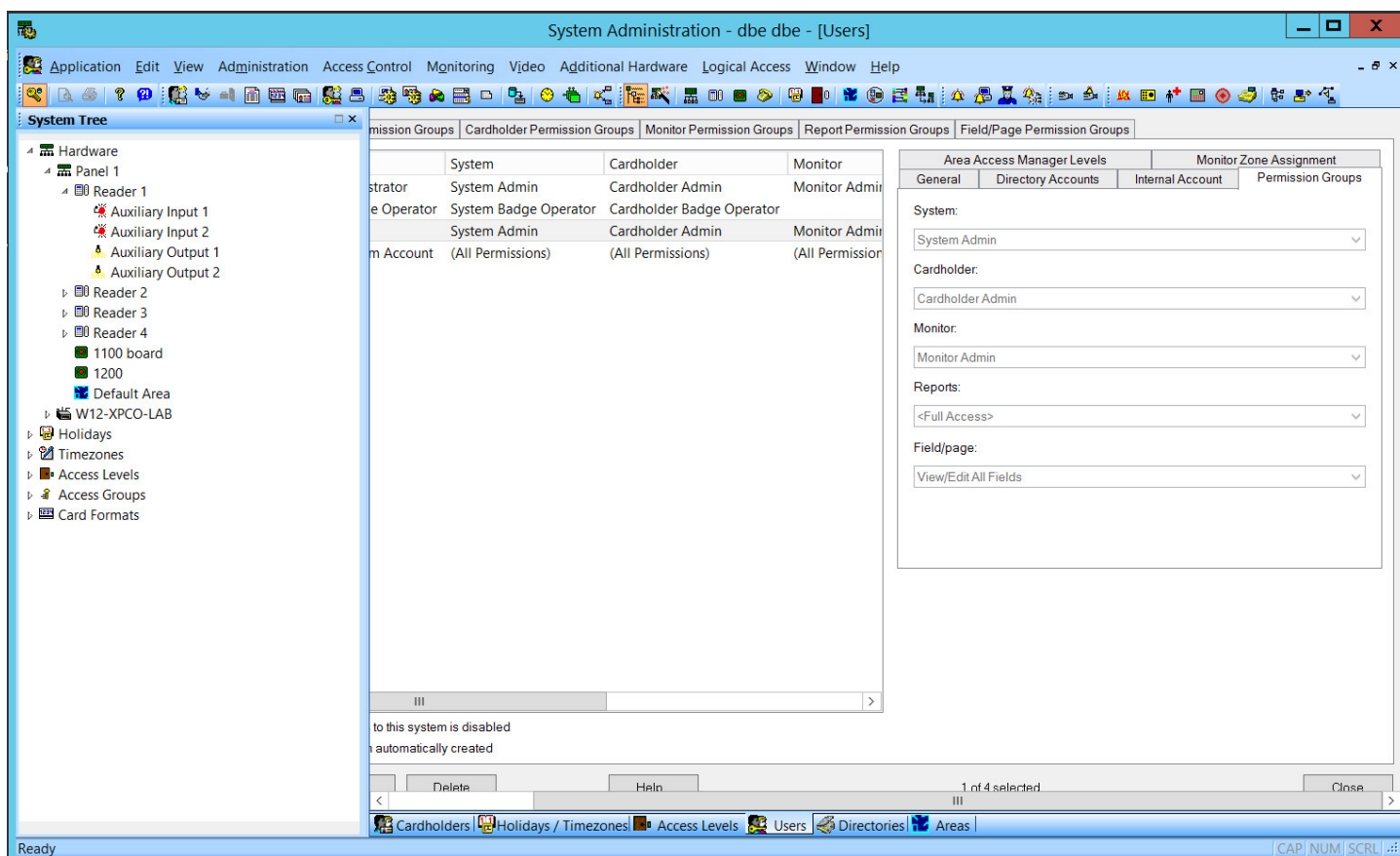


3. Internal Account tab

- We tested the integration using both valid 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.
- The "User has internal account" checkbox defaults to being checked. It's sufficient to leave it checked.
- Enter login credentials.
 - 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

- Assign the following permission groups:
 - System = System Admin
 - Cardholder = Cardholder Admin
 - Monitor = Monitor Admin
 - Reports = Full Access
 - 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.

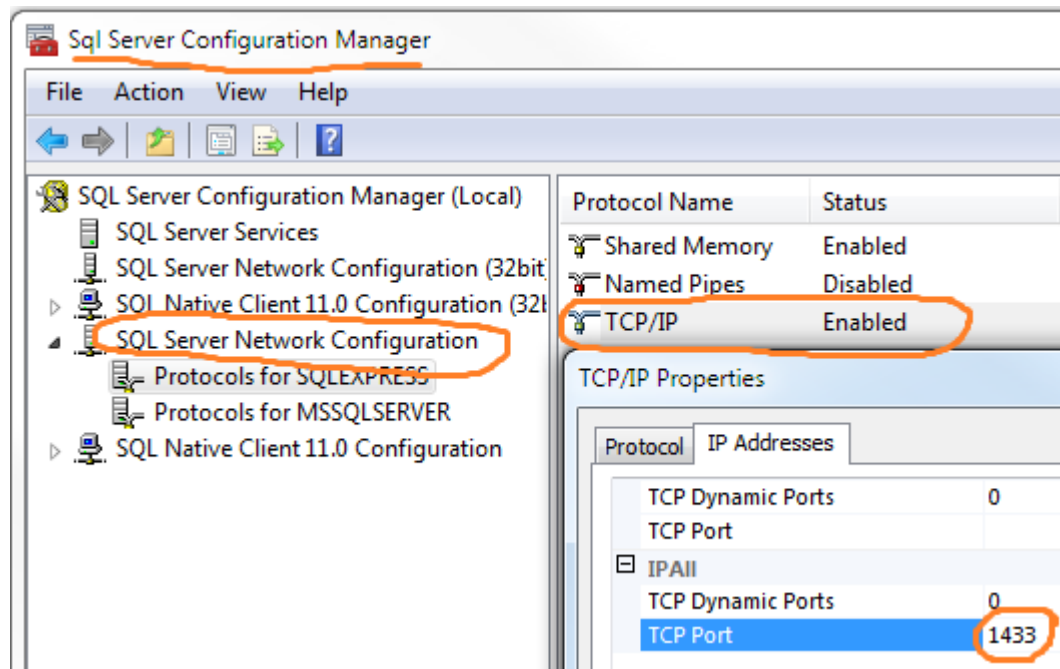
Configure SQL Server for Connections

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 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.

Installation

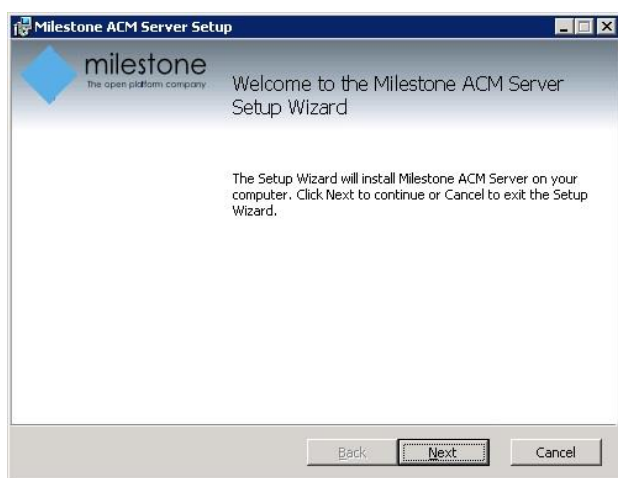
It is *essential* that the same version of the Lenel ACM integration be installed on both the XProtect and Lenel machines.

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

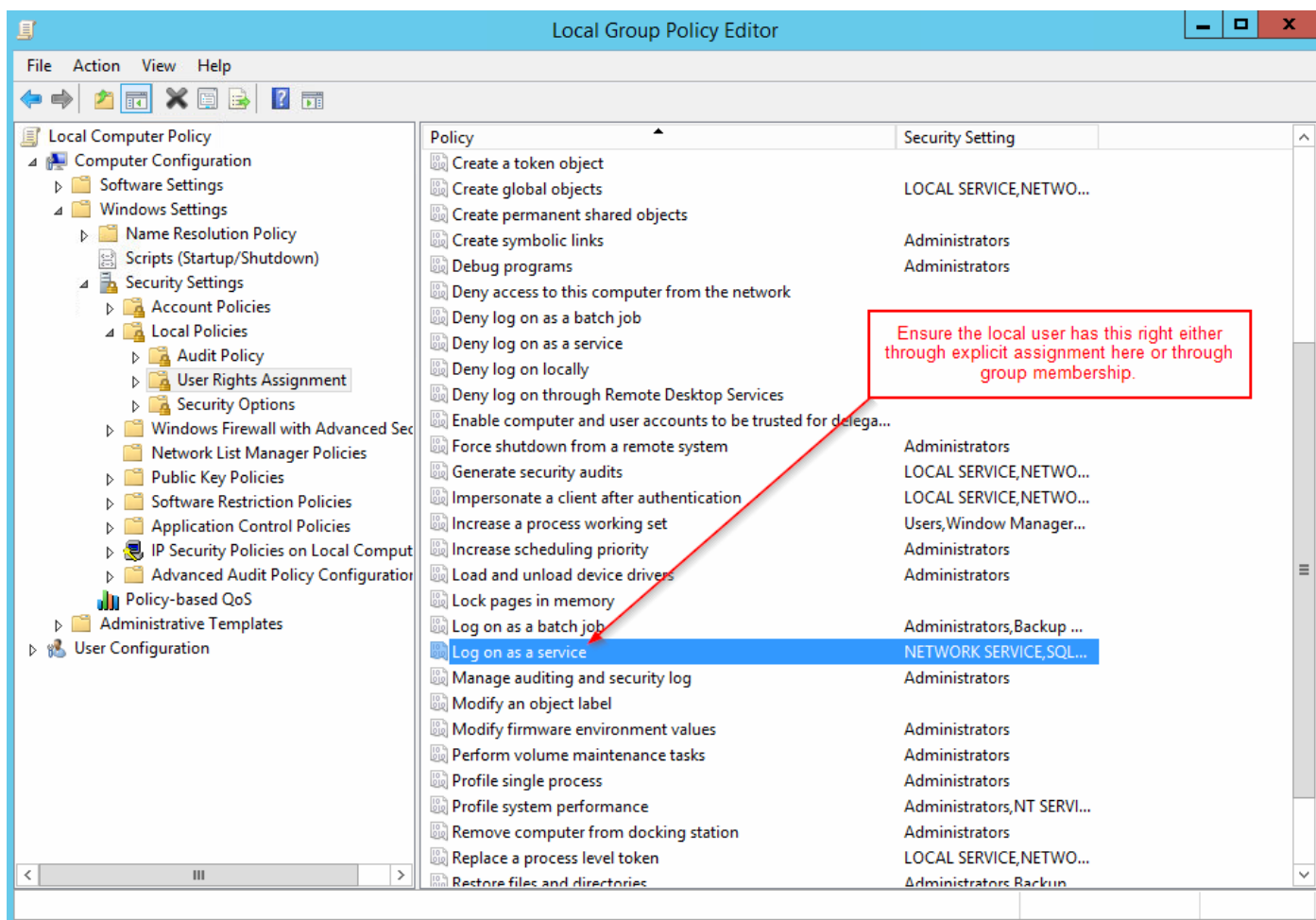
- 1) Install the pre-requisites on the Lenel server machine
 - a) .NET Framework 4.5
- 2) Milestone.ACMServer.msi: Installer for the [ACM Server](#)
 - a) **Must be installed on the Lenel server machine**
- 3) Milestone.ACMServer.LenelOnGuard.msi: Installer for the [Lenel-OnGuard ACM Server plugin](#)
 - 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:



In the next dialog, 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 [Configure Lenel OnGuard for Single Sign-On](#)). This user must have the “Log on as a service” right in Windows (see the following image). Do not leave the fields blank. WMI integration will not work if the ACM Server is running as the Local System Account. Do not prefix the user name with the machine name or “.” (e.g. machineName\userName, .\userName).



The screenshot shows the 'Milestone ACM Server Setup' window. The 'ACM Server RunAs Credentials' section is active, displaying the text 'Enter the credentials for the ACM Server to run as'. Below this, there is a checkbox for 'Run as LocalSystem' which is unchecked. There are four input fields: 'Domain:' with the value 'CDO-ONGUARD72', 'User Name:' with the value 'administrator', 'Password:' with masked characters, and 'Confirm Password:' with masked characters. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

ACM Server RunAs Credentials
Enter the credentials for the ACM Server to run as

☐ Run as LocalSystem

Domain: CDO-ONGUARD72

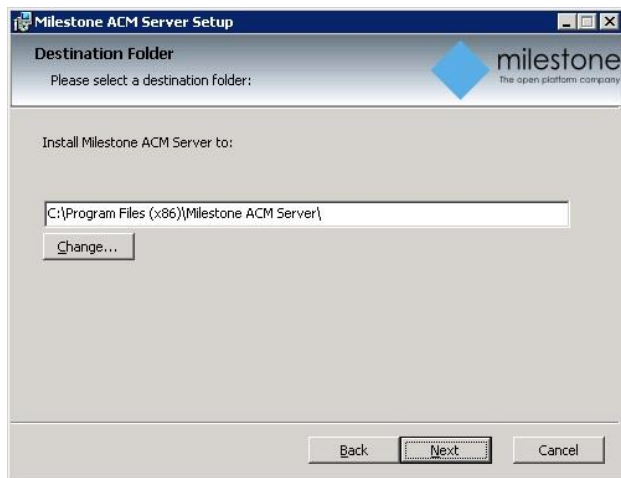
User Name: administrator

Password: ●●●●●●●●

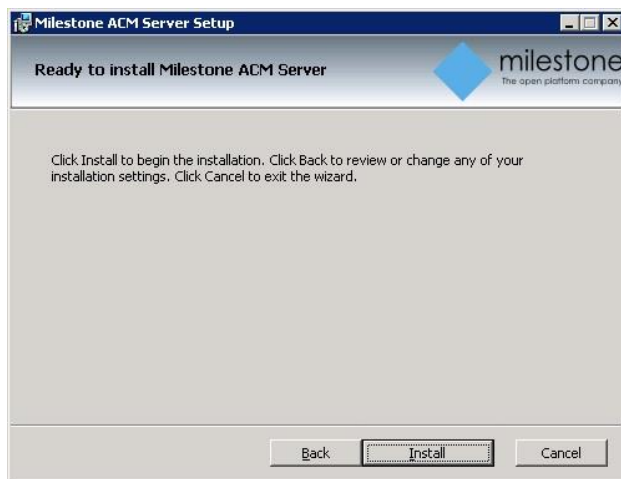
Confirm Password: ●●●●●●●●

Back Next Cancel

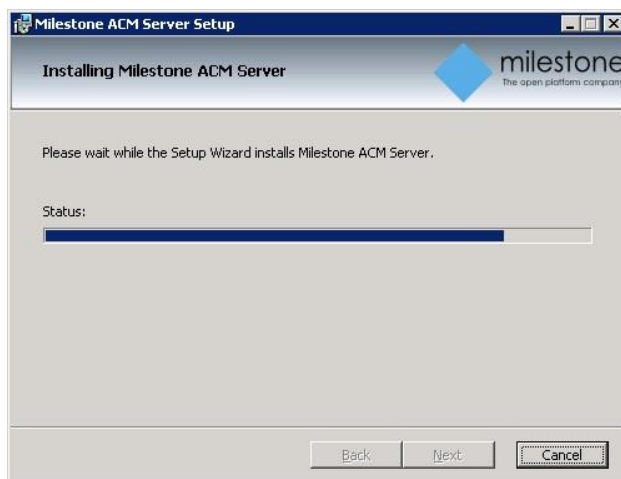
Press next and you will now be able to select the installation path, it is recommended to use the default as displayed:



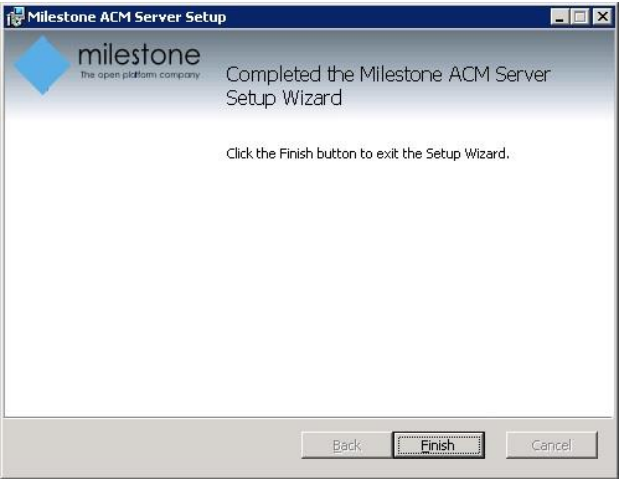
Press next and you are now ready to install, if you are satisfied with the selected options, press install to continue:



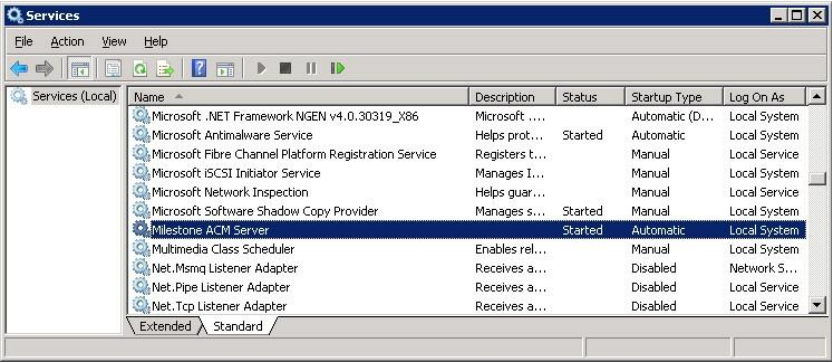
Install progress...



You have successfully installed the ACM Server:

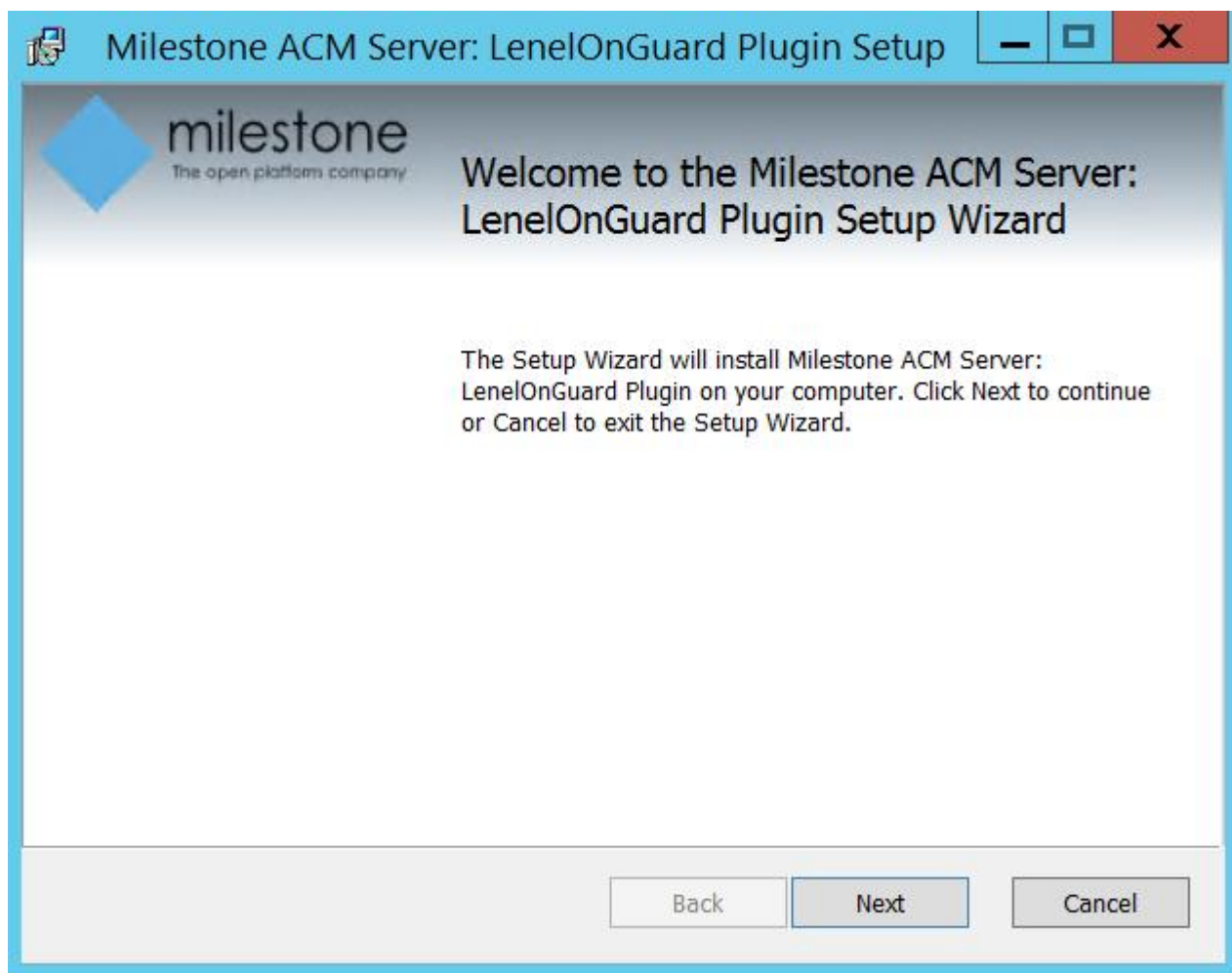


You can verify that the service installed successfully by looking in the Services control panel for a service named Milestone ACM Server.



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:

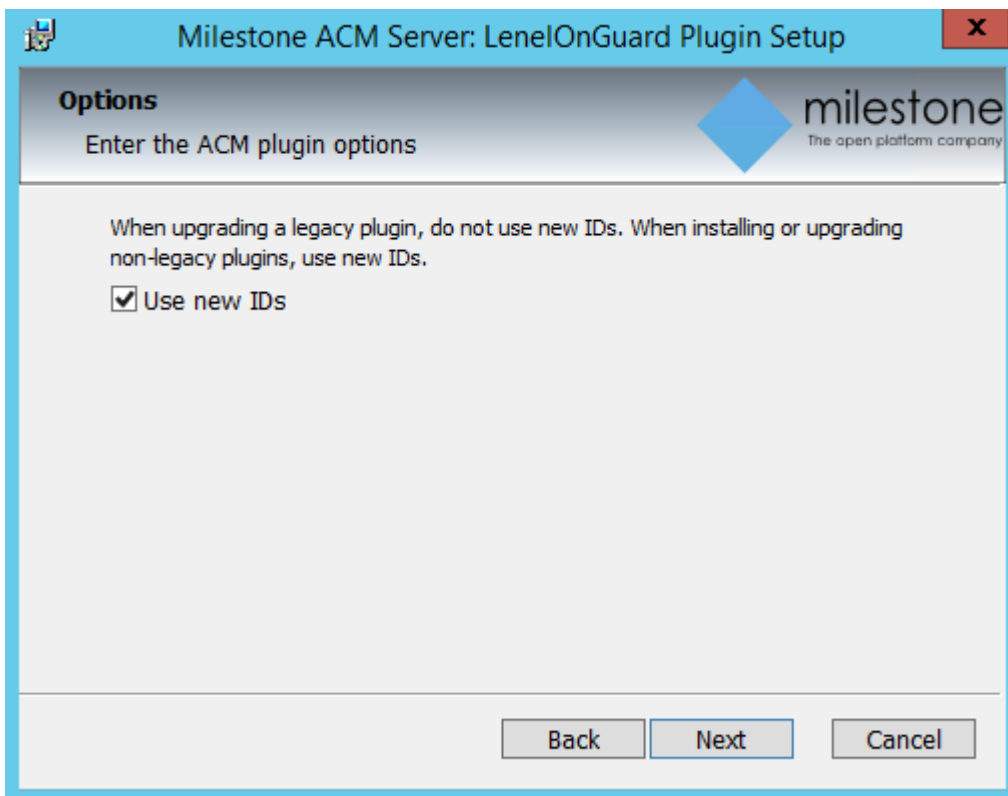


The Lenel-OnGuard plugin automatically detects the presence of both the Lenel server and the pre-installed ACM Server. If either is missing it will refuse to install.

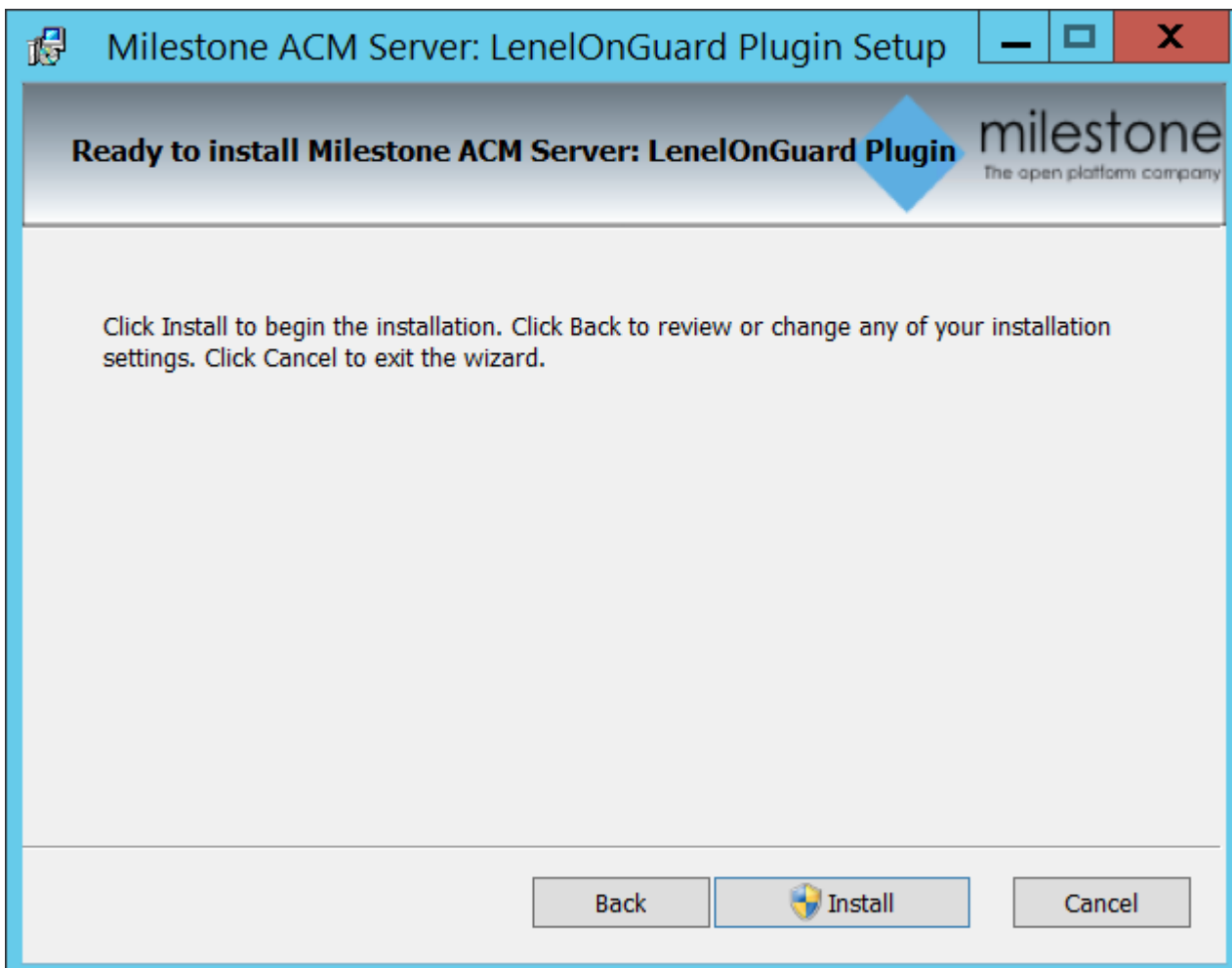
Press Next to go to the Options screen. Here is where you tell the plugin to provide ACM Server-scoped IDs (i.e. "Use new IDs") to XProtect, or not.

- If you are upgrading a legacy plugin, do not use new IDs. This is to ensure that the the upgraded plugin uses the same IDs already being used by XProtect for the Lenel panels, readers, card holders, etc.
- If you are installing a new plugin, or upgrading a non-legacy plugin, then use new IDs. This will ensure that the IDs are scoped to a particular ACM Server.

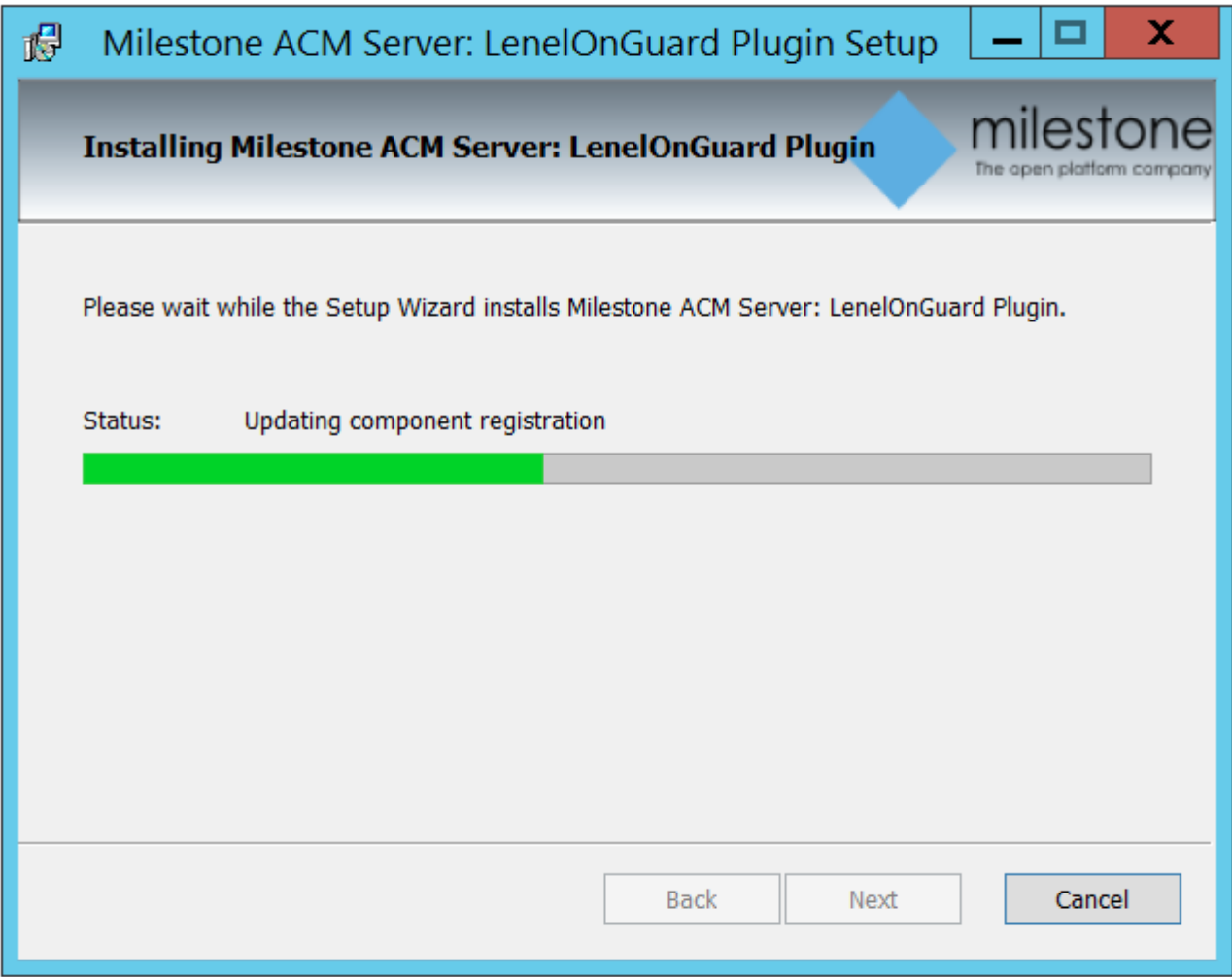
IMPORTANT – If using new IDs, then changing the Lenel server machine name after installing the plugin will break the plugin.



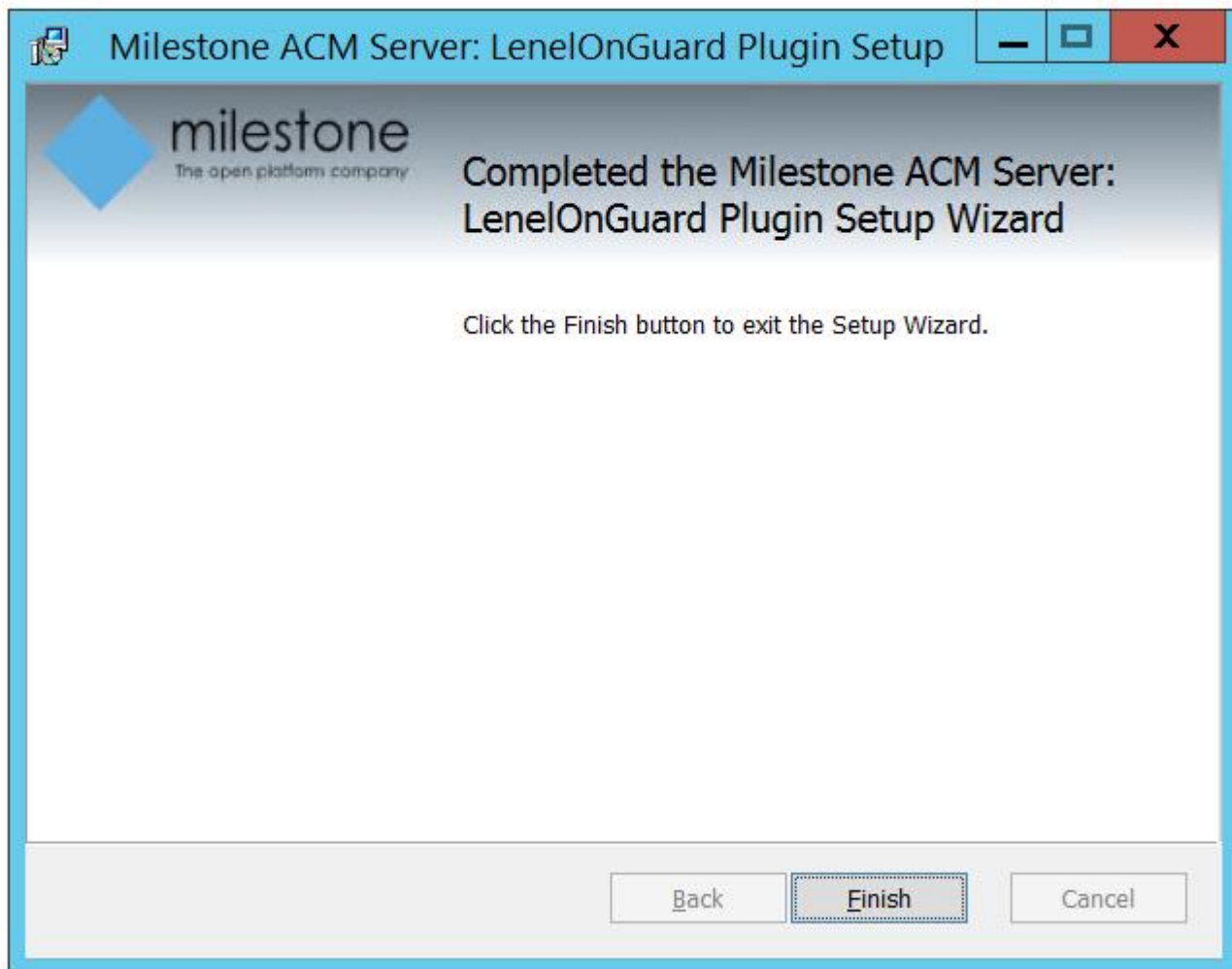
Press Next to go to the final screen. When you are ready, press install.



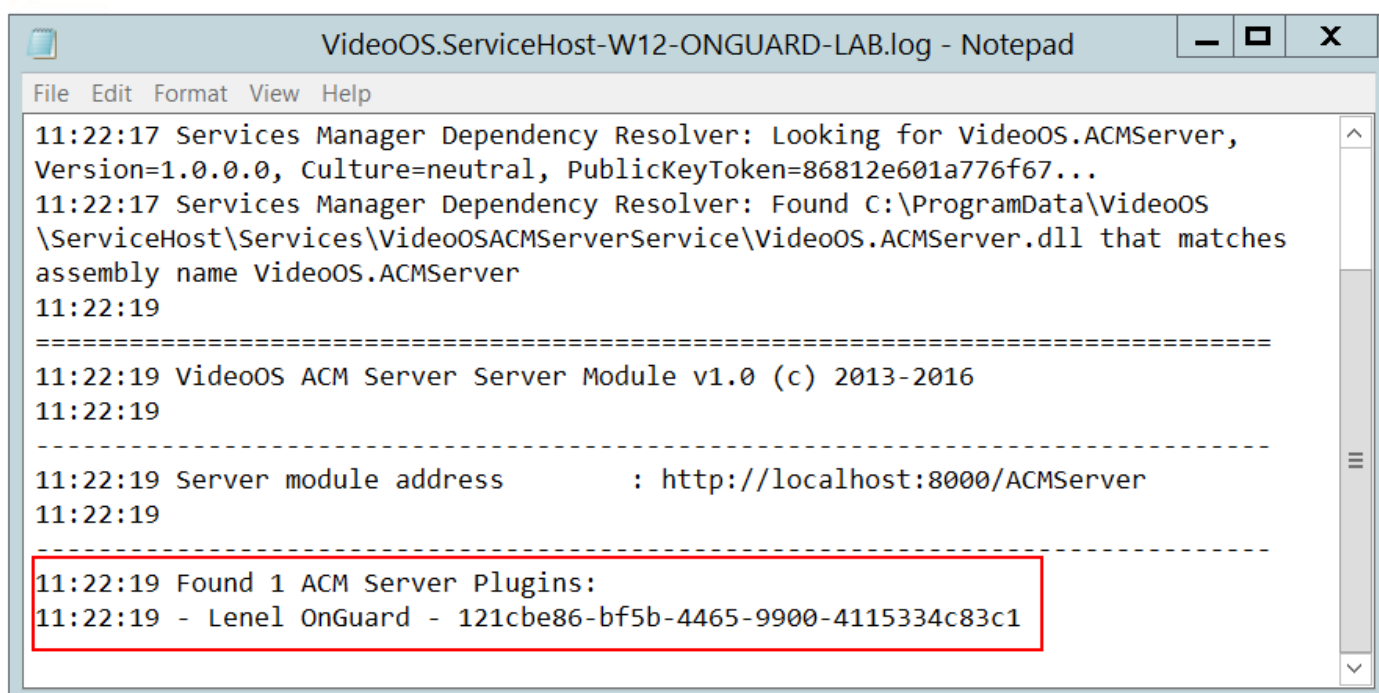
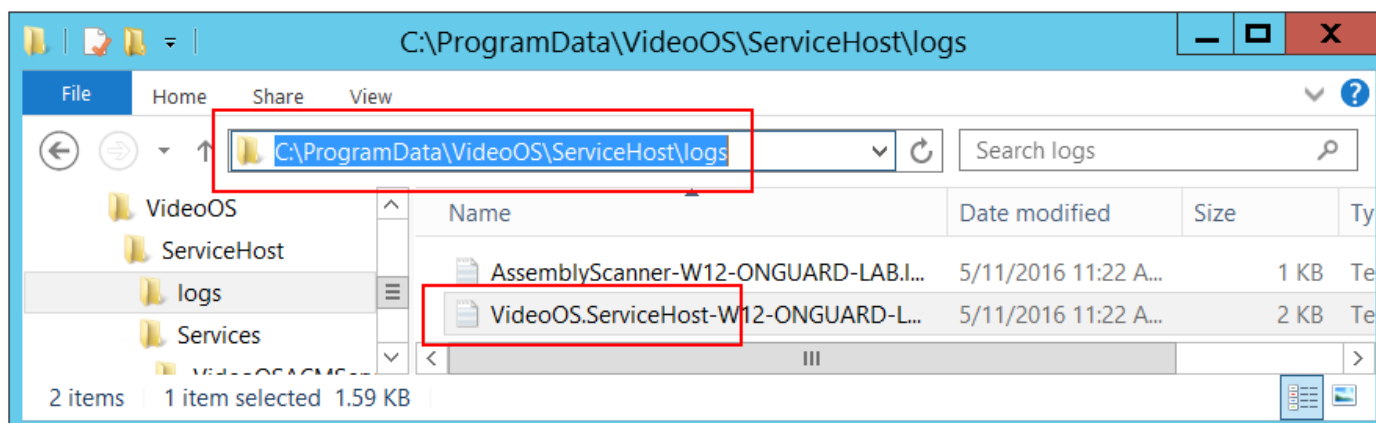
Install progress...



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

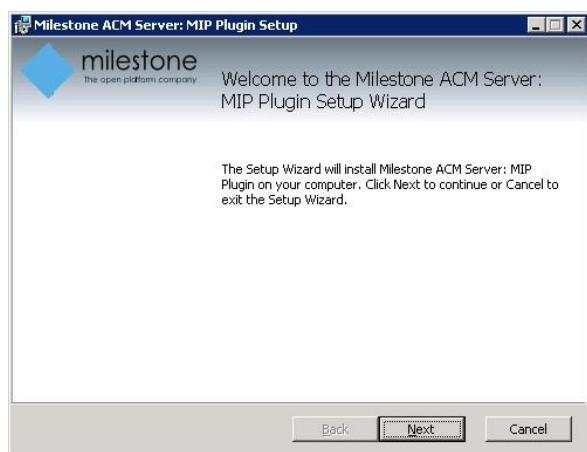


You can verify that the Lenel-OnGuard Plugin is installed and loaded from the logs below:

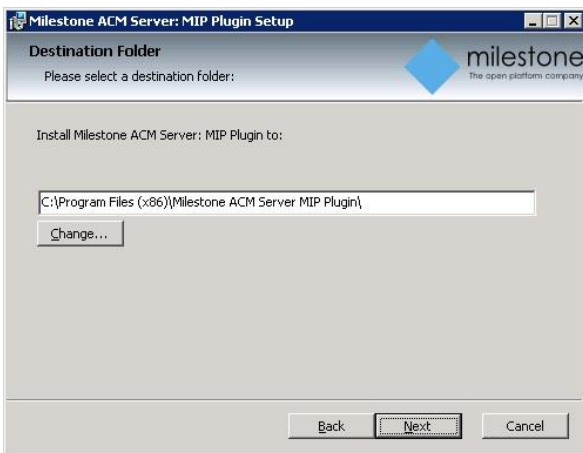


ACM Server: XProtect ACM MIP Plugin

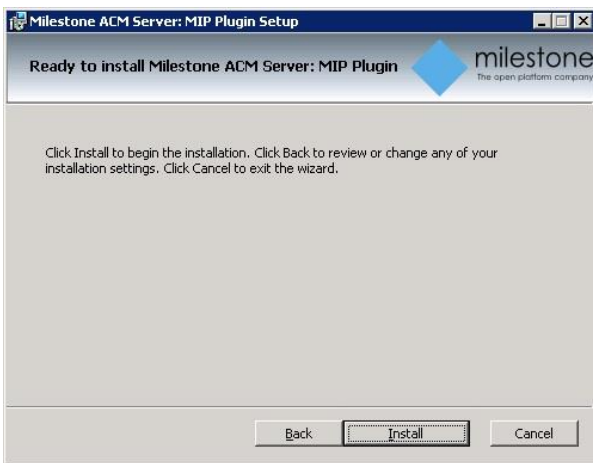
Copy the "Milestone.ACMServer.MipPlugin.msi" file to a temporary folder on the server where the XProtect Event Server is installed (in a typical deployment, this is the XProtect Management Server) and double-click to install. You should see a screen similar to the following:



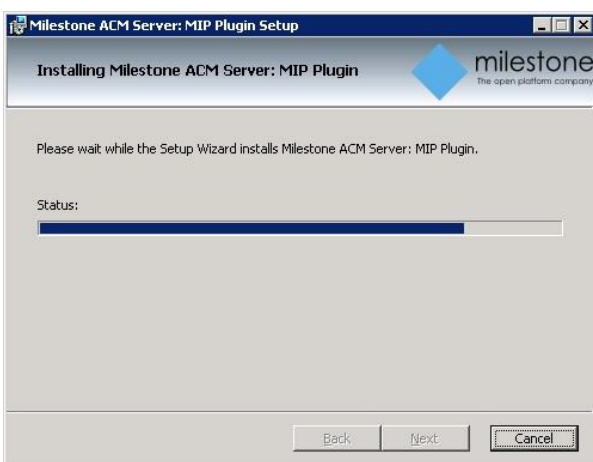
The installer will detect the presence of the XProtect Event Server on the machine and will refuse to install if it cannot be found. It is recommended to leave the default install path as displayed below and press next.



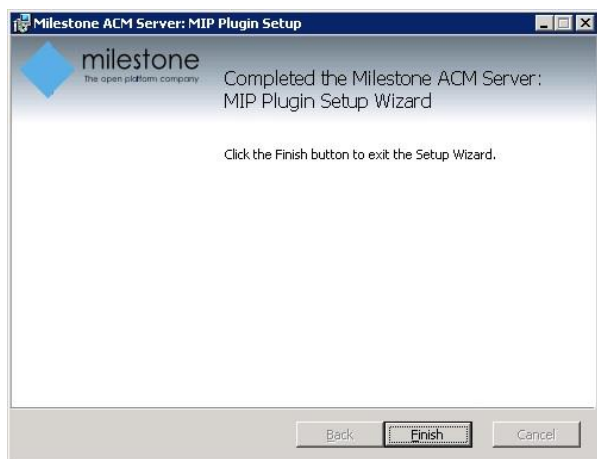
If you are satisfied with the path selection and you are ready to install press "Install"



Installation progress...

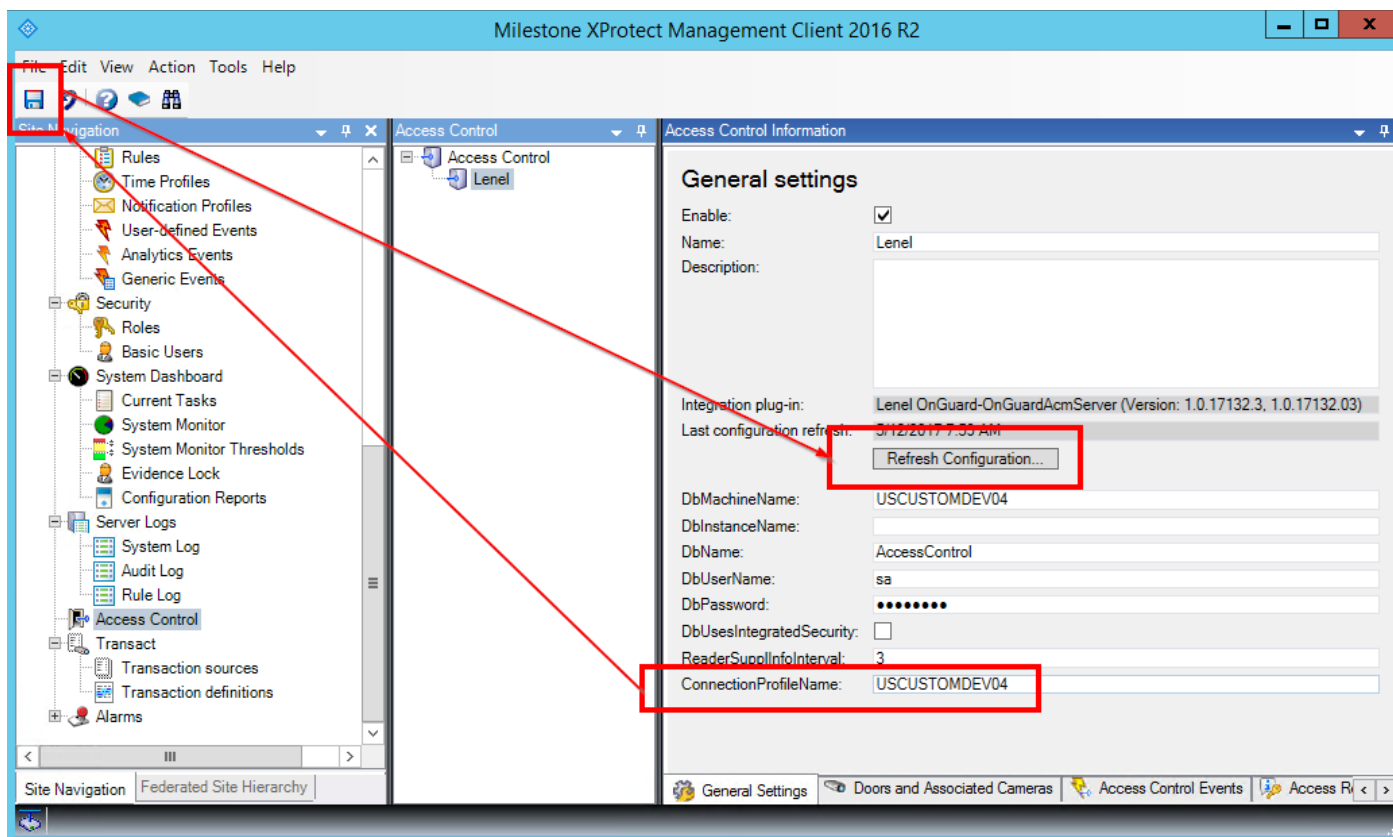


You have successfully installed the ACM MIP Plugin for ACM Server



MIP Plugin Upgrades

- **IMPORTANT – Always upgrade both the ACM Server and Lenel ACM plugin on the Lenel 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:
 1. Set the ConnectionProfileName property to the name of the ACM Server machine. Press Save to save the configuration change.
 2. Click Refresh Configuration to update the configuration.



- Upgrading will result in the following negative side-effects:
 - Smart Client event history will be lost.
 - Rules based off events and configured OnGuard hardware will no longer function. Rules based off the default access control event categories will not be affected and will continue to function.

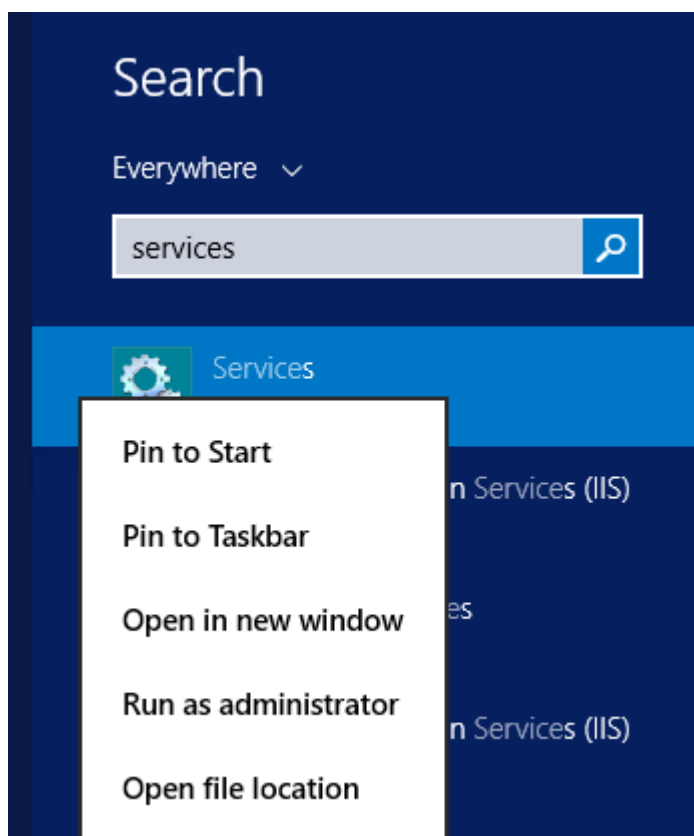
- Custom event category assignments will be lost. The custom category will still exist; the user will just have to re-assign the category to events in the Management Client.

Configuration

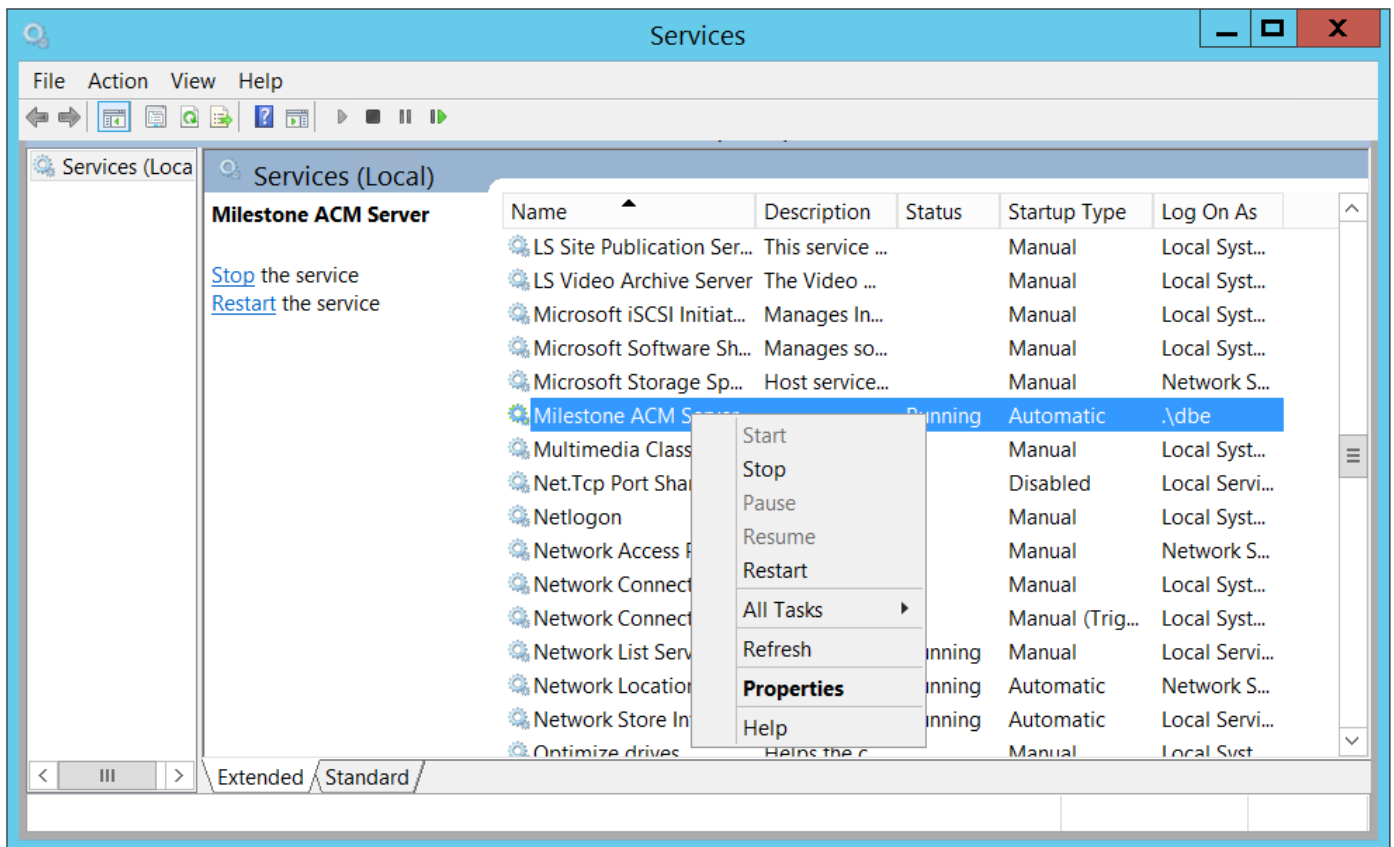
ACM Server: Configure to RunAs Lenel Single-Signon Account

The [Lenel-OnGuard Plugin installer](#) has already configured the ACM Server to run as the single-signon account. You only need to do the following if you need to change the ACM Server's credentials.

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).

The screenshot shows the 'Milestone ACM Server Properties (Local Computer)' dialog box with the 'Log On' tab selected. The 'Log on as:' section has two radio buttons: 'Local System account' (unselected) and 'This account:' (selected). Below 'Local System account' is a checkbox for 'Allow service to interact with desktop'. The 'This account:' section has a text box containing '.\dbe' and a 'Browse...' button. Below this are two password fields labeled 'Password:' and 'Confirm password:', both containing masked characters (dots). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

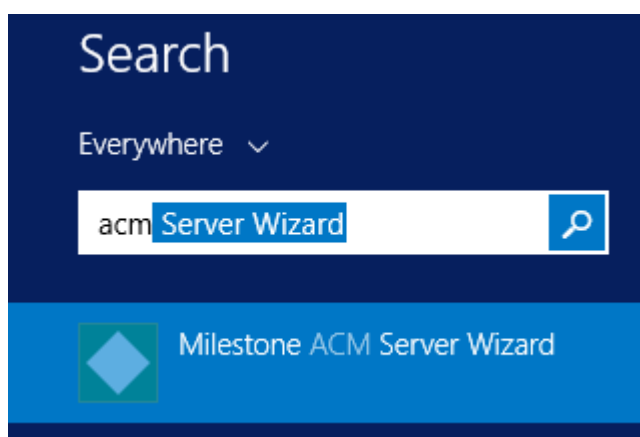
IMPORTANT: Restart the Milestone ACM Server service.

Reducing Permissions

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

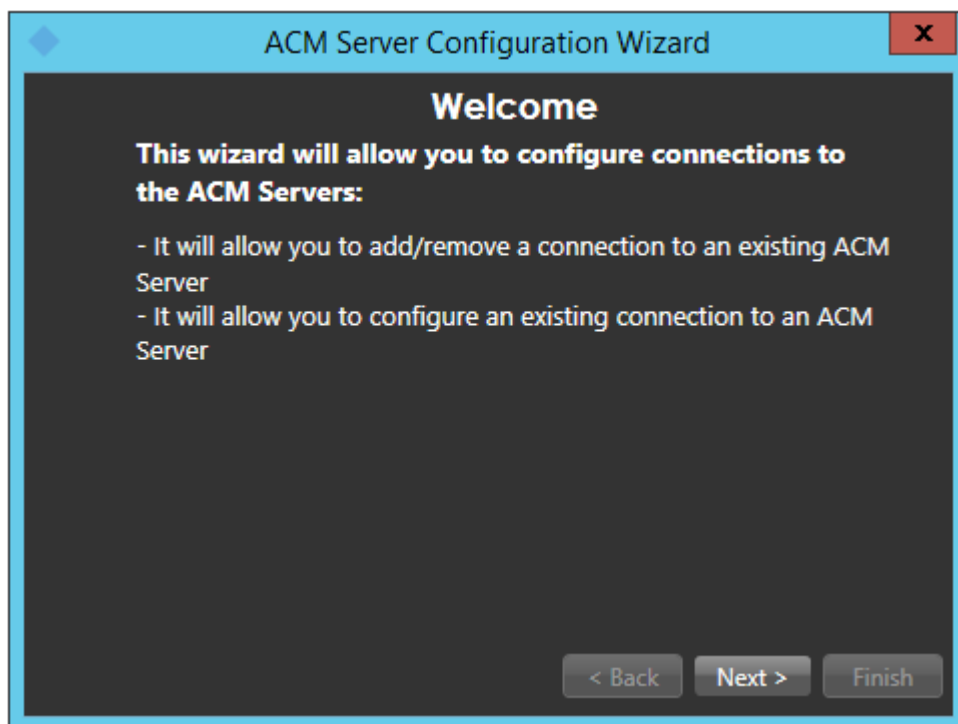
ACM Server: XProtect ACM MIP Plugin

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:

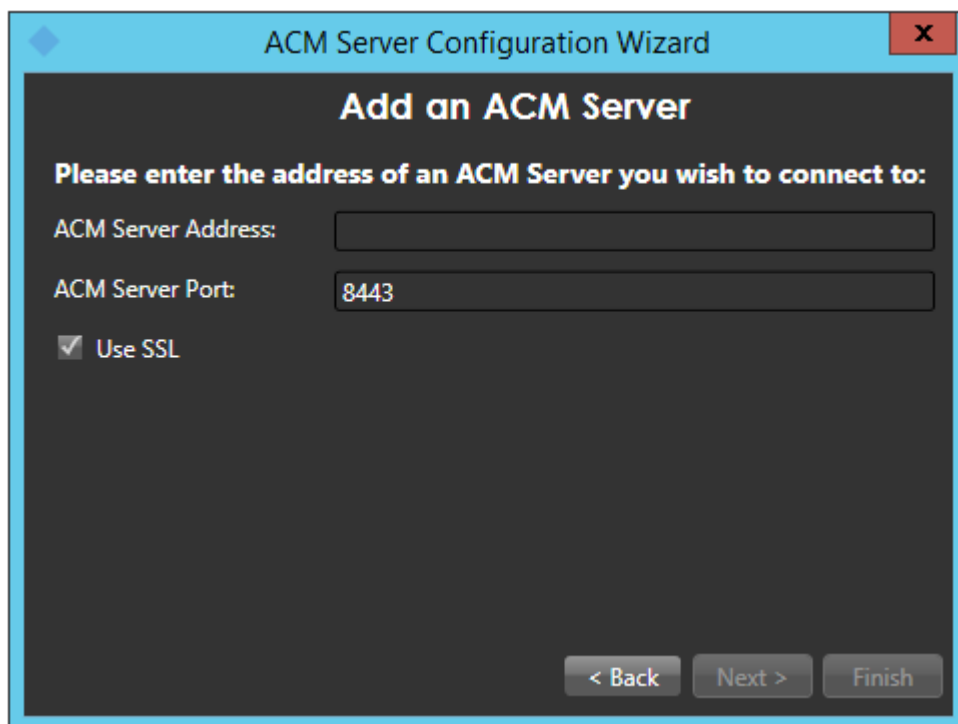


Installing an ACM Server

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 server on which the ACM Server package was installed.



ACM Server Configuration Wizard

Add an ACM Server

Please enter the address of an ACM Server you wish to connect to:

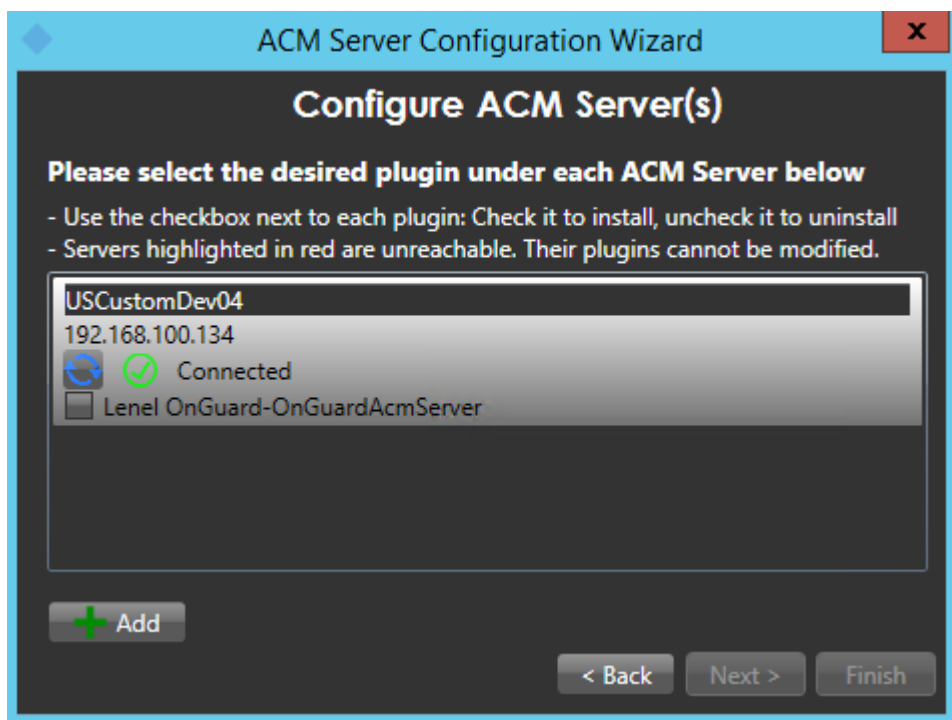
ACM Server Address:

ACM Server Port:

☒ Use SSL

< Back Next > Finish

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.



ACM Server Configuration Wizard

Configure ACM Server(s)

Please select the desired plugin under each ACM Server below

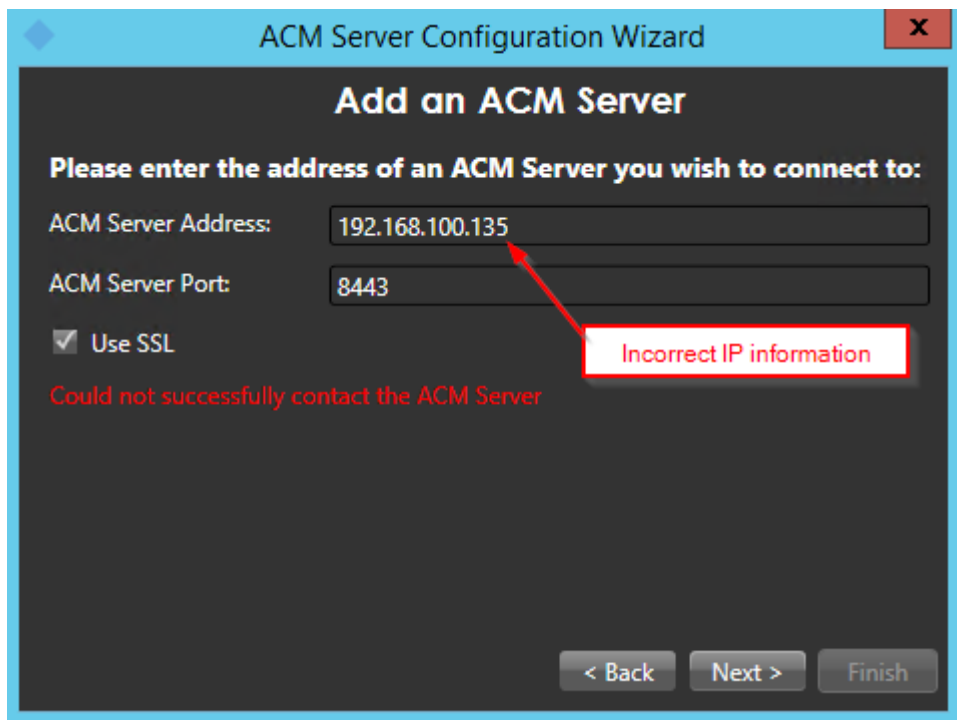
- Use the checkbox next to each plugin: Check it to install, uncheck it to uninstall
- Servers highlighted in red are unreachable. Their plugins cannot be modified.

USCustomDev04	192.168.100.134	  Connected
☐	Lenel OnGuard-OnGuardAcmServer	

 Add

< Back Next > Finish

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 machine is not running with sufficient administrative privileges.



ACM Server Configuration Wizard

Add an ACM Server

Please enter the address of an ACM Server you wish to connect to:

ACM Server Address: 192.168.100.135

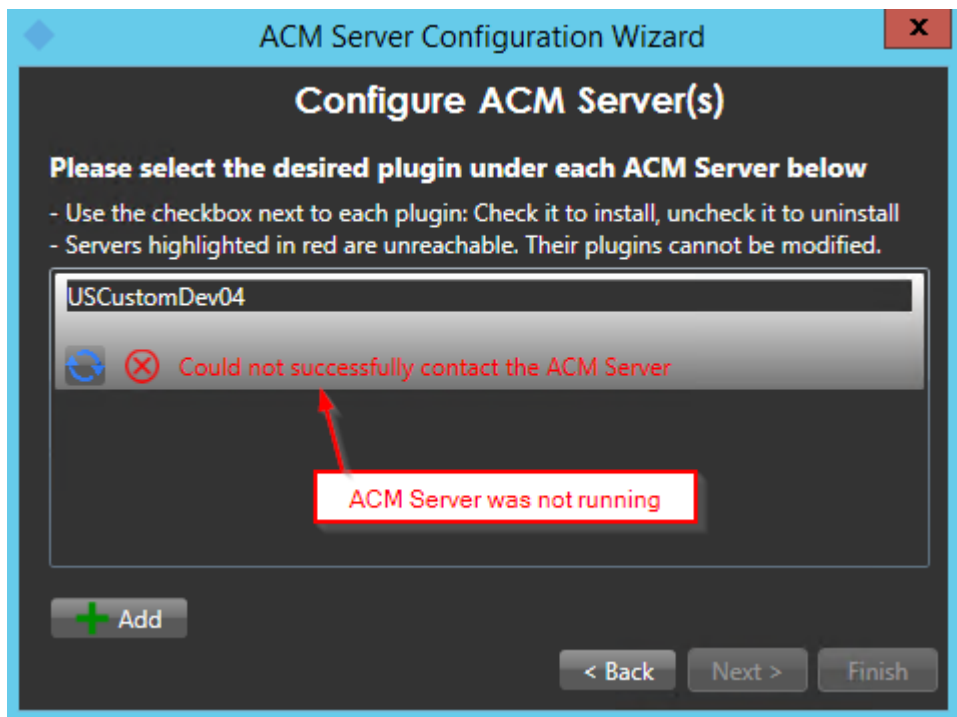
ACM Server Port: 8443

☒ Use SSL

Could not successfully contact the ACM Server

Incorrect IP information

< Back Next > Finish



ACM Server Configuration Wizard

Configure ACM Server(s)

Please select the desired plugin under each ACM Server below

- Use the checkbox next to each plugin: Check it to install, uncheck it to uninstall
- Servers highlighted in red are unreachable. Their plugins cannot be modified.

USCustomDev04

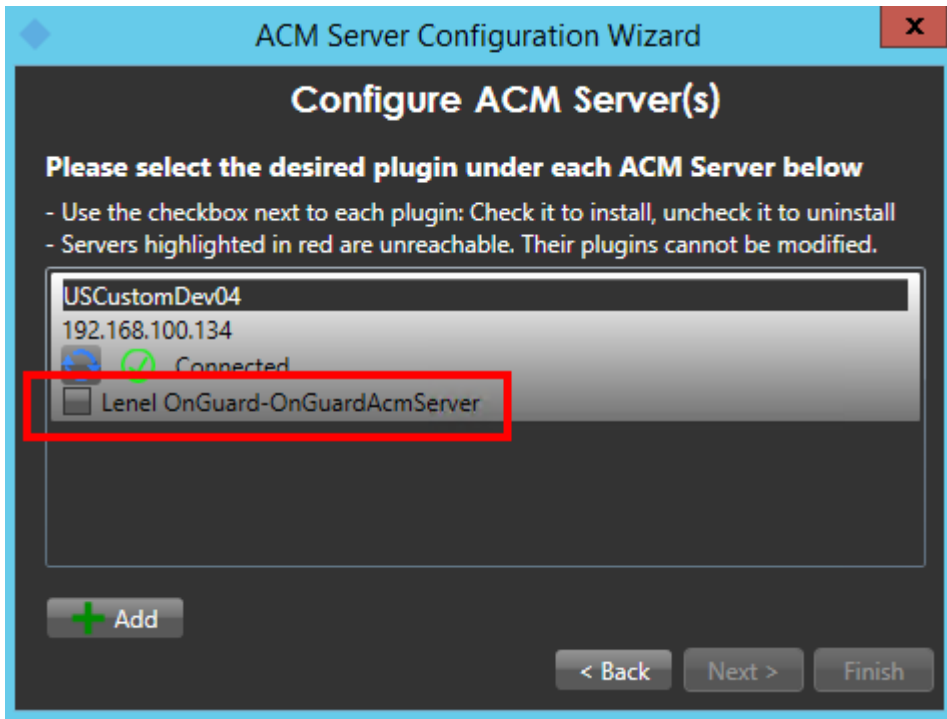
⌂ ⓧ Could not successfully contact the ACM Server

ACM Server was not running

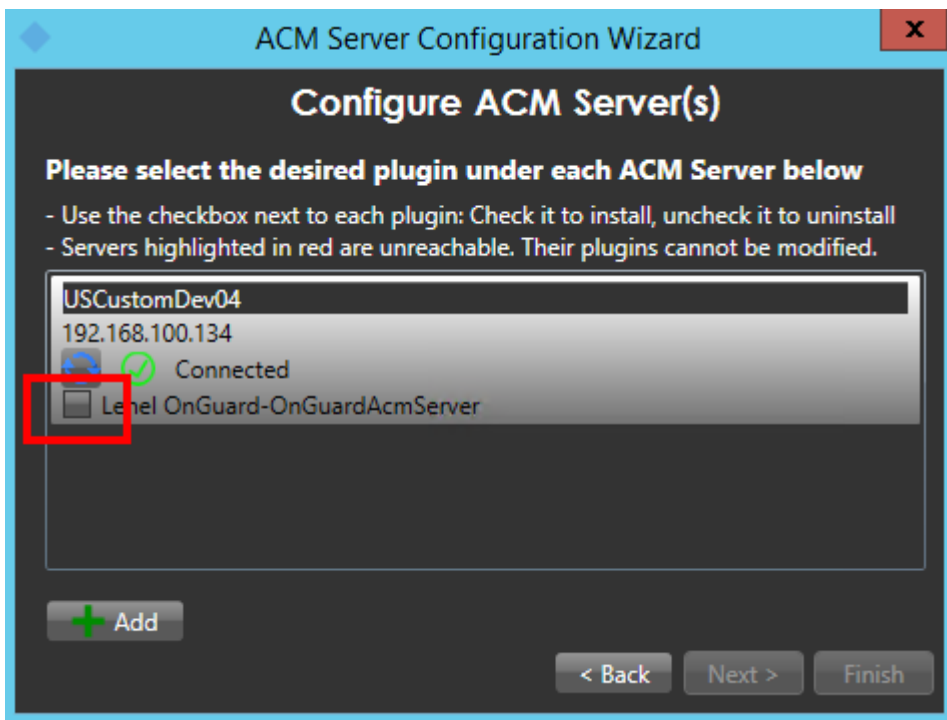
+ Add

< Back Next > Finish

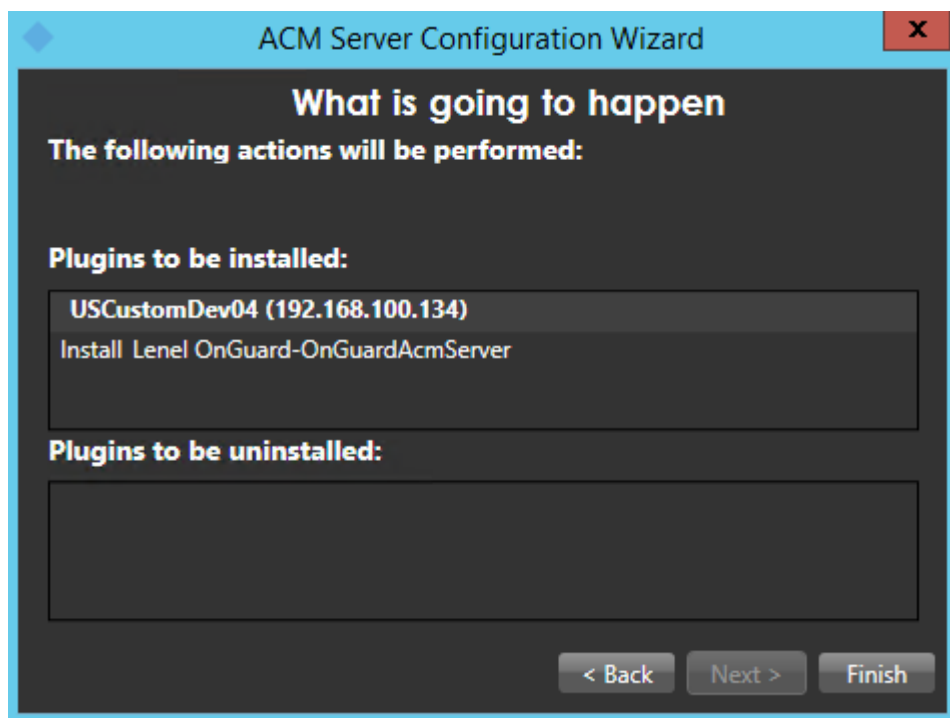
Once you have a successful connection, notice that there is a list of checkboxes under the server heading that represents all detected ACM server plugins installed on that machine. In this case we are looking for Lenel-OnGuard.



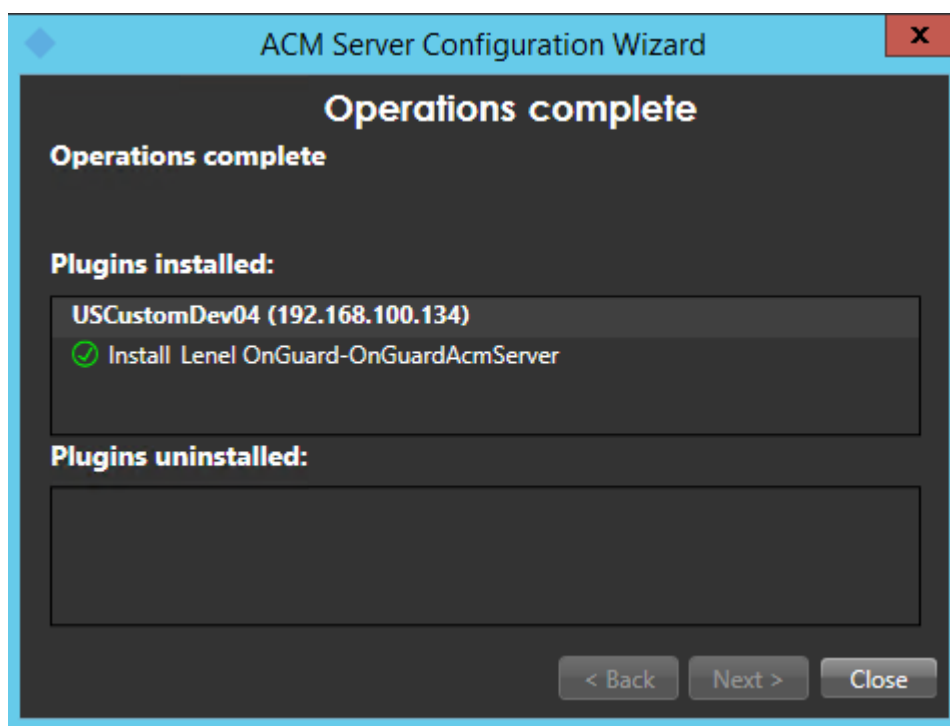
Check the box circled in red below and press next to install a MIP plugin on this host to connect to the Lenel-OnGuard server identified.



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



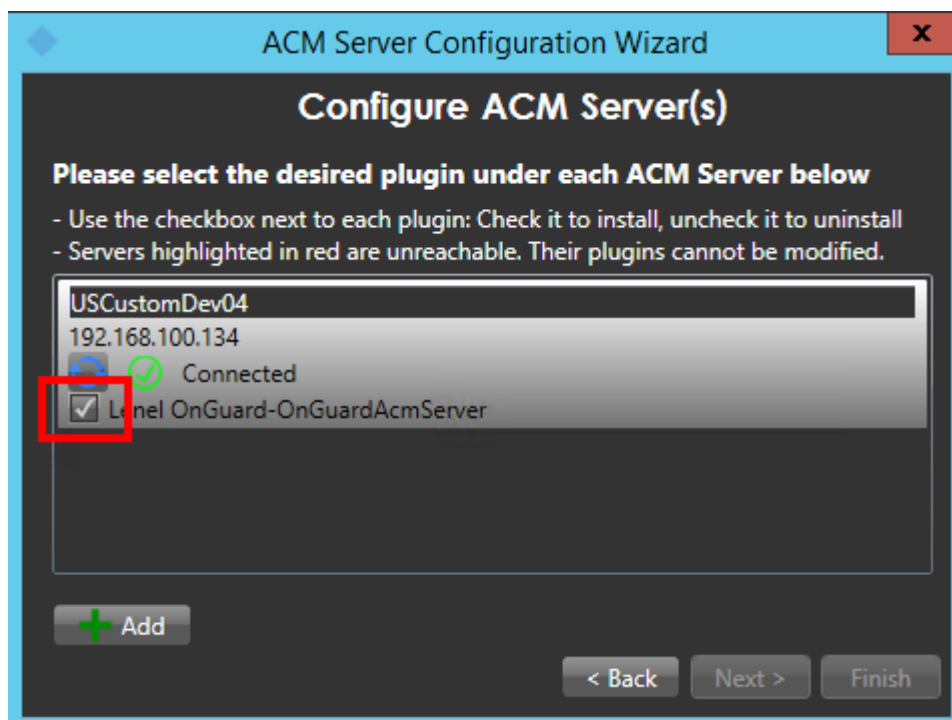
Once the operations are completed, the wizard will display a green checkmark for successful operations and a red x for failed operations.



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

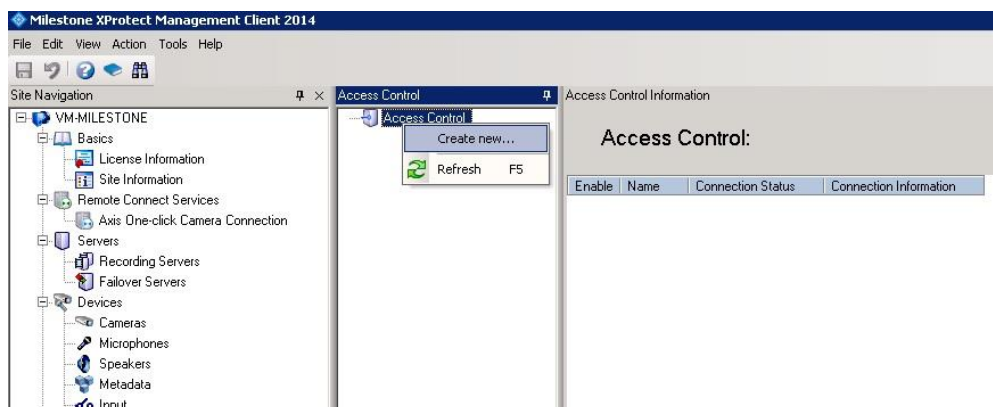
Uninstalling an ACM Server

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



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 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-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, optimize particular settings, etc.

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

The Profile Name should be set to the same as was shown in the ACM Wizard when you added the ACM server. For example:

ReaderSupplInfoInterval – is a counter of how many times to fetch reader information from the internal cache *before* re-fetching that information from Lenel again. Legitimate values are greater than or equal to zero. It's recommended to not set this value to zero as that effectively disables caching of reader information. Lenel doesn't provide notification of certain reader attribute changes (e.g. extended strike time) so this value provides a way to force the system to re-fetch reader information earlier than it normally would.

EventProcessBatchSize – 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.

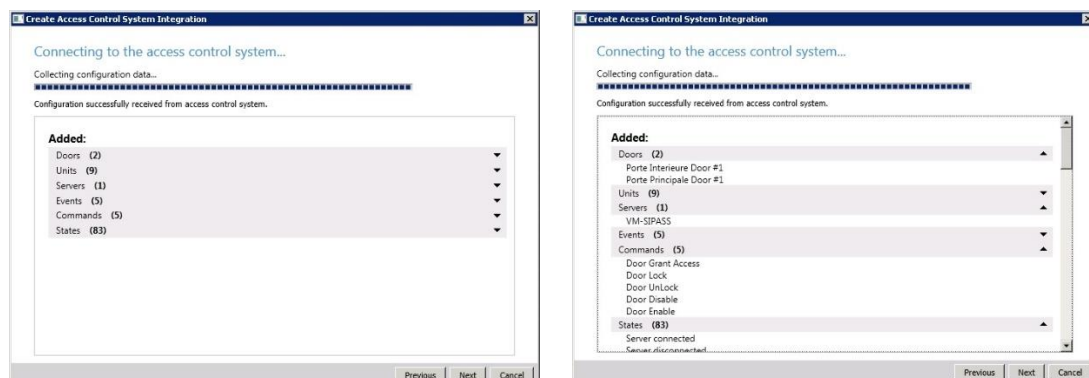
EventProcessSleepInterval - Defines how long the event processor subsystem will sleep (in milliseconds) between batches of events. The subsystem does not sleep when it finishes a batch of events if there is another batch of events ready to process.

CardHolderProcessSleepInterval - Defines how long the Lenel plugin will sleep (in minutes) between fetching card holders from Lenel OnGuard. 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.

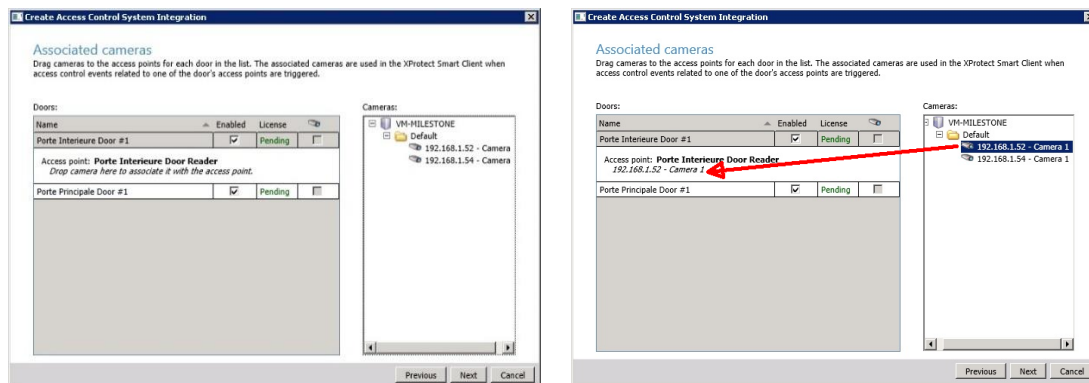
The wizard will now fetch the configuration of the Lenel AC system into Milestone.

When creating a new access control instance, 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 system. If the wizard moves to the “fetching configuration” screen (the image below) but seems to hang with no progress or displays an error message, simply click the Previous button to return the previous wizard page (the image above) and then click Next again.

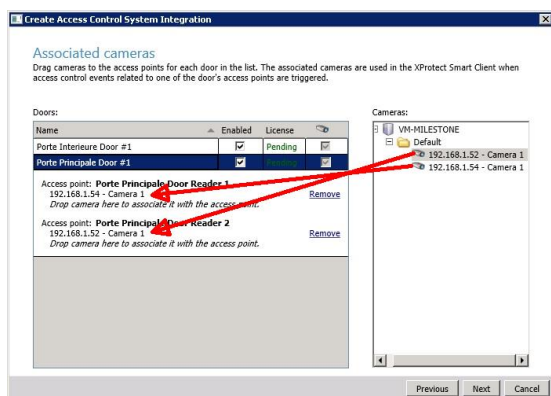
The screen below is an example of the configuration found on the server:



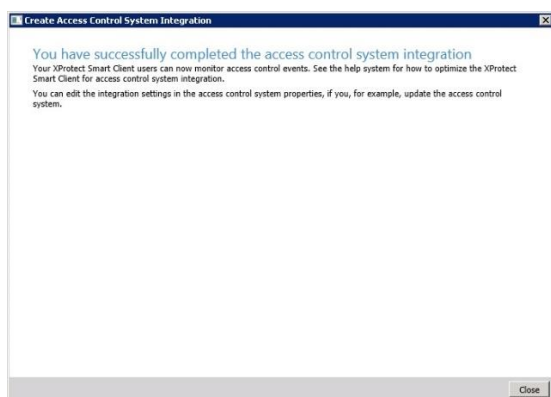
On this screen an association has to be created between each access point of a door and cameras in the Milestone system. This is done so that the system will know which cameras to display on door alarms. For each access point of each door drag a camera from the right tree and place it under the desired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



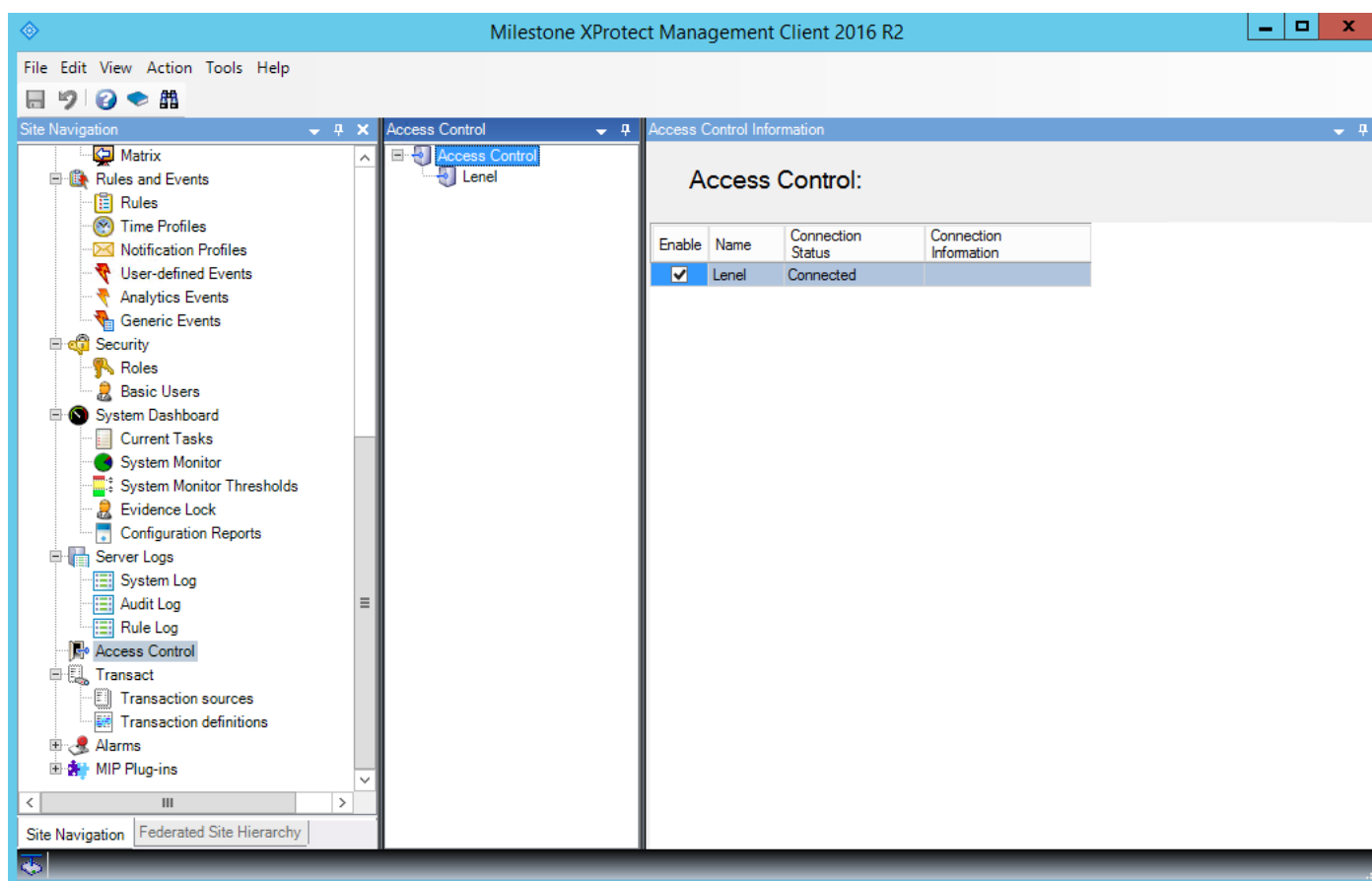
When there is more than one access point per door, you can select the different cameras for the different angles. You can also select more than one camera per access point:



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 ACM integration uses for read-only access to the Lenel 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 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 ACM integration with the following minimal database permissions:

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

Editing Lenel Event Types

The Lenel 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 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.

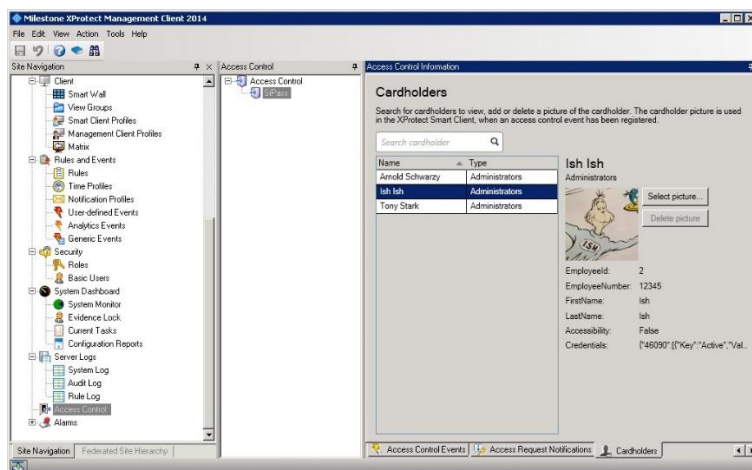
After making and saving changes to the event type file, the administrator should do the following:

1. On the Lenel 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.

Operations

Searching for cardholders

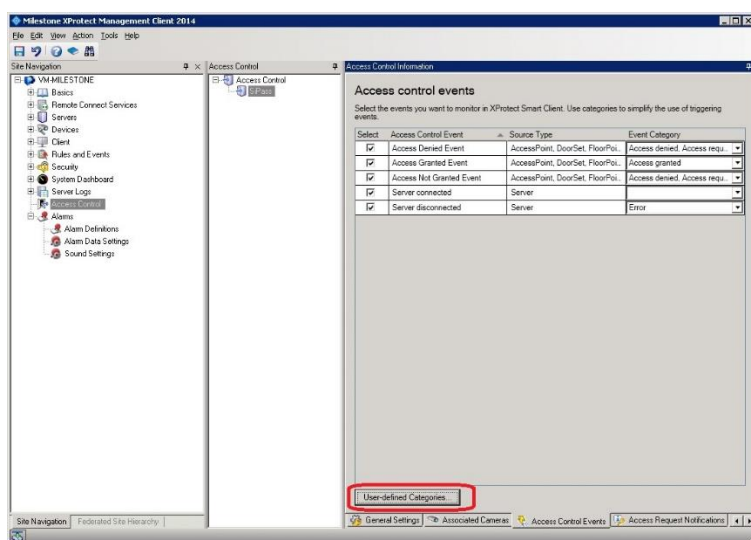
The user can search for existing cardholders in the Lenel system through the management client interface:



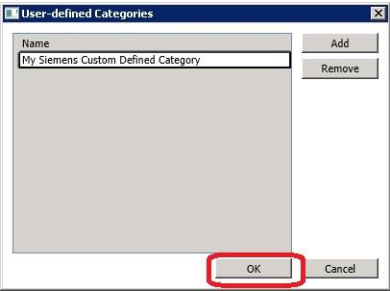
The cardholder picture and detailed information are downloaded from the Lenel server. The search can be made by first name, last name, card number, and employee id. Enter the search string in the search cardholder text box.

Defining Alarms based on Lenel events

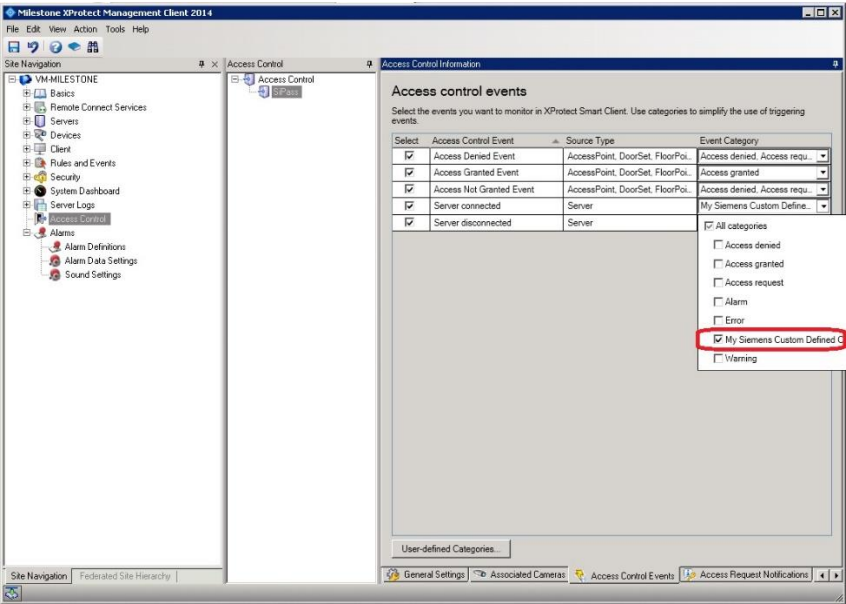
To define alarms based on Lenel events, the events must be part of an event category. The category can be one of the pre-defined Access Control Event categories such as (Access Granted, Access Request, Access Denied, Alarm, Error, and Warning) or a user-defined category. Here is how to create an alarm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



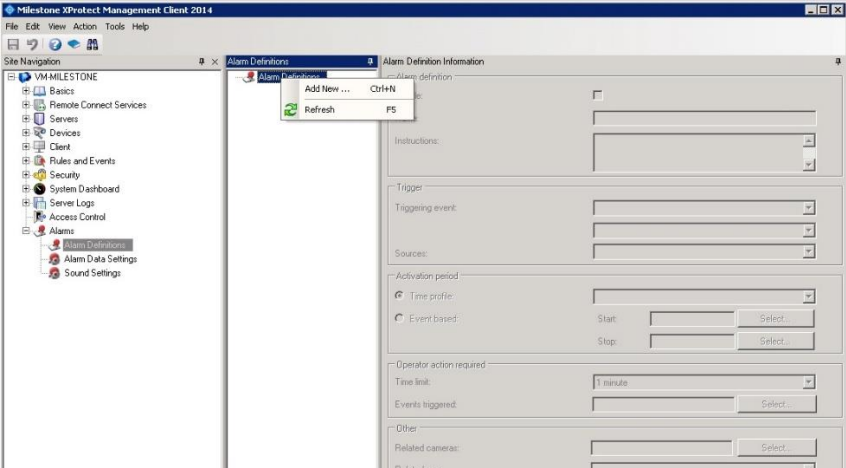
Name the category a pertinent name which represents the group of events and press OK



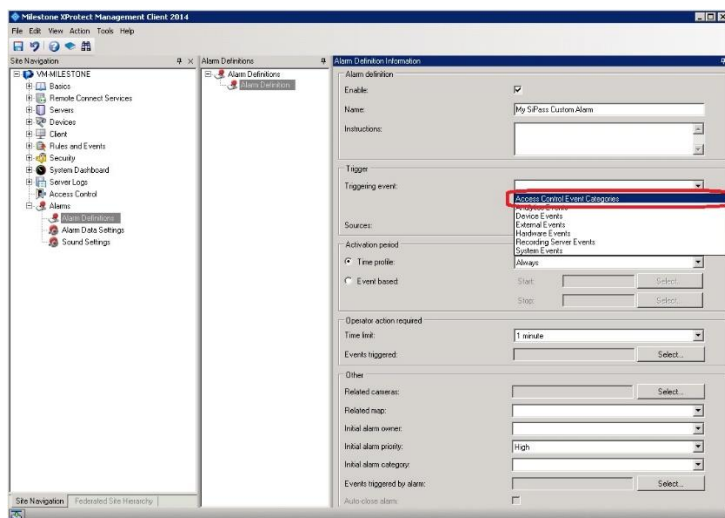
Associate the category with one of the Lenel AC events:



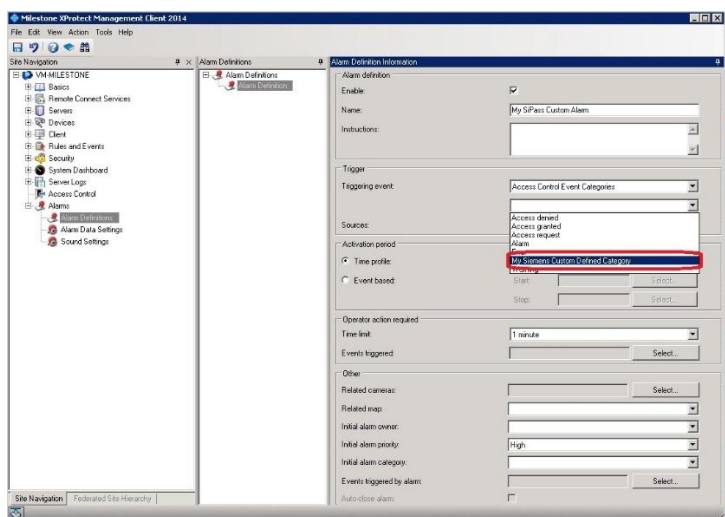
Save your changes and move to the Alarm Definitions section to create an alarm based on that user-defined event category.



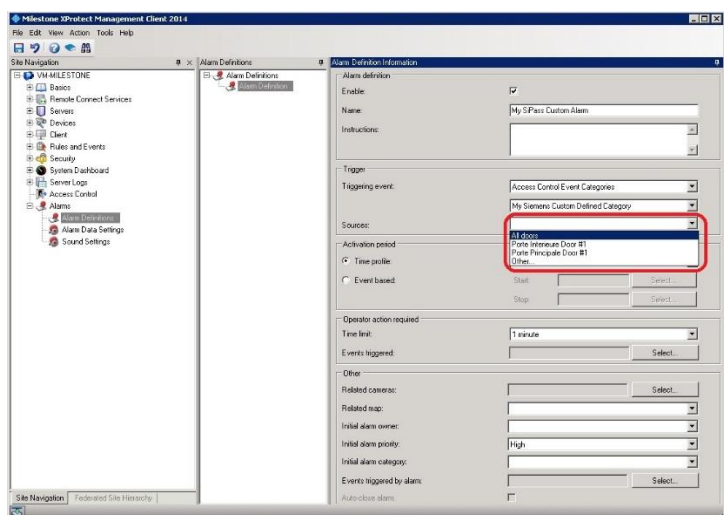
Name the alarm a pertinent name and select Access Control Event Categories in the Triggering event dropdown:



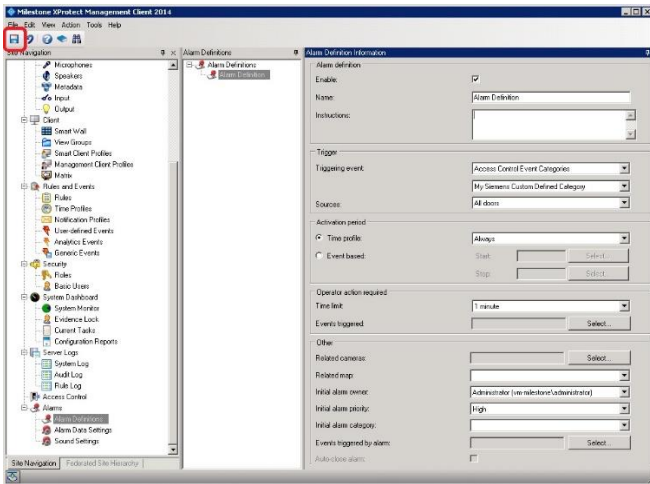
Select the new user-defined event category that was defined earlier:



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



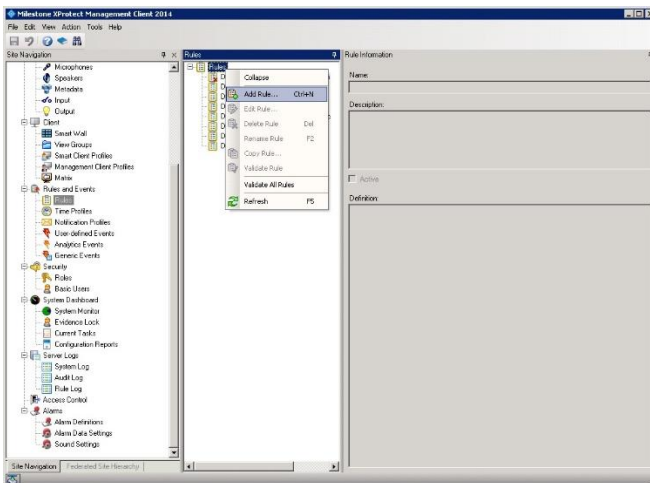
Select all the other alarm parameters and save:



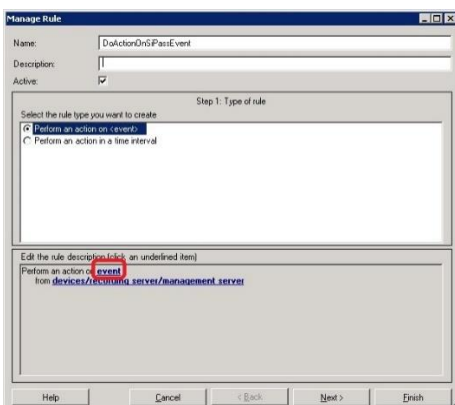
Alarms acknowledged in Milestone are acknowledged in Lenel.

Defining Rules based on Lenel events

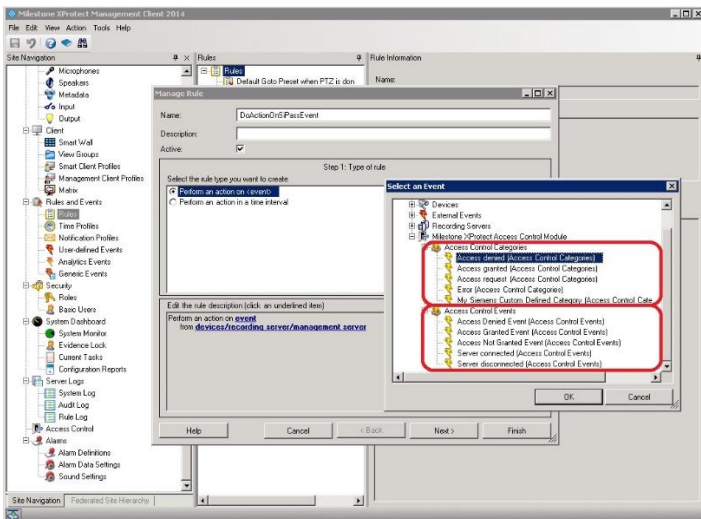
To define rules in Milestone based on Lenel events, create a rule in the Rules tab:



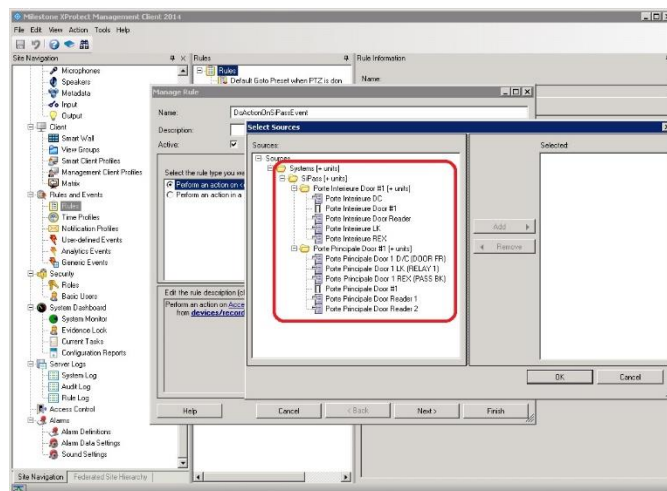
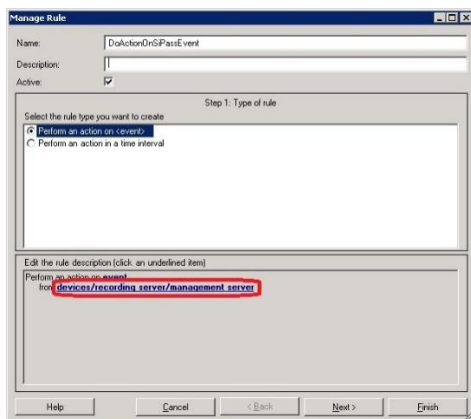
Select the event hyperlink:



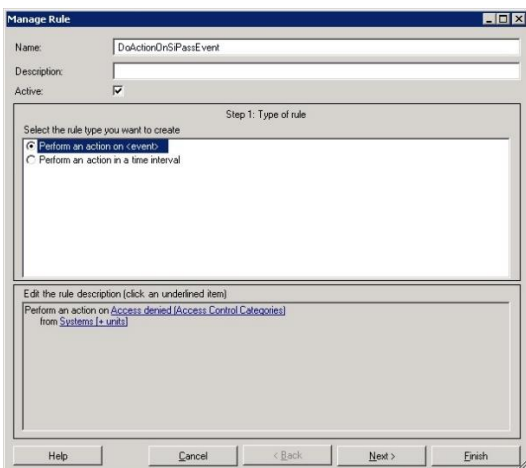
Select an event category or event from the Select an Event dialog:



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.

Manage Rule

Name: DoActionOnSPassEvent

Description:

Active: ☒

Step 2: Conditions

Select conditions to apply:

- ☐ Within selected time in <time profile>
- ☐ Outside selected time in <time profile>
- ☐ Within the time period (starttime) to (endtime)
- ☐ Day of week is <day>
- ☐ Event is from <motion window>

Edit the rule description (click an undefined item)

Perform an action on Access denied (Access Control Categories) from Systems [+ units]

Help Cancel < Back Next > Finish

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:

Manage Rule

Name: DoActionOnSPassEvent

Description:

Active: ☒

Step 3: Actions

Select actions to perform:

- ☐ Start recording on <devices>
- ☐ Start feed on <devices>
- ☐ Set <Smart Wall> to <preset>
- ☐ Set <Smart Wall> <monitor> to show <cameras>
- ☐ Set live frame rate on <devices>
- ☐ Set recording frame rate on <devices>
- ☐ Set recording frame rate to all frames for H.264/MPEG4 on <devices>
- ☐ Start patrolling on <device> using <profile> with PTZ <priority>
- ☐ Pause patrolling on <devices>
- ☐ Move <device> to <preset> position with PTZ <priority>
- ☐ Move to default preset on <devices> with PTZ <priority>
- ☐ Set device output to <state>
- ☒ Create bookmark on <devices>
- ☐ Send notification to <profile>
- ☐ Make new <log entry>
- ☐ Start plug-in on <devices>
- ☐ Stop plug-in on <devices>
- ☐ Apply new settings on <devices>
- ☐ Set Matrix to view <devices>
- ☐ Send SNMP trap
- ☐ Retrieve and store remote recordings from <devices>
- ☐ Retrieve and store remote recordings between <start and end time> from <devices>
- ☐ Save attached images
- ☐ Activate archiving on <archives>
- ☐ On <site> trigger user-defined event
- ☐ Door Grant Access (DoorSet)
- ☐ Door Lock (DoorSet)
- ☐ Door UnLock (DoorSet)
- ☐ Door Disable (DoorSet)
- ☐ Door Enable (DoorSet)
- ☐ Show (access request notification)

Access Control Commands

Edit the rule description (click an undefined item)

Perform an action on Access denied (Access Control Categories) from Systems [+ units]

Create bookmark Bookmark on devices

Help Cancel < Back Next > Finish

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:

Edit the rule description (click an undefined item)

Perform an action on Access denied (Access Control Categories) from Systems [+ units]

Create bookmark Bookmark on devices

Help Cancel < Back Next > Finish

Bookmark Details

Headline: MySPassBookmark

Description: This is an access denied event

Pre-bookmark time (seconds): 10

Post-bookmark time (seconds): 30

Add system information (click links to insert variables in bookmark text)

Device name

Event name

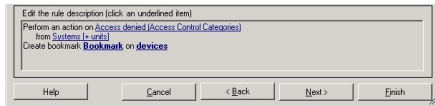
Triggering time

Rule name

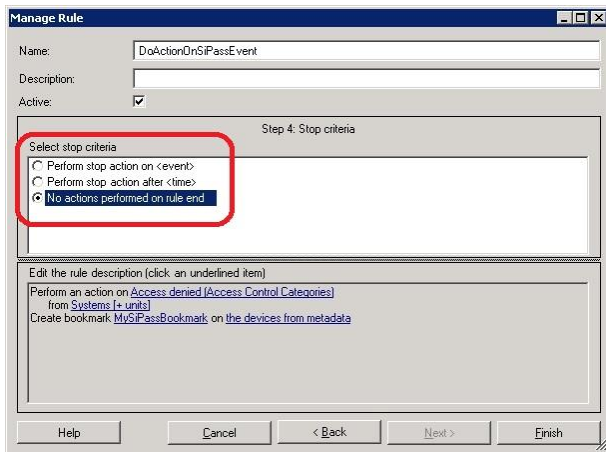
Recording server name

OK Cancel

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



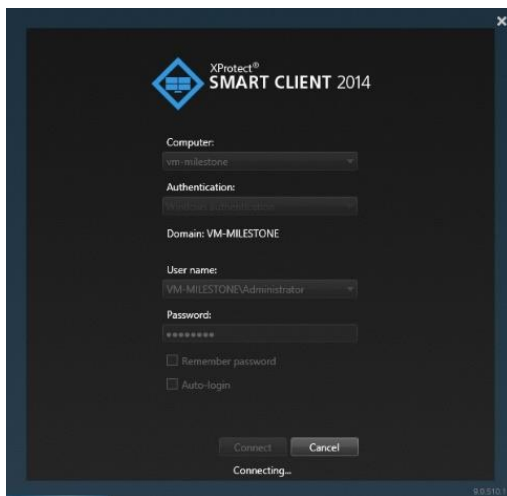
Click next on the rule wizard and select an optional stop criteria, in this example there is no stop criteria.



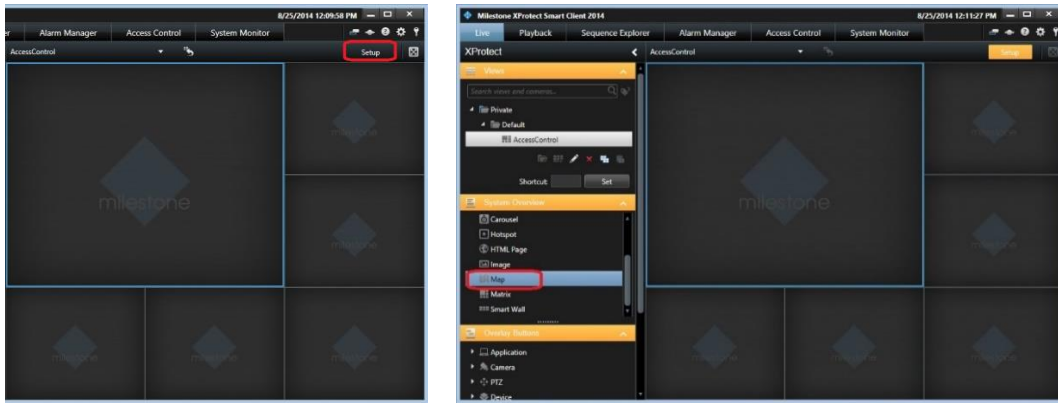
Click finish and the rule is set.

Smart Client Maps

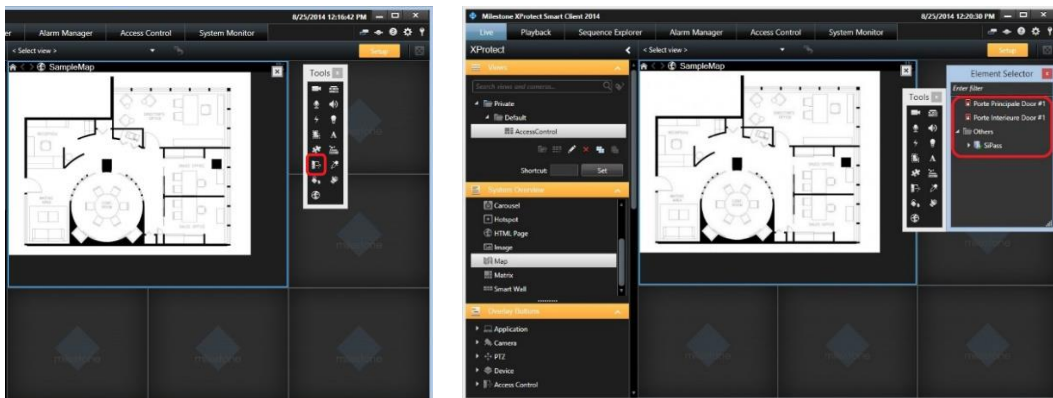
It is possible to put doors and Lenel server(s) on an existing Smart Client Map to display door and server status as well as execute manual commands. Login to the smart client:



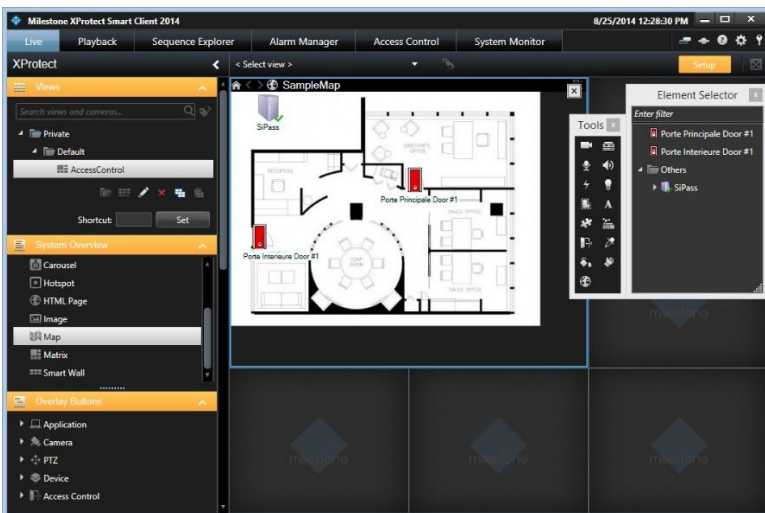
Use an existing view, go into setup mode by pressing the setup button in red below and create a map by dragging it onto a tile once in setup mode.



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

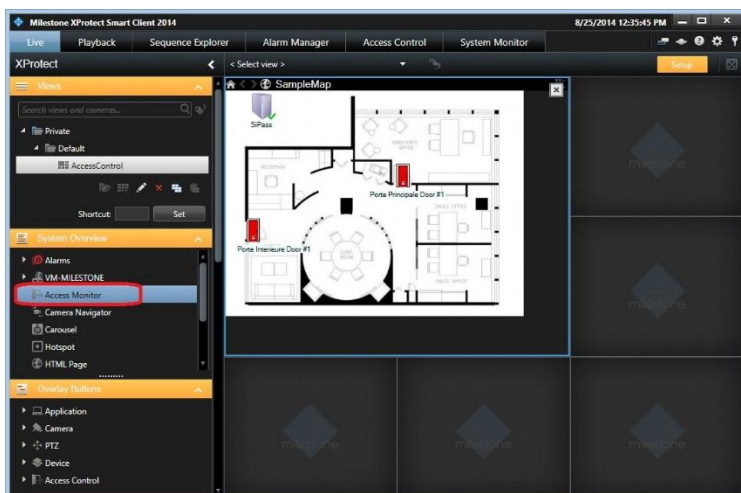


The finalized map with the doors and server added in this example will look like this:

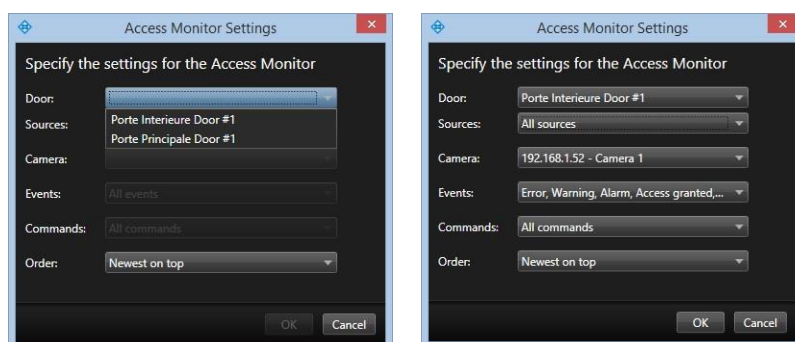


Access Monitor Tiles

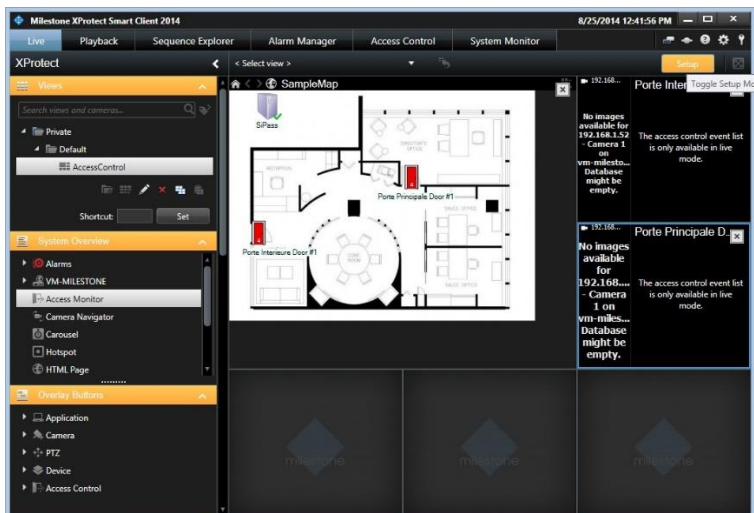
Access monitor tiles allows the monitoring of access events on a specific door by displaying cardholder credentials next to the video content. Drag the “Access Monitor” item from the System Overview onto a tile:



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:



Alarm Acknowledgment

Alarm acknowledgment from XProtect (2016 R3 or greater) to Lenel 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.

Alarm acknowledgment from Lenel to XProtect is not implemented due to the lack of such functionality in Lenel.

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.

Milestone XProtect Smart Client

Live Playback Sequence Explorer Alarm Manager Access Control System Monitor

No map has been selected

Quick Filters

- New (2)
- In progress (0)
- On hold (0)
- Closed (0)

Servers

USCUSTOMDEV02

Alarms No filter

Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
12:53:31 PM 6/9/2011	1	1	New	OnGuard Acc	2 - Lenel OpenProx		2
12:52:52 PM 6/9/2011	1	1	New	OnGuard Acc	2 - Lenel OpenProx		1

Acknowledge

Set on hold

Close

Edit

Disable new alarms

Print

NOTE – As mentioned above, selecting either Acknowledge or Close will cause the alarm to be acknowledged in Lenel and removed from 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. The reason is simple – the alarm was removed from 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.

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 Event 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.

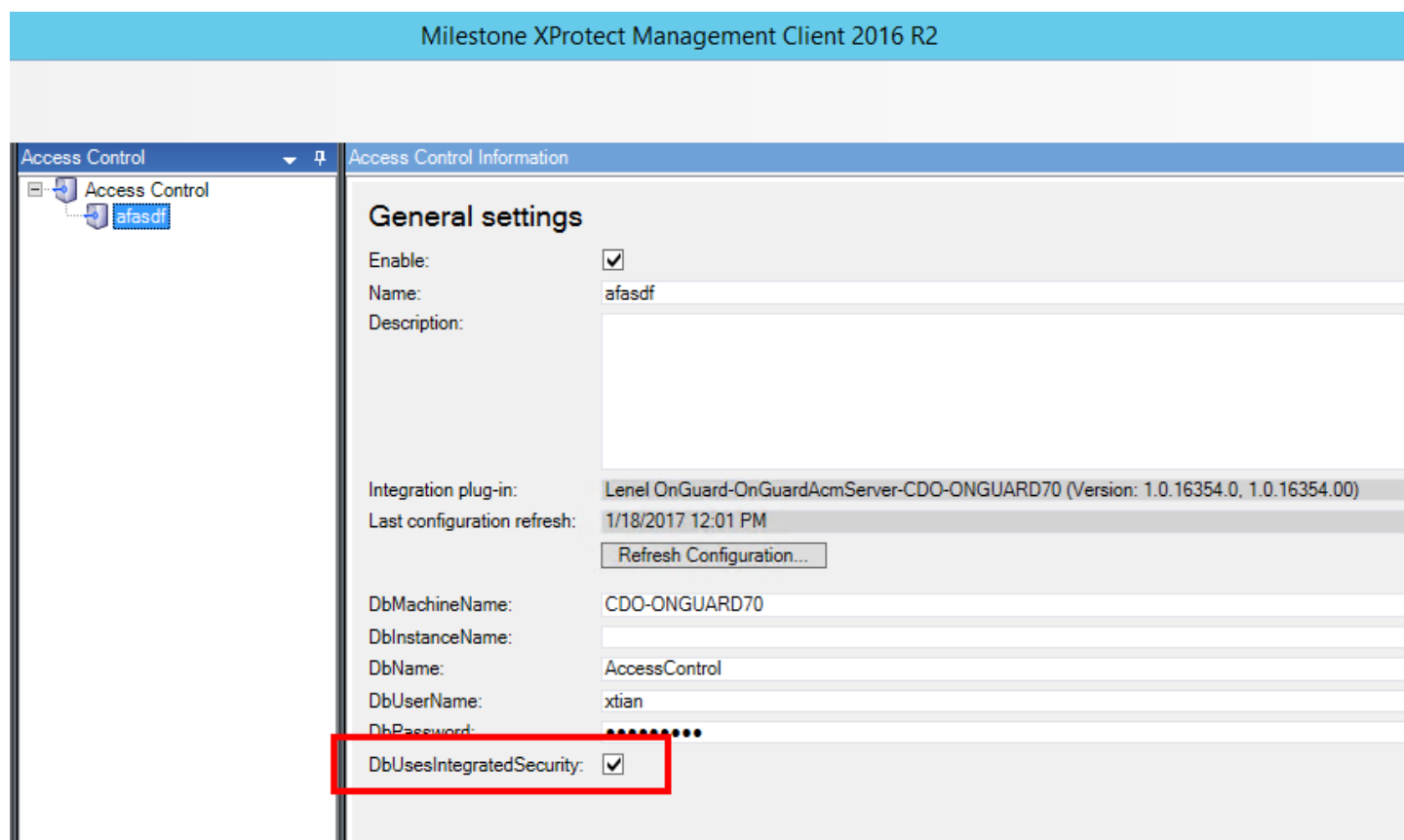
If the debug log shows an error similar to:

```
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.

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](#).

Optimizing Event Processing Performance

To maximize event processing performance, adjust the following 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](#)):
 - ReaderSupplInfoInterval – Set this to a large number (e.g. 10,000). Frequently reading reader information has a large impact on overall performance.
 - EventProcessBatchSize – Tailor this value as needed. The larger the number, the more events processed in one batch.
 - EventProcessSleepInterval – Tailor this value as needed. The smaller the number, the less time the event processing subsystem waits between attempting to query for more events.

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="*" minlevel="Info" writeTo="mainlog" />"**, **"<logger name="lenel.*" minlevel="Info" writeTo="lenel.*" />"**, and **"<logger name="OnGuard.*" minlevel="Info" writeTo="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

- This ACM integration was only tested against the MIP SDK 2016. The MIP SDK is backwards-compatible; so it is assumed that the ACM integration will work with MIP SDK 2014.
- This ACM integration has only been tested when running the Lenel and Milestone systems on Windows Server 2012 R2.
- This 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.
- 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 system.
- See the negative side-effects of [upgrading](#).
- Lenel Enterprise is not supported.

Events Handled

The Lenel OnGuard ACM integration will attempt to handle all the events generated by Lenel.

The actual events handled may vary from one version of Lenel to another. There may also be other circumstances that affect if the integration can handle an event or not (e.g. the Lenel API used by the integration doesn't forward the event, the event relates to a type of hardware not supported in the integration, etc).

LenelFetchEventTypes Utility

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

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

This application must be run on the Lenel OnGuard machine where the Lenel 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 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.

Example Event List

This list of events came from a Lenel OnGuard 7.3 system and is listed here only as an example of the events supported by the Lenel ACM integration. The event list has been sorted alphabetically.

24 Hour Alarm
24 Hour Alarm Restore
24 Hour Auto Test
24 Hour Non-Burglary Alarm
24 Hour Non-Burglary Alarm Restore
24 Hour Report Closed
24 Hour Report Open
24 Hour Zone Bypassed
24 Hour Zone Unbypassed
30 Minutes Since Fallback Command
32 Hour Event Log Marker
AC Battery Fail
AC Restore
AC Trouble
ACU Firmware Upgraded
AFC Mode Off
AFC Mode On
ARDIS Module Communication Loss
ARDIS Module Communication Restored
Abort
Accepted Biometric Score
Access Closed
Access Code Used

Access Denied
Access Denied (denied_access_denied)
Access Denied : AAM Timeout
Access Denied : AAM Validation Failed
Access Denied Door Secured
Access Denied Interlock
Access Denied Passback
Access Denied Unauthorized Arming State
Access Denied Unauthorized Entry Level
Access Denied Unauthorized Time
Access Denied Under Duress
Access Denied to Destination Floor
Access Denied: Access Control Format Not Found
Access Denied: Area Empty
Access Denied: Area Occupied
Access Denied: Asset Required
Access Denied: Biometric Reader Offline
Access Denied: Card Expired
Access Denied: Escort Timeout Expired
Access Denied: Invalid Access Control Data
Access Denied: Invalid Access Control Data Length
Access Denied: Invalid Access Control Data Parity
Access Denied: Invalid Access Control Data Type
Access Denied: Invalid Smart Card Authentication
Access Denied: Invalid Smart Card Data
Access Denied: Invalid Smart Card Location
Access Denied: Invalid Smart Card Type
Access Denied: Invalid Timezone
Access Denied: No Biometric Template
Access Denied: No Occupant Approval
Access Denied: Reader Locked
Access Denied: Secured Mode
Access Denied: Smart Card Format Not Found
Access Door Propped
Access Door Status Monitor Shunt
Access Door Status Monitor Trouble
Access Exit Request Trouble
Access Granted
Access Granted (intrusion_granted_access_granted)
Access Granted - Anti-Passback Not Used
Access Granted - Anti-Passback Used
Access Granted Entry Made
Access Granted No Entry Made
Access Granted Under Duress
Access Granted Under Duress - No Entry Made
Access Granted on Facility Code
Access Granted on Facility Code, No Entry Made
Access Granted to Destination Floor
Access Granted: Reader Unlocked
Access Level Change
Access Lockout
Access Open

Access Point Bypass
Access Program Exit
Access Relay/Trigger Fail
Access Request to Exit Shunt
Access Schedule Change
Access Trouble
Access Zone Shunt
Account Status Failure
Account Status Restore
Acknowledgment Action Executed
Acknowledgment Action Failed
Activate Output
Activity Resumed
Add Holiday
Add User
Air Flow Loss
Air Flow Loss Restore
Alarm
Alarm Active
Alarm Canceled
Alarm Cause
Alarm Condition Priority Level 1
Alarm Condition Priority Level 2
Alarm Condition Priority Level 3
Alarm Condition Priority Level 4
Alarm Condition Priority Level 5
Alarm Condition Priority Level 6
Alarm Condition Priority Level 7
Alarm Condition Priority Level 8
Alarm Mask Group Armed
Alarm Mask Group Arming Failure, Active Points
Alarm Mask Group Disarmed
Alarm Mask Group Force Armed
Alarm Mask Group Mask Count Decrement
Alarm Mask Group Mask Count Increment
Alarm Monitoring Action Group Executed
Alarm Monitoring Action Group Failed
Alarm Not Configured, Memory Low
Alarm Relay Disable
Alarm Relay Disable Restore
Alarm Silenced
Alarm Tamper Loop
Alarm/Restore
All Lockouts Removed
All Points Tested
All Systems Normal
Analog Restore
Analog Restored
Analog Service Requested
Analog Service Required
Anti-Passback Violation
Archive Server Failure

Area APB Reset
Area Alarm - Confirmed
Area Alarm - Unconfirmed
Area Arm Failure
Area Arm with Override
Area Closed
Area Confirm Alarm Reset
Area Limit Exceeded
Area Limit Minimum
Area Watch End
Area Watch Start
Armed Off
Armed On
Armed On with Bypasses
Armed On with Isolates
Armed Perimeter Delay
Armed Perimeter Instant
Armed Stay
Asset Denied - Asset Disable Command Sent
Asset Denied - Invalid Access
Asset Denied - Invalid Asset
Asset Denied - Invalid Cardholder
Asset Denied - No Asset Privileges
Asset Granted - Asset Owner
Asset Granted - Asset Privileges Only
Audible Alarm
Audible Alarm Restore
Audibles Silenced
Audibles Unsilenced
Audio Level
Audio Level Restored
Audit Trail Cleared
Audit Trail Limit Reached
Auto Arming Time Changed
Auto-Arm Failed
Automatic Closing
Automatic Opening
Automatic Phone Test
Automatic Test
Auxiliary Power Fault
Auxiliary Power Supply AC Loss
Auxiliary Power Supply AC Restored
Auxiliary Power Supply Communication Loss
Auxiliary Power Supply Communication Restored
Auxiliary Power Supply Fault Restored
Auxiliary Power Supply Output Low
Auxiliary Power Supply Output Low Restored
Background Map Found
Background Map Not Found
Background Scene Changed
Background Scene Changed Restored
Backup Battery Critical

Backup Battery Low
Bad 9112 Packet
Bad Card Lockout
Bad PIN Lockout
Bad System ID
Battery Level Test Failure
Battery Level Test Success
Battery Restored
Battery Status
Battery Test Fail
Battery Test Fail Restore
Battery Trouble
Bell 1 Disable
Bell 1 Disable Restore
Bell 2 Disable
Bell 2 Disable Restore
Bell Fault
Bell Restore
Biometric Mismatch
Biometric Verify Mode Disabled
Biometric Verify Mode Enabled
Blind Camera
Blind Camera (AI)
Blind Camera (AI) Restored
Blind Camera Restored
Block Acknowledge
Blocked
Brightness Change
Brightness Change Restored
Burglary Alarm
Burglary Alarm Cross Point
Burglary Alarm Restore
Burglary Bypass
Burglary Cancel
Burglary Close
Burglary Inactive
Burglary Open
Burglary Restore
Burglary Supervisory
Burglary Test
Burglary Trouble
Burglary Trouble Restore
Burglary Unbypass
Burglary Verified
Busy Seconds
Buzzer Test Failure
Buzzer Test Success
Bypass - Closed
Bypass Restore
C900 Battery Low
C900 Battery Restore
C900 Input Open

C900 Input Restored
C900 Input Shorted
C900 Intercept Disabled
C900 Intercept Enabled
C900 Output Activated
C900 Output Deactivated
C900 Reboot
C900 Switched to Fallback
C900 Switched to Intercept
CPU Data Error
CPU Utilization Threshold Exceeded
CPU Utilization Threshold Restored
Cabinet Tamper
Call Conferenced
Call Disconnected
Call Ended
Call Established
Call Failed
Call Queued
Call Removed from Queue
Call Transferred
Call to a Busy Subscriber
Call to a Private Subscriber
Call to an Open Subscriber
Callback Request
Camera Motion Detected
Camera Motion Detected Restored
Camera Tamper Active
Camera Tamper Restored
Cancel Alarm
Cancel Entire Sale
Cancel Report
Canceled Cabinet Tamper
Canceled Grounded Loop
Canceled Line Error
Canceled Open Line
Canceled Power Failure
Canceled Shorted Line
Cannot Arm - Users Left In Area
Cannot Open Door: Interlock Area Busy
Capture Source Mismatch
Carbon Monoxide Detected
Card Added
Card Assigned
Card Cancelled
Card Deleted
Card Not Removed
Card Not Valid
Card Only Mode Change Denied: Blocked Mode
Card Only Mode Change Denied: Security Mode
Cash Amount Tendered
Cash or Safe Drop

Central Station Report Delay
Central Station Report Success
Change Due
Change Language
Change Language Failure
Change Lock Mode
Change Mode Denied
Change of State
Charge Account Tender
Check Tender
Checksum Fail
Cipher Mode Disabled
Cipher Mode Enabled
Circuit Reset
Clear Audit Trail Failure
Clear Audit Trail Success
Clear Lock Failure
Clear Lock Success
Clerk Name or Number
Clock Failure
Clock Stopped
Close Area
Close Exception
Close Out of Window
Close by User
Closing
Closing Delinquent
Closing Extend
Closing Out of Window by User
Closing Report
Closing Switch
Closing Time Changed
Collection of Openings
Combustion Alarm
Combustion Alarm Restore
Command 10 Set From Reader
Command 11 Set From Reader
Command 12 Set From Reader
Command 13 Set From Reader
Command 14 Set From Reader
Command 15 Set From Reader
Command 4 Set From Reader
Command 5 Set From Reader
Command 6 Set From Reader
Command 7 Set From Reader
Command 8 Set From Reader
Command 9 Set From Reader
Command Pin+10 Set From Reader
Command Pin+20 Set From Reader
Command Point Failure
Command Point Reset
Command Point Trip

Command Sent
Communication Access Denied
Communication Access Restored
Communication Initialization Failed
Communication Path Switch - Primary to Secondary
Communication Path Switch - Secondary to Primary
Communication Trouble Restore
Communications Fail
Communications Lost
Communications Restore
Communications Restored
Communications Trouble
Communications With Host Lost
Communications With Host Restored
Complimentary Tender
Computer Trouble
Config No Reply
Congestion
Congestion (C)
Congestion (C) Restored
Congestion (R)
Congestion (R) Restored
Congestion Restored
Controller Connection Mismatch
Controller Encryption Error
Controller Memory Overflow - Badges
Credit Card Tendered
Cross Zone Trouble
Current Time
Custom Function Executed
Custom GOV Length Incompatible With Camera Recording Settings
DURESS - Access Denied Under Duress
DURESS - Access Denied: Area Empty
DURESS - Access Denied: Area Occupied
DURESS - Access Denied: Asset Required
DURESS - Access Denied: Biometric Reader Offline
DURESS - Access Denied: Escort Timeout Expired
DURESS - Access Denied: No Biometric Template
DURESS - Access Denied: No Occupant Approval
DURESS - Access Denied: Reader Locked
DURESS - Access Granted
DURESS - Access Granted - Anti-Passback Not Used
DURESS - Access Granted - Anti-Passback Used
DURESS - Access Granted No Entry Made
DURESS - Access Granted Under Duress
DURESS - Access Granted Under Duress - No Entry Made
DURESS - Access Granted on Facility Code
DURESS - Access Granted on Facility Code, No Entry Made
DURESS - Access Granted: Reader Unlocked
DURESS - Anti-Passback Violation
DURESS - Area Closed
DURESS - Area Limit Exceeded

DURESS - Asset Denied - Asset Disable Command Sent
 DURESS - Asset Denied - Invalid Access
 DURESS - Asset Denied - Invalid Asset
 DURESS - Asset Denied - Invalid Cardholder
 DURESS - Asset Granted - Asset Owner
 DURESS - Asset Granted - Asset Privileges Only
 DURESS - Biometric Mismatch
 DURESS - Denied - No Host Approval
 DURESS - Denied - Unauthorized Assets
 DURESS - Denied Count Exceeded
 DURESS - Denied, Badge Not in Panel
 DURESS - Denied, PIN Only Request
 DURESS - Inactive Badge
 DURESS - Interlock Area Busy
 DURESS - Invalid Access Level
 DURESS - Invalid Badge
 DURESS - Invalid Facility Code
 DURESS - Invalid Issue Code
 DURESS - Invalid PIN Number
 DURESS - Smart Card Authentication Failed
 DURESS - Timeout Exceeded - No Second Card
 DURESS - Use Limit Exceeded
 Data Lost
 Database Error in Panel Download
 Database Error: Event Polling Stopped
 Database Event Queue Limit Exceeded
 Database Write Time Exceeded
 Date Changed
 Day Trouble
 Day Trouble Restore
 Day/Night Alarm
 Day/Night Alarm Restore
 Daylight Savings Time Audit
 Daylight Savings Update
 Deactivate Output
 Dealer ID
 Debit, ATM, Check Card Tender
 Deferred Close
 Deferred Open/Close
 Delete Device
 Delete User
 Denied - Area Out of Schedule
 Denied - Dual Custody Violation
 Denied - Group Mismatch
 Denied - No Host Approval
 Denied - No Off Authority
 Denied - No On Authority
 Denied - No Stay Authority
 Denied - Pending Enroll
 Denied - Unauthorized Assets
 Denied Count Exceeded
 Denied Low Battery

Denied UnMask - Active Zones in Group
Denied, Badge Not in Panel
Denied, Duplicate Card
Denied, Invalid Common Pin
Denied, No Command Authority
Denied, Not Authorized
Denied, PIN Only Request
Denied, Reader Excluded
Deposit Amount Paid Pending Purchase
Deposit Return
Detector High Sensitivity
Detector High Sensitivity Restore
Detector Low Sensitivity
Detector Low Sensitivity Restore
Detector Test
Detector Test Fail
Detector Test OK
Device Turned Off
Device Turned On
Device Type Mismatch
Diagnostic
Diagnostic Card
Diagnostic Error
Diagnostics Battery
Diagnostics Keypad LED Buzzer
Diagnostics Switches
Dial Out Method
Dialer Disabled
Dialer Disabled Restore
Dialer Shutdown
Dialing Error
Dialup Last Connection Time Expired
Dialup Stored Command Limit Exceeded
Digital Dialer Daily Test Fail
Directional Motion
Directional Motion (C)
Directional Motion (C) Restored
Directional Motion (R)
Directional Motion (R) Restored
Directional Motion Restored
Disable Intercept Mode
Disarm From Alarm
Discount Entered as Absolute Amount
Discount Entered as Percentage
Disk Access Threshold Exceeded
Disk Access Utilization Threshold Restored
Disk Read Utilization Threshold Exceeded
Disk Read Utilization Threshold Restored
Disk Write Utilization Threshold Exceeded
Disk Write Utilization Threshold Restored
Door Close
Door Closed Exterior

Door Contact Tamper
Door Contact Tamper Canceled
Door Cycled
Door Forced
Door Forced Open
Door Forced Open Bypassed
Door Forced Open Canceled
Door Forced Open Disabled
Door Forced Open Masked
Door Forced Open Restored
Door Forced Open Unmasked
Door Forced Trouble
Door Held Open
Door Held Open Bypassed
Door Held Open Canceled
Door Held Open Disabled
Door Held Open Masked
Door Held Open Pre Alarm
Door Held Open Restored
Door Held Open Unmasked
Door Left Open
Door Left Open Alarm
Door Left Open Restore
Door Left Open Trouble
Door Locked
Door Locked Out
Door Mag Trouble Clear
Door MagTrouble
Door Not Secured
Door Open
Door Open by Key
Door Open by Key Restored
Door Open by Portable Programmer
Door Open from Inside
Door Reinstated
Door Request
Door Restore
Door Restore (intrusion_trouble_door_restore)
Door Secured
Door Shunt Command Executed From Reader
Door Shunt Command Results - Canceled
Door Station
Door Status
Door Status Bypassed
Door Status Disabled
Door Status Restored
Door Unlocked
Door/Control Unit Tamper
Door/Control Unit Tamper Restored
Drift Compensation Error
Driver Error in Panel Download
Dual Custody User Off (Disarm)

Duct Alarm
Duct Alarm Restore
Duress
Duress Access Grant
Duress Disable
Duress Egress Grant
Duress Enable
EEPROM Fault
EEPROM Fault Restored
Early Close
Early Open
Early to Open From Alarm
Egress Denied
Egress Granted
Elevator Terminal Mode Access to Authorized Floors
Elevator Terminal Mode Default Floor
Elevator Terminal Mode Default Floor or User Entry of Destination Floor
Elevator Terminal Mode User Entry of Destination Floor
Embedded Analytics Failure
Embedded Analytics Restored
Emergency Alarm
Emergency Alarm Restore
Emergency Bypass
Emergency Close
Emergency Off
Emergency Open
Emergency Restore
Emergency Supervisory
Emergency Trouble
Emergency Trouble Restore
Emergency Unbypass
Employee Sign Off
Employee Sign On
End of Office Mode
Engineer Reset
Entry Exit
Entry/Exit Alarm Restore
Equipment Fail Restore
Equipment Failure Condition
Error
Event Log 50% Full
Event Log 90% Full
Event Log Reset
Event Recording Threshold Exceeded
Event Recording Threshold Restored
Event not Sent
Exception Open/Close
Exception Schedule Change
Exit Alarm
Exit Error
Exit Error - Zone
Exit Push Button Failure

Exit Request Denied: Interlock Area Busy
Expander Module DC Loss
Expander Module DC Loss Restore
Expander Module Failure
Expander Module Failure Restore
Expander Module Low Battery
Expander Module Low Battery Restore
Expander Module Reset
Expansion Device Missing
Expansion Device Tamper
Expansion Missing Restore
Expansion Module Fault
Expansion Module Fault Restored
Expansion Module Supervision
Expansion Module Supervision Restored
Expansion Module Tamper
Expansion Module Tamper Restore
Expansion Restore
Expansion Tamper Restore
Expansion Trouble
Extended Held Command Denied
Extended Held Command Set From Reader
Extended Held Open Mode Disabled
Extended Held Open Mode Enabled
External Deadbolt
External Deadbolt Off
External Device Condition
Extra Account
Extra Account Report
Extra Close Time
Extra Point
Extra RF Point
Face Detection (R)
Face Detection (R) Restored
Facial Detection
Facial Detection (C)
Facial Detection (C) Restored
Facial Detection Restored
Facility Code Only Mode Change Denied: Blocked Mode
Facility Code Only Mode Change Denied: Security Mode
Facility Occupancy Too High
Facility Occupancy Too High Restored
Facility Occupancy Too Low
Facility Occupancy Too Low Restored
Fail to Close
Fail to Communicate to RAM
Fail to Execute
Fail to Open
Fail to Open/Close
Fail to Receive Status Message
Fail to Receive Status Message Restore
Fail to Report

Fail to Report Restore
Fail to Test
Failed to Report Expected Event
Fap Processing Start
Fire Alarm
Fire Alarm Acknowledge
Fire Alarm Acknowledged Clear
Fire Alarm Block Acknowledge
Fire Alarm Cross Point
Fire Alarm In
Fire Alarm Out
Fire Alarm Restore
Fire Alarm Silenced
Fire Button Set
Fire Bypass
Fire Cancel
Fire Close
Fire Inactive
Fire Missing
Fire Open
Fire Restore
Fire Supervisory
Fire Supervisory Restore
Fire Supervisory Trouble
Fire Supervisory Trouble Restore
Fire Test
Fire Test Begin
Fire Test End
Fire Trouble
Fire Trouble Restore
Fire Unbypass
Fire Walk Test Ended
Fire Walk Test Started
Fire Zone Walk Tested
Firmware Download Completed
Firmware Download Failed
Firmware Download Started
Firmware Upgrade Failed: Low Battery
First Card Unlock Mode Change Denied: Blocked Mode
First Card Unlock Mode Change Denied: Security Mode
First Card Unlock Mode Disabled
First Card Unlock Mode Enabled
Flame Alarm
Flame Alarm Restore
Flame and Smoke Detection (C)
Flame and Smoke Detection (C) Restored
Flame and Smoke Detection (R)
Flame and Smoke Detection (R) Restored
Flame/Smoke Detection
Flame/Smoke Detection Restored
Foil Break Alarm
Foil Break Restore

Foodstamps Tender
Force Close Early
Force Close Late
Force Close Late Point
Forced Access
Forced Armed Perimeter Delay
Forced Armed Perimeter Instant
Forced Closing
Forced Perimeter Arm
Forced Point
Freeze Alarm
Freeze Alarm Restore
Freeze Bypass
Freeze Restoral
Freeze Supervisory
Freeze Trouble
Freeze Trouble Restore
Freeze Unbypass
Full Panel Download Completed
Full Panel Download Started
Gas Alarm
Gas Alarm Restore
Gas Bypass
Gas Restore
Gas Supervisory
Gas Test
Gas Trouble
Gas Trouble Restore
Gas Unbypass
Gasoline Prepayment
Gasoline Prepayment Refund
Gate Valve Sensor
Gate Valve Sensor Restore
Generic Event
Get Lock Mode Failed
Get Lock Mode Success
Global Linkage Action Executed
Global Linkage Action Failed
Grant Last User (Override)
Granted Access, Common Pin
Granted Double Card
Granted-Dual Custody
Granted-Escort
Granted-Exit-Dual Custody
Granted-Exit-Escort
Granted-Exit-Master
Granted-Master
Granted-Pending Entry
Ground Fault
Ground Fault Restore
Grounded Loop Alarm Active
Group Bypassed

Group Bypassed Restore
Guard Tour Action Executed
Guard Tour Action Failed
HSC Reset
HSC-IP Restored
HSC-IP Trouble
Heart Signal
Heat Alarm
Heat Alarm Restore
Heat Bypass
Heat Restore
Heat Supervisory
Heat Trouble
Heat Trouble Restore
Heat Unbypass
High Pitch Sounds
High Pitch Sounds Restored
High Temperature
High Temperature Restore
History Report End
History Report Start
Hold
Holdup Alarm
Holdup Alarm Restore
Holdup Bypass
Holdup Restore
Holdup Supervisory
Holdup Test
Holdup Trouble
Holdup Trouble Restore
Holdup Unbypass
Holiday Changed
Host Executed Function List
IVS Channel Processing Failed
IVS Channel Processing Restarted
IVS Connection Lost
IVS Connection Restored
IVS Engine Connection Lost
IVS Engine Connection Restored
Impact Sounds
Impact Sounds Restored
Improper ID Code
In-Camera-Memory Download Completed
In-Camera-Memory Download Failed
In-Camera-Memory Download Restored
In-Camera-Memory Download Started
Inactive
Inactive / Help
Inactive Badge
Incoming Call
Indefinite Suspension Initiated
Index Storage Threshold Exceeded

Index Storage Threshold Restored
Industrial Alarm
Information Message
Initialize Failed
Initialize Success
Initiated
Input Alarmed
Input Bypassed
Input Disabled
Input High
Input High High
Input Low
Input Low Low
Input Masked
Input Normal
Input Restored
Input Unmasked
Instant Command 16
Instant Command 17
Instant Command 18
Instant Command 19
Instant Command 20
Instant Command 21
Instant Command 22
Instant Method
Insufficient Frame Rate Detected
Insufficient Frame Rate Restored
Intercom Exchange Failure
Intercom Function
Interior Alarm
Interior Alarm Restore
Interior Pushbutton:
Interlock Area Busy
Internal Deadbolt
Internal Deadbolt Off
Intrude Verify
Intrude Verify Restore
Intruder High
Intruder Low
Intrusion Command Accepted
Intrusion Command Denied
Intrusion Zone Walk Tested
Invalid Access Level
Invalid Badge
Invalid Camera
Invalid Camera (C)
Invalid Camera (C) Restored
Invalid Camera (R)
Invalid Camera (R) Restored
Invalid Camera Restored
Invalid Card Format
Invalid Device Serial Number

Invalid Facility Code
Invalid Issue Code
Invalid Message
Invalid OEM Code
Invalid PIN Number
Invalid Programming Access
Invalid Remote Access
Invalid Report
Isolate
Item Correct of Previously Entered Item
Item Sold
Key Override
Keypad Buzzer Test Failed
Keypad Buzzer Test Success
Keypad Denied Blocked Mode
Keypad Denied Privacy State
Keypad Emergency
Keypad Fault
Keypad Fault Restored
Keypad Fire
Keypad Panic
Keypad Tamper
Keypad Tamper Restored
Keyswitch Armed Stay
LED Test Failure
LED Test Success
Lamp Test Activated
Lamp Test Complete
Latchkey Alert
Latchkey Supervision
Late Close
Late Open
Late to Close
Late to Open
Late to Open From Alarm
Legal Code Entry
Level Change
License Expiration Warning
Line Error Active
Line Fault
Line Status Normal
Listen-In Begin
Listen-In Ended
Listen-In to Follow
Load Database Failure
Load Database Success
Local I/O Executed Function List
Local Program
Local Program Denied
Local Program Fail
Local Program Success
Local Programming Ended

Lock Clock Get Failure
Lock Clock Get Success
Lock Initialized
Lock Powered Up by Portable Programmer
Lock Tamper
Lock Tamper Restored
Lock Type Read
Lock Updated
Locked Under AFC
Locked Under First Card Unlock
Log Overflow
Log Threshold
Logged In Success
Logged Out Success
Login Tamper
Loitering
Loitering (C)
Loitering (C) Restored
Loitering (R)
Loitering (R) Restored
Loitering Restored
Long Range Radio Transmit Fault
Long Range Radio Transmit Fault Restore
Loss of Central Polling
Loss of Central Polling Restore
Loss of Heat Alarm
Loss of Heat Alarm Restore
Loss of Radio Network
Loss of Radio Supervision
Loss of Radio Supervision Restore
Loss of Supervisory - RF
Loss of Supervisory - RF Restore
Loss of Supervisory - RPM
Loss of Supervisory - RPM Restore
Lottery Pay Out
Lottery Sale
Low Battery
Low Battery Man Down / Tether
Low Battery Pendant
Low Battery Personal Help Button
Low Battery Restored
Low Battery Security Lifeguard Unit
Low Battery Security Lifeguard Unit Restore
Low Battery Smoke
Low Battery Unit
Low Battery Watch / Pendant
Low Bottled Gas Level
Low Bottled Gas Level Restore
Low CO2
Low CO2 Restore
Low Received Signal Strength
Low System Battery

Low System Battery Restore
Low Temperature
Low Temperature Restore
Low Voltage
Low Voltage Restored
Low Water Level
Low Water Level Restore
Low Water Pressure
Low Water Pressure Restore
Man Down
Manual Test
Manufacturer Coupon
Manufacturer Coupon Redemption
Mask Group Alarm
Mask Group Alarm Cancelled
Mask Group Armed Away
Mask Group Armed Stay
Mask Group Armed Stay Instant
Mask Group Arming - Exit Delay
Mask Group Disarmed Fault
Mask Group Entry Delay
Max Access Levels Reached
Max Access Levels per Badge Reached
Max Assets Reached
Max Biometric Templates Reached
Max Cardholders Reached
Medic Button Set
Medic Pendant
Medic Watch / Pendant
Medical Abort
Medical Alarm
Medical Alarm Restore
Medical Bypass
Medical Close
Medical Inactive
Medical Open
Medical Restore
Medical Supervisory
Medical Trouble
Medical Trouble Restore
Medical Unbypass
Medication Reminder Off
Medication Reminder On
Memory Backup Battery Low
Memory Fail
Merchandise Returned
Message
Message Unknown
Miscellaneous Tender
Missing Alarm - Recent Closing
Missing Alarm Cross Point
Missing Alarm Exit Error

Missing Fire Supervisory
Missing Fire Trouble
Missing Supervision
Missing Trouble
Modify Auto Changes
Modify Holiday
Modify Timezone
Module Active
Module Cannot Receive Firmware when Encrypted
Module Clear
Motion Detected
Motion Detected (AI)
Motion Detected (AI) Restored
Motion Detected Restored
Multiplex Bus Fault
Multiplex Bus Fault Restored
Muster Mode Reset
Muster Mode Start
Near Alarm
Near Alarm Restore
Need Help Personal Help Button
Need Help Still
Need Help Unit
Negative Tax
Negative Total
Network Condition
Network Failure
Network Join
Network Join Failure
Network Join Success
Network Restore
Network Utilization Threshold Exceeded
Network Utilization Threshold Restored
New Log
No Acknowledgment Received+I601
No Activity
No Battery
No Biometric Template Data
No Blocking Override
No Escort Authority
No Intrusion Off or Stay Authority
No Motion Alarm
No Privacy Override
No Response to Acknowledgment
No Response to Handshake
No Sale
Non-Fire Active
Non-Fire Active Cleared
Non-Fire Cancel
Normal
Not Allowed
Not Available

Not Configured
Not Dialing
Notify Appliance Circuit #3
Notify Appliance Circuit #4
Object Crosses A Region (R)
Object Crosses A Region (R) Restored
Object Crosses a Region
Object Crosses a Region (C)
Object Crosses a Region (C) Restored
Object Crosses a Region Restored
Object Detection
Object Detection (C)
Object Detection (C) Restored
Object Detection (R)
Object Detection (R) Restored
Object Detection Restored
Object Left Behind
Object Left Behind (C)
Object Left Behind (C) Restored
Object Left Behind (R)
Object Left Behind (R) Restored
Object Left Behind Restored
Object Lurking
Object Lurking (C)
Object Lurking (C) Restored
Object Lurking (R)
Object Lurking (R) Restored
Object Lurking Restored
Object Moves Too Fast
Object Moves Too Fast (C)
Object Moves Too Fast (C) Restored
Object Moves Too Fast (R)
Object Moves Too Fast (R) Restored
Object Moves Too Fast Restored
Object Removed
Object Removed (C)
Object Removed (C) Restored
Object Removed (R)
Object Removed (R) Restored
Object Removed Restored
Object Starts To Move (R)
Object Starts To Move (R) Restored
Object Starts to Move
Object Starts to Move (C)
Object Starts to Move (C) Restored
Object Starts to Move Restored
Object Stops
Object Stops (C)
Object Stops (C) Restored
Object Stops (R)
Object Stops (R) Restored
Object Stops Restored

Octal Relay Module Communication Loss
Octal Relay Module Communication Restored
Office Denied Privacy State
Office First Denied Privacy State
One Ring Method
Open Area
Open Door Command Issued - Door Not Used
Open Door Command Issued - Door Used
Open Line Alarm Active
Open Lock Failed
Open Lock Success
Open Out of Window
Open/Close by User
Opening
Opening Keyswitch
Opening Out of Window by User
Opening Report
Opening by User
Operator Audit
Out of Service
Out of Time
Outdoor Alarm
Outdoor Restore
Output Error
Output State - Restore
Output State - Trouble
Overcurrent Restore
Overcurrent Trouble
Override Preprogrammed Price
Panel Badge Data Conflict
Panel Configuration Change
Panel Event Capacity Exceeded - Events Overwritten
Panel Free Memory Low
Panel ID Mismatch
Panel Invalid Login
Panel License Incorrect
Panel License Missing
Panel Marked Offline After Timeout
Panel Options Mismatch
Panel Power Up Complete
Panel Program Changed
Panel Reboot
Panel Reboot To Factory Defaults
Panel Reset Watchdog
Panel Restart
Panel Substitution
Panel Successful Login
Panel User Log Out
Panic 3 Button Remote
Panic Abort
Panic Alarm
Panic Alarm Restore

Panic Button Set
Panic Bypass
Panic Close
Panic Inactive
Panic Open
Panic Pendant
Panic Restore
Panic Supervisory
Panic Trouble
Panic Trouble Restore
Panic Unbypass
Panic Watch / Pendant
Panic Zone Walk Tested
Parameter Changed
Parameter Checksum Fail
Parameters Bad
Partial Arm
Pass Code Duress
Pay Out
Payment Toward Charge Account Balance
Payment of Refund to Customer
Pendant Transmitter Alarm
Pendant Transmitter Restore
Pending first user
People Counting
People Counting (C)
People Counting (C) Restored
People Counting (R)
People Counting (R) Restored
People Counting Restored
People Entry Rate Too High
People Entry Rate Too High Restored
People Entry Rate Too Low
People Entry Rate Too Low Restored
People Exit Rate Too High
People Exit Rate Too High Restored
People Exit Rate Too Low
People Exit Rate Too Low Restored
Perimeter Alarm
Perimeter Alarm Restore
Perimeter Armed
Perimeter Armed, User Defined
Perimeter Delay Armed
Periodic RF Transmission
Periodic Test Report
Periodic Test, System Trouble
Periodic Test, System Trouble Restore
Peripheral Disable
Permanent Close Schedule Changed
Permanent Open Schedule Changed
Phone Line Module Communication Loss
Phone Line Restore

Phone Line Trouble
Phone Module Communication Restored
Phone Test
Pick Up
Pod Trouble
Pod Trouble Restored
Point Bus Fail
Point Bus Restore
Point Closing
Point Disabled
Point Enabled
Point Opening
Point Test Fail
Point User Code Delete
Point User Code Restore
Point not Tested
Polling Loop Open
Polling Loop Open Restore
Polling Loop Open Trouble
Polling Loop Open Trouble Restore
Polling Loop Short
Polling Loop Short Restore
Polling Loop Short Trouble
Polling Loop Short Trouble Restore
Poor Video Visibility Detected
Poor Video Visibility Restored
Power Failure
Power Supply Restore
Power Supply Trouble
Power Up
Power Up Lock Failure
Power Up Lock Success
Pre-Alarm
Pre-Alarm Clear
Previously Reported
Price Lookup
Primary Communication Path Lost
Primary Communication Path Restored
Printer Down
Printer Offline
Printer Online
Printer Paper In
Printer Paper Out
Printer Restore
Printer Status
Printer Test
Printer Trouble
Program Mode Entry
Program Mode Exit
Protection Loop
Protection Loop Open
Protection Loop Open Restore

Protection Loop Restore
Protection Loop Short
Protection Loop Short Restore
Pull Station Alarm
Pull Station Alarm Restore
Pump Activated
Pump Activated Restore
Pump Failure
Pump Failure Restore
Quantity or Weight
Quick Arm
RAM Access Fail
RAM Access OK
RAM Bypass
RAM Checksum Bad
RAM Checksum Bad Restore
RAM Fault
RAM Fault Restored
RF Interference
RF Interference Restore
RF Keypad Fault
RF Keypad Fault Restored
RF Keypad Low Battery
RF Keypad Low Battery Restored
RF Receiver Restore
RF Receiver Tamper
RF Receiver Tamper Restore
RF Receiver Tamper Trouble
RF Receiver Trouble
RF Receiver Trouble Restored
RF Transmitter Low Battery
RF Transmitter Low Battery Restore
ROM Checksum Bad
ROM Checksum Bad Restore
ROM Fault
ROM Fault Restored
Radio Modem Fault
Radio Modem Fault Restored
Radio Network Restored
Radio Transmitter Disabled
Radio Transmitter Disabled Restore
Radio VSWR Trouble
Radio VSWR Trouble Restore
Re-Arm After Alarm
Read EEPROM
Read EEPROM Failure
Read EEPROM Success
Read Lock Audits
Read Lock Audits Failure
Read Lock Clock
Read Lock Information
Read Lock Type Failure

Read Lock Type Success
Read Network Data from ACU
Reader Authority Toggle
Reader Input Tamper
Reader Input Tamper Canceled
Reader Low Battery
Reader Low Battery Restored
Reader Mode Blocked
Reader Mode Card Only
Reader Mode Card and Pin
Reader Mode Card and Pin Unlocked
Reader Mode Cipher or Card
Reader Mode Facility Code
Reader Mode First Card Unlock
Reader Mode Locked
Reader Mode Office
Reader Mode Office First
Reader Mode PIN Only
Reader Mode Pin or Card
Reader Mode Secured
Reader Mode Security
Reader Mode Standard
Reader Mode Unlocked
Reader Mode Unsecured
Reader Module Firmware Upgraded
Reader Motor Stalled
Reader Motor Stalled Restored
Reader Offline
Reader Offline Restored
Reader Reset
Reader Toggle
Reader Very Low Battery
Reader in Dual Custody Mode
Reader in Escort Mode
Reader in Normal Mode
Realtime Clock Updated
Receiver Communication Fault
Receiver Communication Fault Restored
Receiver Fault
Receiver Fault Restored
Receiver Jammed
Receiver Jammed Restored
Receiver Line Card Restored
Receiver Line Card Trouble
Receiver Tamper
Receiver Tamper Restored
Recent Closing
Refrigeration Alarm
Refrigeration Alarm Restore
Register X Report
Register Z Report
Reject Command

Rejected Biometric Score
Relay Close
Relay Contact Activated
Relay Contact Deactivated
Relay Open
Relay Reset
Relay Reset by Programmer
Relay Reset by RAM
Relay Reset by Schedule
Relay Reset by User
Relay Set
Relay Set by Programmer
Relay Set by RAM
Relay Set by Schedule
Relay Set by User
Remote Closing
Remote Link Active
Remote Link Inactive
Remote Opening
Remote Program
Remote Program Begin
Remote Program Denied
Remote Program Fail
Remote Program Success
Remote Programmer Call Failed
Remote Reset
Remote System Shutdown
Remote Up/Down Disable
Repeater Failure
Repeater Failure Restore
Request to Enter
Request to Enter Denied
Request to Exit
Request to Exit - Door Not Used
Request to Exit - Door Used
Request to Exit Denied
Reserved Event
Restore - Keyfob Device
Restore Condition
Retrieved
Reversing Relay
Reversing Relay Disable
Reversing Relay Disable Restore
Reversing Relay Restore
Ringing
Runaway Device
Runaway Device Restored
Runaway System
Runaway System Restored
SDI Device Fail
SDI Device Restoral
SIA Session Code

Sale Subtotal
Schedule Changed
Schedule Executed
Schedule Resumed
Schedule Suspended
Scheduler Action Executed
Scheduler Action Failed
Secondary Communication Path Lost
Secondary Communication Path Restored
Security Alarm Acknowledge
Security Alarm Block Acknowledge
Security Alarm In
Security Alarm Out
Security Denied Blocked Mode
Security Denied Privacy State
Security Mode Card Not Swiped
Security Passage Denied Blocked Mode
Security Passage Denied Privacy State
Self-Test Fail
Self-Test Fail Restore
Senior Watch Trouble
Sensor Reset
Sensor Self Test Fail
Sensor Supervisory Fail
Sensor Tamper
Sensor Tamper Restore
Sensor Tamper Trouble
Sensor Tamper Trouble Restore
Sensor Trouble
Sensor Trouble Restore
Sensor Watch Trouble
Serial Interface Device Communication Loss
Serial Interface Device Communication Restored
Serial Interface Device Receive Error
Serial Interface Device Receive Error Restored
Serial Interface Device Transmit Error
Serial Interface Device Transmit Error Restored
Service Completed
Service On/Off Premise
Service Requested
Service Required
Service Walk Test Ended
Service Walk Test Started
Shorted Line Alarm Active
Shunted
Signal Silence
Silent Alarm
Silent Alarm Restore
Silent Burglary Alarm
Silent Burglary Alarm Restore
Slot/Line Caller Unknown
Slot/Line Codec Error

Slot/Line Communication Error
Slot/Line Communication Restore
Slot/Line Data Error
Slot/Line No Call Number
Slot/Line No Data Received
Slot/Line Private Call
Slot/Line Reset
Smart Card Authentication Failed
Smart VMD
Smart VMD (C)
Smart VMD (C) Restored
Smart VMD (R)
Smart VMD (R) Restored
Smart VMD Restored
Smoke Alarm
Smoke Alarm Restore
Smoke Detector High Sensitivity
Smoke Detector High Sensitivity Restore
Smoke Detector Low Sensitivity
Smoke Detector Low Sensitivity Restore
Solid State Telegraph Box Transmission
Sunder/Relay Disabled
Sunder/Relay Disabled Restore
Sunder/Relay Trouble
Sunder/Relay Trouble Restore
Sprinkler Alarm
Sprinkler Alarm Restore
Sprinkler Bypass
Sprinkler Restore
Sprinkler Supervisory
Sprinkler Trouble
Sprinkler Trouble Restore
Sprinkler Unbypass
Standard Denied Privacy State
Status - Alarm
Status - Analog Service
Status - Close
Status - Close Late
Status - Close by Area
Status - Door Forced
Status - Door Left Open
Status - Fire Alarm
Status - Fire Missing
Status - Fire Supervision
Status - Fire Trouble
Status - Log Overflow
Status - Log Threshold
Status - Missing Alarm
Status - Missing Fire Supervision
Status - Missing Supervision
Status - Missing Trouble
Status - Open

Status - Open by Area
Status - Parameters Bad Checksum
Status - Perimeter Delay
Status - Perimeter Delay Receiver 01
Status - Perimeter Instant
Status - Power Fail
Status - RF Battery Low
Status - RF Receiver Tamper
Status - RF Tamper Alarm
Status - RF Tamper Trouble
Status - Restoral
Status - SDI Failure
Status - Supervision
Status - Trouble
Status - User Tamper
Status In
Status Out
Status Perimeter Delay Armed
Status Perimeter Instantly Armed
Status Report
Still Need Help
Stop Two-Way Audio
Storage Failure
Store Coupon
Success - Download Access
Successful Upload
Supervision Rate Changed
Supervisory
Supervisory Acknowledge
Supervisory Block Acknowledge
Supervisory In
Supervisory Out
Supervisory Zone Bypassed
Supply Fuse Restored
Supply Fuse Trouble
Suspended Account Manual Restore
Swinger Bypassed
Swinger Bypassed Restore
Swinger Trouble
Swinger Trouble Restore
Switch Test Failed
Switch Test Success
Switch to Fallback Mode
Switch to Intercept Mode
System APB Reset
System Battery Missing
System Battery Trouble
System Confirm
System Confirm Alarm Reset
System Disable
System Inactivity
System Message

System Password Fail
System Peripheral
System Peripheral Restore
System Power Restore
System Program Changed
System Program Fail
System Reset
System Reset (fire_system_reset)
System Restored
System Shutdown
System Time Lost
System Trouble
System Unconfirm
Tamper Alarm
Tamper Alarm Restore
Tamper Bypass
Tamper Restore
Tamper Trouble
Tamper Trouble Restore
Tamper Unbypass
Tank Level
Tax Amount
Taxable Subtotal
Telco (SIA/CID) Reset
Telco Line 1 Fault
Telco Line 2 Fault
Telco Line Fault 1 Restore
Telco Line Fault 2 Restore
Temperature Alarm
Temporary Close Schedule Changed
Temporary Code Expiration Date Changed
Temporary Open Schedule Changed
Temporary Suspension Expired
Temporary Suspension Initiated
Test - Alarm
Test - Close
Test - Open
Test - Restore
Test End
Test Failed
Test Key
Test Key Failure
Test Key Success
Test Report
Test Report (intercom_test_report)
Test Start
Test off Normal
Tether
Time Changed
Time Out-Of-Sync
Time Out-Of-Sync Restored
Time/Date Inaccurate

Time/Date Inaccurate Restore
Time/Date Set
Timeout Exceeded - No Second Card
Total Amount Due
Transaction Number
Transfer, Diagnostics
Transfer, History
Transfer, PDA to Lock
Transmitter Acknowledge
Transmitter Alarm
Transmitter Alarm Restored
Transmitter Battery Restore
Transmitter Battery Trouble
Transmitter Inactivity
Transmitter Low Battery
Transmitter Low Battery Restored
Transmitter No Response
Transmitter Pre-Tilt
Transmitter Pre-Tilt Restored
Transmitter Pull Cord Alarm
Transmitter Pull Cord Restored
Transmitter Removal Alarm
Transmitter Tamper
Transmitter Tamper Restored
Transmitter Temporary Tilt Disable
Transmitter Tilt
Transmitter Tilt Disabled
Transmitter Tilt Enabled
Transmitter Tilt Restored
Transmitter Touch Alarm
Trouble Acknowledge
Trouble Acknowledged Clear
Trouble Alarm Relay
Trouble Alarm Relay Restore
Trouble Bell 1
Trouble Bell 1 Restore
Trouble Bell 2
Trouble Bell 2 Restore
Trouble Block Acknowledge
Trouble Condition
Trouble In
Trouble Out
Trouble Relay
Trouble Relay Disable
Trouble Relay Disable Restore
Trouble Relay Restore
Trouble Report
UPS AC Fail
UPS AC Restore
UPS Battery Low
UPS Battery Restore
USB 1 Fuse Blown

USB 1 Fuse Reset
USB 2 Fuse Blown
USB 2 Fuse Reset
Unable to Send Command
Unanswered Call
Unauthorized Off
Unblocked
Unbypass - Open
Unclassified Sounds
Unclassified Sounds Restored
Undefined
Unexpected Access
Unexpected Access Attempt
Unknown Cause
Unknown Elevator Terminal
Unknown Event
Unknown Message
Unknown User Command
Unlocked Mode Change Denied: Blocked Mode
Unlocked Mode Change Denied: Low Battery
Unlocked Mode Change Denied: Security Mode
Unlocked Under AFC
Unlocked Under First Card Unlock
Unsuccessful Remote Access
Unsupported Hardware
Untyped Abort
Untyped Alarm
Untyped Alarm Restore
Untyped Bypass
Untyped Close
Untyped Inactive
Untyped Missing Alarm
Untyped Missing Trouble
Untyped Open
Untyped Restore
Untyped Trouble
Untyped Trouble Restore
Untyped Zone Alarm
Untyped Zone Bypass
Untyped Zone Restore
Untyped Zone Supervisory
Untyped Zone Trouble
Untyped Zone Trouble Restore
Untyped Zone Unbypass
Unverified Burglary Event
Unverified Event
Unverified Fire Event
Update Lock Clock Failure
Update Lock Clock Success
Update Lock Failure
Update Lock Success
Update: Now able to Achieve Current Required Storage Setting

Upload Lock Audits Failure
Upload Lock Audits Success
Upload Okay
Upload Portable Programmer Audits Failure
Upload Portable Programmer Audits Success
Use Limit Exceeded
User APB Reset
User Alarm
User Alarm Command 7
User Alarm Command 9
User Code Added
User Code Changed
User Code Deleted
User Code Tamper
User Failed to Reach Destination
User Generated Video Event
User Level Set
User on Premises
Valid Programming Access
Valid Remote Access
Value Added
Verify User
Video Event Threshold Reached
Video Failover Failed
Video Failover Restored
Video Failover Started
Video Overflow Restored
Video Overflow Started
Video Server Disk Full
Video Server is not Recording
Video Source Signal Lost
Video Source Signal Restored
Video Storage Unavailable
Video Transmitter Active
Video Transmitter Active Restore
View Lock Audits
View Lock Audits Failure
View Lock Info Failure
View Lock Info Success
View Portable Programmer Audits Failure
View Portable Programmer Audits Success
Void or Error Correction
WLM Firmware Upgraded
Walk Test ##
Walk Test Ended
Walk Test Point
Walk Test Started
Walk Test Uninstalled
Walk Test Unprogrammed
Walk Test Untest
Walk of Test Accounts
Wandering Patient Alarm Reset

Wandering Patient at Door
Warning - Users Left In Area
Warning: Unable to Achieve Current Required Storage Setting
Warning: Unable to Meet Required Storage Setting! Deleting Oldest Video
Was Forced Armed
Watch Mode
Watchdog Reset
Water Alarm
Water Alarm Restore
Water Bypass
Water Flow Alarm
Water Flow Alarm Restore
Water Leakage Alarm
Water Leakage Alarm Restore
Water Restore
Water Supervisory
Water Trouble
Water Trouble Restore
Water Unbypass
Window Length Changed
Wireless Smoke Detector
Write Door Config
Write Fixed Pin
Write Network Data
Write-Back Error
Wrong Code Entry



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



The Open Platform Company