Milestone XProtect Access OnGuard User Manual

Prepared by: <u>Brian Hayes, Sof</u>tware Developer, Custom Development Americas





Table of Content

Copyright, Trademarks & Disclaimers	4
Copyright	4
Trademarks	4
Disclaimer	4
Version Compatibility	5
Matrix	5
XProtect Version details	5
OnGuard Version details	5
Hardware Support	6
Scalability	6
OnGuard Certification Tested Setup	6
Events Handled	6
General Description	7
Introduction	7
Solution overview	8
Prerequisites	8
Time Synchronization	8
SQL Server: Configure OnGuard SQL for remote connections	8
.NET Framework: Installation on OnGuard Server machine	9
Milestone XProtect [®] : License Options	9
Milestone XProtect [®] : Event Server machine DNS / Name resolution	9
Milestone XProtect [®] : Smart Client Profiles	10
OnGuard: License Options	10
OnGuard: Mandatory Windows Services	10
OnGuard: Generate software events settings	11
OnGuard: Create Single Sign-On (SSO) Directory	11
OnGuard: Create Single Sign-On (SSO) User	12
OnGuard: Enterprise Configurations	14
Installation	16
ACM Server Installation	17
ACM Server Credentials	18
ACM Server: OnGuard Plugin Installation	19
ACM Server: OnGuard Plugin Post-Installation	20
ACM Server: XProtect ACM MIP Plugin	21
MIP Plugin Upgrades	22
OnGuard Configuration	23
Configure to run as OnGuard Single-Sign-On Account	23
Reducing Permissions	26
XProtect ACM MIP Plugin Configuration	27



ACM Server Wizard	27
Installing an ACM Server	27
Uninstalling an ACM Server	32
XProtect Management Client Configuration	33
XProtect Management Client	33
Properties	34
Reducing Permissions	40
Personalized Login	41
Common Actions	45
Editing OnGuard Event Types	45
Searching for cardholders	46
Defining alarms based on OnGuard events	48
Defining rules based on OnGuard events	53
XProtect [®] Smart Client Maps	56
XProtect [®] Access Monitor tiles	57
Alarm Acknowledgment	58
Fetching OnGuard event types	59
Defining cardholder properties to display in Milestone XProtect	60
Logging	60
Gathering the logs	61
Changing logging level	61
Troubleshooting Guide	62
OnGuard loses communication with the access control hardware	62
Failure of the ACM plugin to communicate with Window	
Management Interface (WMI)	62
Milestone Event Server MIP Plugin cannot communicate with the	
ACM Server (DataCondulT only)	63
Debug log shows SqlAccess.connect() failed	63
Failure to connect to SQL Server	63
Not receiving card holder or badge changes	64
Optimizing Event Processing Performance	64
Refreshing cardholders	65
WMI related errors	66
OnGuard OpenAccess connectivity	66
XProtect [®] Smart Client not showing alarm panels or their	
inputs/outputs	66
OnGuard ACM integration flooding user transaction report	67
OnGuard ACM instance is not displayed in the XProtect®	
Management Client	67
LS OpenAccess service automatically stops seconds after starting	67
I/Os connected to OSDP readers are no longer detected	68
LS OpenAccess fails to send any events when running in an	
Enterprise configuration	68
All other support issues	68
Known issues	68



Copyright, Trademarks & Disclaimers

Copyright

© 2019 Milestone Systems.

Trademarks

XProtect[®] is a registered trademark of Milestone Systems. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This document is intended for general information purposes only, and due care has been taken in its preparation. Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty. Milestone Systems A/S reserve the right to make adjustments without prior notification. All names of people and organizations used in this document's examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended. This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file *3rd_party_software_terms_and_conditions.txt* located in your Milestone surveillance system installation folder.

lestone 🔶

Version Compatibility

Matrix

Here is the compatibility matrix between OnGuard and Milestone XProtect.

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

OnGuard	XP 2016 R3	XP 2017 R1-R3	XP 2018 R1-R3	XP 2019 R1	XP 2019 R2
7.0	U*	U*	U*	U*	U*
7.1	S	S	S	S	S
7.2	S	S	S	S	S
7.3	S	S	S	S	S
7.4	S	S	S	S	Т
7.5	S	S	S	S	Т

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

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

XProtect Version details

Version	Version Information
XProtect 2016 R1-R2	While these versions of XProtect remain compatible with the XProtect Access OnGuard integration, they do not however support user privileges and alarm acknowledgement functionality. Milestone does not recommend using these versions of XProtect for the OnGuard integration
XProtect 2016 R3	First version to add support for Alarm Acknowledgement in OnGuard
XProtect 2017 R1-R3	These versions are fully supported*
XProtect 2018 R1-R3	
XProtect 2019 R1-R2	

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

OnGuard Version details

Version	Minimum update / patch level	Version Information
OnGuard 7.0	7.0.1107.0	This OnGuard version is end-of-life from Lenel and is no longer supported. Milestone follows the support lifecycle of OnGuard for the integration.
OnGuard 7.1 OnGuard 7.2	7.1.481.74 7.2.269.67	Make sure OnGuard is on at least version 7.1.481.74 or 7.2.269.67. Some bugs in DataCondulT prevent the integration from working on older versions of 7.1 / 7.2
OnGuard 7.3	7.3.345.0	These versions are fully supported



OnGuard 7.4 RTM	7.4.457.0	
OnGuard 7.4 Update 1	7.4.457.69	OnGuard has issues detecting I/Os on OSDP connected readers.
OnGuard 7.5	7.5.375.0	This version is fully supported

Hardware Support

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



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

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

Scalability

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

OnGuard Certification Tested Setup

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

Events Handled

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

	DataCondulT	OpenAccess
Number of events sent from OnGuard	15,000	15,000
Time to send 15,000 events by OnGuard	3 minutes	11 minutes
Number of events received in XProtect	15,000	15,000
Time to receive 15,000 events in XProtect	4 minutes	26 minutes
Nb of events that had associated alarms in XProtect	10,200	10,200
Event Throughput from OnGuard to XProtect	15,000 evts / 4 mins	15,000 evts / 26 mins
	62.5 events / second	9.61 events / second





Alarm Generation Throughput (XProtect)	10,200 alarms / 4 mins	10,200 alarms / 26 mins
	42.5 alarms / second	6.5 alarms / second
XProtect Version	2018 R2	2018 R2
XPA Version	3.0.18262	3.0.18262
OnGuard Version	7.4.457.69	7.4.457.69
Test Date	September 20, 2018	September 19, 2018

General Description

Introduction

7

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

- Retrieve configuration from the OnGuard AC system, e.g. doors and event types
- Receive AC event streams and state changes from the OnGuard system
- Get/Search cardholder information with picture association
- Create alarms in alarm manager based on AC events.
- Alarm state synchronization between XProtect (2016 R3 or greater) and OnGuard when the alarm is acknowledged in XProtect. Alarm acknowledgment synchronization when the alarm is acknowledged in OnGuard is not implemented due to the lack of support for this feature in the OnGuard SDK.
- Association of access control events to cameras for simultaneous display of events and video
- Select and categorize the events the user wants to view from the OnGuard system
- Trigger rules or actions based on access events e.g. start recording, go to PTZ preset, display access
 request, send camera to matrix and system actions such as activate output or trigger manual event. With
 XProtect Corporate and Expert this functionality is extended to full use of the event as a triggering
 mechanism for the rules system.





Solution overview



The solution provided is split in 3 components:

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

Prerequisites

Time Synchronization

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

SQL Server: Configure OnGuard SQL for remote connections

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

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



i. Enable TCP/IP protocol for port 1433

SOL Server Configuration Manager (Local) SOL Server Services SOL Server Network Configuration (32bit) SOL Native Client 11.0 Configuration SOL Server Network Configuration Protocols for MSSQLSERVER SOL Vision Client 11.0 Configuration	Protocol Name Status Shared Memory Enabled Named Pipes Enabled TCP/IP Properties	? >
	Protocol IP Addresses Protocol IP Addresses Active Enabled IP Address TCP Dynamic Ports TCP Port IP Address TCP Dynamic Ports TCP Port IP Address TCP Dynamic Ports TCP Port IP3 Active Enabled IP Address TCP Dynamic Ports TCP D	Yes • No • fe80::9da4:cb3b:d4ef:e09%4 • 1433 • Yes • No • 172.28.152.179 • 1433 • Yes • No • 172.28.152.179 • 1433 • Yes • No • 11 • 1432 •

4. Restart the SQL Server database server.

.NET Framework: Installation on OnGuard Server machine

.NET Framework 4.5 must be installed on the OnGuard server machine (dotnetfx45_full_x86_x64.exe). This is mostly for older OS editions, anything above Windows 8 and Windows 2012 Server will have it already installed as part of the OS. Milestone recommends that you use Microsoft Windows Server Editions of the OS.

Milestone XProtect®: License Options

The customer must have Milestone XProtect Access enabled (1) and the appropriate number of doors (2) in their XProtect SLC. See the management client license screen for more details.

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

-	
-	
-	

License Type	Activated	
Hardware Device	13 out of 25	
Access control door	7 out of 29	2

Milestone XProtect®: Event Server machine DNS / Name resolution

License Details - All Sites...

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



milestone

Milestone XProtect®: Smart Client Profiles

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

	M	lestone XProtect Management Client 2016	_ D X
File Edit View Action Tools Help			
🖶 🦻 🕜 🗢 🛱			
Site Navigation	Properties 09		9
🖃 🞲 WIN-7F1AKEGTGKC - (10.0 🔒	🖃 🚰 Smart Client Profiles (sorted by p	Smart Client profile settings - Access Control	
Basics	👷 Default Smart Client Profile	Title Setting	Locked
- 🔚 License Information		Show access request notifications Yes	· · □
Site Information			
Remote Connect Service			
Axis One-click Camer 😑			
E Servers			
Recording Servers			
Failover Servers			
E 😵 Devices			
🖉 Microphones			
Speakers			
- 🕎 Metadata			
o Input			
Output			
🖻 🖳 Client			
Smart Wall			
View Groups			
Smart Client Profiles			
Management Client P			
Matrix			
< III II X			
Site Navigation Federated Site Hier	< III >	🚺 Info 🛃 General 💫 Advanced 🖙 Live 🗞 Playback 🍪 Setup 🗞 Export 🚈 Timeline 🎼 Acc	ess Control 🛄 Vie < 🗲

OnGuard: License Options

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

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

OnGuard: Mandatory Windows Services

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

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



OnGuard: Generate software events settings

General System Options	General Asset Options	Web Applications	Client Update	Hardware Settings	Anti-Passback	Biometrics	User Commands	•	2
Log on authorization wa	aming		Pase	sword options					

None v Text	Enforce strong passwords
DataCondulT service ☑ Generate software events	FIPS mode
Set for DataConduIT	Configuration Download Service host
Monitoring 3 Number of days to save queued events Specify monitor zone assignments	Message Broker Service host BHA-LENEL-02 Browse
Linkage Server host BHA-LENEL-02 Browne	OpenAccess host BHA-LENEL-02 Browse Browse Browse
Set to Lenel OnGuard Server Machin	ne Set for OpenAccess
0K. Cancel	Help Close

Under Administration, System Options:

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

OnGuard: Create Single Sign-On (SSO) Directory

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

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

Using the OnGuard System Administration app:

Select Administration -> Directories from the application menu

_	
	<u>C</u> ardholders
	<u>V</u> isits
	Asse <u>t</u> s
	<u>R</u> eports
	Card <u>F</u> ormats
	<u>B</u> adge Types
	Directories
	Users

DataCondulT

OpenAccess



For DataCondulT support, the single sign-on ac- count MUST be a "Windows Local Account".	For OpenAccess support, the single sign-on ac- count MUST "Allow manual signal sign-on" as shown below.		
Directories	Directories		
Name ^ˆ Type ✓ BHA-LEN Windows Local Accounts Image: BHA-LENELA Type: Type: Image: BHA-LENELA Type: Image: BHA-LENELA Image: BHA-LENELA Browse Image: BHA-LENELA Browse	Name Type ✓ custdev.us Microsoft Active Directory Mane: custdev us Type: Microsoft Active Directory Domain: bustdev us bustdev us Browse Use SSL Pot: 393 Start node: de-custdev, dc=us Enable angle sign-on ✓ Enable angle sign-on ✓ Alow manual single sign-on		

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

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

OnGuard: Create Single Sign-On (SSO) User

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

Select Administration -> Users from the application menu in System Administration		Add a new user.
Ad	ministration Access Control Monit	
	<u>C</u> ardholders	
	<u>V</u> isits	
	Asse <u>t</u> s	
	Reports	
	Card <u>F</u> ormats	
	<u>B</u> adge Types	
	Directories	
	Users	







Internal Account tab	Permission Group tab
- Make sure that the "User has internal ac-	Assign the following permission groups:
count" checkbox is checked.	System = System Admin
- Enter login credentials.	Cardholder = Cardholder Admin
General Directory Accounts Internal Account Permission Groups	Monitor = Monitor Admin
User has internal account	Reports = Full Access
User name:	Field/page = View/Edit All Fields
ВНА	General Directory Accounts Internal Account Permission Groups
Password	System:
	System Admin V
	Cardholder:
Confirm password:	Cardholder Admin
•••••	Monitor:
	Monitor Admin 🗸
	Reports:
	<full access=""></full>
	Field/page:
	View/Edit All Fields \checkmark

OnGuard: Enterprise Configurations

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



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









Installation

The installation package consists of three independent installers:

- Milestone.ACMServer.msi: Installer for the <u>ACM Server</u>
 Installed on the OnGuard server machine
- 2. Milestone.ACMServer.OnGuard.msi: Installer for the OnGuard ACM Server plugin
 - Installed on the OnGuard server machine, after the ACMServer.
- 3. Milestone.ACMServer.MipPlugin.msi: Installer for the XProtect Event Server ACM MIP Plugin
 - Installed on the XProtect Machine that hosts the Event Server Windows service

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



It is mandatory that the <u>same version</u> of the OnGuard ACM integration be installed on both the XProtect and OnGuard machines.





ACM Server Installation





ACM Server Credentials

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

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

Services							- 0	×
File Action View	Help							
(n n n n n n n n n n n n n n n n n n n	à 🖦 🛛 📰 🕨 🔳 II 🕨							
Services (Local)	Services (Local)	-						
	Milestone ACM Server	Name	C	escription	Status	Startup Type	Log On As	^
	Stop the service Restart the service	Microsoft Passport Co Microsoft Software Sh Microsoft Storage Spa Microsoft Storage Spa	ontainer M Iadow M Ices S H	/lanages lo /lanages so lost service		Manual (Trig Manual Manual	Local Service Local System Network Service	
	Extended / Standard /	Mileton ACM Serve Miletone ACM Serve Meliopon Meliopon Network Connt Network Connt Network Connt Network Connt Network Connt Network Connt Network Locati Network Stole Contine Elect	Start Stop Pause Resume Restart All Tasks Refresh Propertie: Help	· · · · · · · · · · · · · · · · · · ·	Running Running Running Running Running	Automatic Manual Disabled Automatic Manual (Trig Manual Automatic Manual (Trig Manual Cautomatic Manual (Trig Automatic Disablad	Local System Local System	•

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

Milestone ACM Server	Properties (Local Computer)	×
General Log On Rec	covery Dependencies	
Log on as:		
Local System according Allow service to	unt interact with desktop	
This account:	custdev.us\bha Browse	
Password:	•••••	
Confirm password:	•••••	
	OK Cancel Appl	y



ACM Server: OnGuard Plugin Installation

Copy the "Milestone.ACMServer.OnGuard.msi" file	There are no configurable options in this installer.
to a temporay folder and double-click to install, you	When you are ready, press install.
should see a screen similar to the following:	🖟 Milestone ACM Server: LenelOnGuard Plugin Setup
😥 Milestone ACM Server: LenelOnGuard Plugin Setup 📃 💻 🗙	Ready to install Milestone ACM Server: LenelOnGuard Plugin milestone
Welcome to the Milestone ACM Server: LenelOnGuard Plugin Setup Wizard	Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
The Setup Wizard will Install Milestone ACM Server: Lenel@Gusard Plugin on your computer. Click Next to continue or Cancel to exit the Setup Wizard.	2
Back Next Cancel	Back Tristall Cancel
The OnGuard plugin automatically detects the	
presence of both the OnGuard server and the pre-	
installed ACM Server. If either is missing it will	
refuse to install.	
Install progress	You have successfully installed the Milestone ACM
🖟 Milestone ACM Server: LenelOnGuard Plugin Setup	Server OnGuard Plugin
Installing Milestone ACM Server: LenelOnGuard Plugin milestone	🕼 Milestone ACM Server: LenelOnGuard Plugin Setup
Please wait while the Setup Wizard installs Milestone ACM Server: LenelOnGuard Plugin.	The space calculations compared to the Milestone ACM Server: LenelOnGuard Plugin Setup Wizard
Status: Updating component registration	Click the Finish button to exit the Setup Wizard.
	4
Back Next Cancel	Back Einish Cancel

ACM Server: OnGuard Plugin Post-Installation

🐌 ⊋ 🐌 =	C:\ProgramData\VideoOS\Ser	viceHost\logs		_ □)	K
File Home Share V	iew			\sim	0
€ 🔿 ▾ ↑ 🚺 C:\Progr	amData\VideoOS\ServiceHost\logs	✓ C	Search logs	۶	2
👢 VideoOS	^ Name	Da	ate modified	Size	Ту
ServiceHost	AssemblyScanner-W12-ONG	JARD-LAB.I 5/	11/2016 11:22 A	1 KB	Те
Services	VideoOS.ServiceHost-W12-O	NGUARD-L 5/	11/2016 11:22 A	2 KB	Те
		III			>
2 items 1 item selected 1.5	9 KB				
/ Vid	eoOS.ServiceHost-W12-ONGUAR	D-LAB.log - N	otepad	_ D ×	(
File Edit Format View Help	>				
11:22:17 Services Manager Dependency Resolver: Looking for VideoOS.ACMServer, Version=1.0.0.0, Culture=neutral, PublicKeyToken=86812e601a776f67 11:22:17 Services Manager Dependency Resolver: Found C:\ProgramData\VideoOS \ServiceHost\Services\VideoOSACMServerService\VideoOS.ACMServer.dll that matches assembly name VideoOS.ACMServer 11:22:19					
======================================	Server Server Module v1.0 (c	:=========== 2013-2016			
11:22:19 Server modul 11:22:19	e address : http://lo	calhost:8000)/ACMServer		≡
11:22:19 Found 1 ACM 11:22:19 - Lenel OnGu	Server Plugins: ard - 121cbe86-bf5b-4465-990)0-4115334c83	3c1		
					Ť.

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





ACM Server: XProtect ACM MIP Plugin

Copy the "Milestone.ACMServer.MipPlugin.msi" file to a 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"

Milestone ACM Server: MIP Plugin Setup	
Ready to install Milestone ACM Server: MIP Plugin	milestone
Click Install to begin the installation. Click Back to review or change an installation settings. Click Cancel to exit the wizard.	y of your
<u>B</u> ack Install	Cancel



Installation progress...

Milestone ACM Server: MIP Plugin Setup	
Installing Milestone ACM Server: MIP Plugin	mileston The open platform comp
Please wait while the Setup Wizard installs Milestone ACM Server: N	1IP Plugin.
Status:	
Port/	ovt
Dack 19	

You have successfully installed the ACM MIP Plugin for ACM Server



MIP Plugin Upgrades

•

- IMPORTANT Always upgrade *both* the ACM Server and OnGuard ACM plugin on the OnGuard machine *before* upgrading the MIP Plugin. We distribute all the installers with every new OnGuard ACM release.
- Automatic MIP Plugin upgrades of configured and installed instances in the Management Client are supported for all versions of the OnGuard ACM integration.
- Simply run the MIP Plugin installer; it will upgrade any installed ACM Servers.
 - After running the MIP Plugin installer, for each ACM instance in the Management Client:
 - Set the "Connection Profile" property to the name of the ACM Server machine. Press Save to save the configuration change.
 - Click Refresh Configuration to update the configuration.



milestone

Upgrading will result in the following negative side-effects:

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

OnGuard Configuration

Configure to run as OnGuard Single-Sign-On Account

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

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





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





O _		Service	S			_ □	x
File Action Vie	w Help						
le 🔿 🖬 🖬 Q							
🧠 Services (Loca	Services (Local)						
	Milestone ACM Server	Name 🔷	Description	Status	Startup Type	Log On As	^
	Stop the service Restart the service	LS Site Publication Set LS Video Archive Serv Microsoft iSCSI Initiat. Microsoft Software Sh Microsoft Storage Sp	r This service er The Video Manages In h Manages so Host service		Manual Manual Manual Manual Manual	Local Syst Local Syst Local Syst Local Syst Network S	
		Milestone ACM S		Punning	Automatic	\dbe	
		 Multimedia Class Net.Tcp Port Shat Netlogon Network Access F Network Connect Network Connect Network List Serv Network Location Network Store In Ontimize drives 	Start Stop Pause Resume Restart All Tasks Refresh Properties Help	► Inning Inning Inning	Manual Disabled Manual Manual Manual Manual Automatic Automatic Manual	Local Syst Local Servi Local Syst Network S Local Syst Local Syst Local Servi Network S Local Servi	H
< III >	\Extended (Standard /						_

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



Milestone ACM	I Server Properties (Local C	Computer) 🔀
General Log On Recover	ry Dependencies	
Log on as:		
O Local System account		
Allow service to inte	eract with desktop	
This account:	.\dbe	Browse
Password:	•••••	
Confirm password:	•••••	
	OK Cancel	Apply

IMPORTANT: Restart the Milestone ACM Server service.

Reducing Permissions

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



XProtect ACM MIP Plugin Configuration

ACM Server Wizard

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



Installing an ACM Server

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





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

ACM	Server Configuration Wizard		
Add an ACM Server			
Please enter the addr	ress of an ACM Server you wish to connect to:		
ACM Server Address:			
ACM Server Port:	8443		
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
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 OnGuard machine is not running with sufficient administrative privileges.

ACN	I Server Configuration Wizard
	Add an ACM Server
Please enter the add	ress of an ACM Server you wish to connect to:
ACM Server Address:	192.168.100.135
ACM Server Port:	8443
Use SSL	Incorrect IP information
Could not successfully co	ntact the ACM Server
	< 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 OnGuard.

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				
Lenel OnGuard-OnGuardAcmServer				
Add				
< Back Next > Finish				

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





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

	ACM Server Configuration Wizard	x
The follo	What is going to happen owing actions will be performed:	
Plugins t	to be installed:	
USCusto	omDev04 (192.168.100.134)	
Install Le	enel OnGuard-OnGuardAcmServer	
Plugins (to be uninstalled:	
	< Back Next >	Finish

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



ACM Server Configuration Wizard	٢				
Operations complete					
Operations complete					
Plugins installed:					
USCustomDev04 (192.168.100.134)					
Install Lenel OnGuard-OnGuardAcmServer					
Plugins uninstalled:					
< Back Next > Close					

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.

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 I nel OnGuard-OnGuardAcmServer				
Add < Back Next > Finish				



XProtect Management Client Configuration

XProtect Management Client

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

a Edit View Action Tools Help						
e Luic view Action Tools Help						
9 🥑 🗢 曲						
e Navigation	Access	Control	Access D	ontrol Infor	mation	
VM-MILESTONE Basics Elimetry License Information	{J	Create new	A	ccess	Control:	
Site Information Remote Connect Services Servers Failover Servers Cameras Microphones Speakers Wetadata	'n	Kerresn	Enable	Name	Connection Status	Connection Information

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

	Create Access Control System Integration	x
Create access Name the access cor	control system integration trol system integration, select the integration plug-in and enter the connection details.	
Name:	Lenel 7.3	
Integration plug-in:	-	
	Lenel OnGuard-OnGuardAcmServer	
	Next Cancel	

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

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



Properties

General settings			
Enable:	\checkmark		
Name:	Lenel		
Description:			
		_	
Integration plug-in:	Lenel OnGuard-OnGuardAcmServer (Version: 3.0.18235.2, 3.0.18235.02)	_	
Last configuration refresh:	8/2//2018 10:49 AM		
	Refresh Configuration		
Operator login required:			
Connection Profile:	USLT-BHA-01.milestone.dk	\sim	
Database - Host:	BHA-LENEL-03		
Database - Instance:			
Database - Name:	AccessControl		
Database - User:	\$8		
Database - Password:	•••••		
Database - Integrated Security:			
Access Type:	OpenAccess v		
OpenAccess - Host:	BHA-LENEL-03		
OpenAccess - Port:	8080		
OpenAccess - Directory:	custdev.us		
OpenAccess - User:	bha		
OpenAccess - Password:	•••••		
OpenAccess - Page Size:	100		
Options - Event Batch Size:	50	~	
Options - Event Sleep:	5000		
Options - Cardholder Sleep:	60		
Options - Reader Sleep:	60		
Options - Property Sleep:	60		
Options - Event Propogation:	✓		
Options - State Events:	\checkmark		
Options - Disable Commands:			
Options - Database Timeout:	30	,	

Below, the properties are listed by access type.

All Access Types

Connection Profile

Database - Host

Database - Instance



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

Property Details

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



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					
192.108.100.134 Connected Lenel OnGuard-OnGuardAcmServer					
The connection profile name					
Add					
< Back Next > Finish					

Database - Host - Name of the computer hosting the OnGuard SQL Server instance

Database - Instance – Name of the SQL Server instance hosting the OnGuard Access Control database. Leave blank to connect to the default SQL Server instance.

Database - Name - Name of the OnGuard Access Control database.

Database - User – User name to login to the OnGuard Access Control database.

Database - Password – Password to login to the OnGuard Access Control database.

Database – Integrated Security – Flag indicating if the OnGuard Access Control database uses integrated security. If false, the database user name and password is required.

Access Type - Defines the interface method used to access the OnGuard system.

Options – Cardholder Sleep – Defines how long the OnGuard plugin will sleep (in minutes) between fetching card holders from OnGuard. Legitimate values are greater than zero. This is here as a safety to ensure that card holders are kept up-to-date even if card holder modification events from OnGuard are not received or missed.

Options – Reader Sleep – Defines how long the OnGuard plugin will sleep (in minutes) between fetching door and reader information from OnGuard. Legitimate values are greater than zero. OnGuard doesn't provide notification of certain reader attribute changes (e.g. extended strike time) so this polling provides a way to force the system to refresh reader information.

Options – Property Sleep – As hardware events are received from OnGuard, this property defines the time to wait before updating a device's live properties (e.g. reader mode, device hardware status) (in seconds) again. Legitimate values are greater than or equal to zero. This property allows tradeoffs to improve OnGuard event processing speed. For every hardware event received from OnGuard, the OnGuard ACM integration generates related state change events. These state change events are very slow to process compared to the raw hardware events; this delay is caused by having to update the devices' live properties. The smaller you set LivePropertyUpdateInterval, the more "real time" will be those live property values; however, the cost is



more cpu usage and slower state change processing. The higher you set LivePropertyUpdateInterval, state change processing will be faster due to using the currently cached values of the live properties; the cost is that state change events may be sent to MIP that contain "stale" live property values.

Options – Event Propogation – If checked, then applicable events will be propagated to child hardware. For example, a panel offline event would end up triggering offline events for all the panel's child hardware (e.g. readers, alarm panels, inputs, outputs, etc). If not checked, event propagation is not done.

Note that certain functionality is dependent on event propagation. For example, if event propagation is disabled, a Smart Client reader map icon may not display the correct state when its panel is toggled between online and offline because we rely on receiving reader online/offline events to keep that up-to-date.

Options – State Events – If unchecked, then state change processing (including propagated state changes) is disabled. If checked, state change processing is performed and the DoEventPropagation setting is respected. This property can be disabled to maximize raw OnGuard event processing speed. Note that unchecking this property will prevent XProtect Smart Client map icons from showing the current device state.

Options – Disable Commands – This is a setting to enhance security. If checked (the default), then no commands will be executed. The commands will still be visible in XProtect Smart Client maps and in the Dev tabs of the XProtect Management Client; however, they will be silently ignored if a user attempts to execute them. If unchecked, commands will execute as normal.

Options – Event Batch Size – Defines the maximum number of events to process per batch. This is an approximate number; the actual number could be less than or slightly more than this number due to several factors – less events available, more events with the same filter criteria, etc.

Options – Event Sleep - Defines how long the event processor subsystem will sleep (in milliseconds) between batches of events. Legitimate values are greater than zero. The subsystem does not sleep when it finishes a batch of events if there is another batch of events ready to process.

Options – Database Timeout – Events are fetched from OnGuard using a direct SQL query. Internally, there is a timeout for how long to wait to get the results of the query. This default timeout is 30 seconds. When querying for events from an OnGuard table containing many (i.e. millions) of rows, the query can easily take longer than 30 seconds. In that case, the query will fail, events won't get processed, and errors will be written to the debug log. To prevent failures in this situation, increase the event command timeout (e.g. 240 seconds). Legitimate values are greater than or equal to 30 seconds. Changing this property value has NO impact on the actual time it takes to perform the query; it only is an attempt to prevent premature timeouts. It is *always* better to keep the number of rows in the OnGuard EVENTS table to a reasonable amount. OnGuard provides the capability to archive events; contact OnGuard Support for help setting that up. OpenAccess - Host – Name of the machine hosting the OnGuard OpenAccess service.

OpenAccess - Port - The port the OnGuard OpenAccess service is listening on.

OpenAccess – Page Size – The OnGuard OpenAccess service limits the number of instances returned for a given query. For example, multiple queries are required if the number of OnGuard card holders is greater than the page size. Legitimate values are greater than or equal to 20 and less than or equal to 100. Performance is better with a larger page size.

OpenAccess - User – The name of an OnGuard administrative user to use to log into the OnGuard OpenAccess web service. This user should have access to all hardware, cardholders, etc in the system. OpenAccess - Password – The password of an OnGuard user to use to log into the OnGuard OpenAccess web service.

OpenAccess - Directory – The name of the OnGuard directory to be used when loging into the OnGuard OpenAccess web service. If left blank, the OnGuard internal directory will be used.

milestone

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



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

ccess control events related to one of th	he door's access points are	triggered.		access control events related to one of the door's access points are triggered.	
oors:			Cameras:	Doors: Camera	as:
Vame	- Enabled Licens	ie 😘	E VM-MILESTONE	Name 🔺 Enabled License 🤏 🗊	VM-MILESTONE
orte Interieure Door #1	Pendir	ng IT	🖻 🚞 Default	Porte Interieure Door #1 🔽 Pending 🗖	Default
Access point: Porte Interieure Door Drop camera here to associate it with	r Reader th the access point.		192.168.1.54 - Camera	Access point: Porte Interieure Door Reader 192.168.1.52 - Camera 1	192.168.1.54 - Came
orte Principale Door #1	Pendir	ng 🕅		Porte Principale Door #1 🔽 Pending	

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.



 Image: A set of the set of the	Milestone XProtec	t Management Client 2016 R2		_ □	x
File Edit View Action Tools Help					
🗟 🦻 🕝 🗢 🏛					
Site Navigation 🗸 🕂 🗙	Access Control 🗸 🗸	Access Control Information			
Matrix Matrix Matrix Mules and Events Mules Mules Wine Profiles	E-Ontrol Lenel	Access Control:	Connection		
		Enable Name Status	Information		
Vser-defined Events		Lenel Connected			
Ceneric Events					
Security					
- 👫 Roles					
🔒 Basic Users					
System Dashboard					
System Monitor					
System Monitor Thresholds					
- 2 Evidence Lock					
Configuration Reports					
Server Logs					
System Log					
Audit Log =					
Access Control					
Transact					
Transaction sources					
Transaction definitions					
E 🛃 Alarms					
< III >					
Site Navigation Federated Site Hierarchy				 	

Reducing Permissions

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

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

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

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



Personalized Login

Personalized login is an optional feature of XProtect access control plugins. If enabled, when someone logs into the Smart Client, for *each* access control instance with personalized login enabled in the Management Client, the smart client will ask for user credentials. These credentials will be validated against the specific access control system, and, if valid, will be used to fetch a personalized configuration from the access control system. The personalized configurations will be used throughout that instance of the Smart Client. When personalized login is being used, XProtect manages two configurations – a "global" one used by the Management Client, and, as described above, personalized configurations used by the Smart Client. The personalized configurations are always subsets of the global configuration. This is necessary to ensure proper event handling, command execution, etc.

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

Enable/Disable Personalized Login

Enabling/disabling personalized login for a specific access control plugin is done in the Management Client. The first step is to configure your access control instances as described in <u>Milestone Management Client</u> <u>Configuration</u>.

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

Access Control 🚽 👎	Access Control Information	
Access Control	General settings	
	Enable:	\checkmark
	Name:	log
	Description:	
	Integration plug-in:	OnGuard-OnGuardAcmServer (Version: 1.0.19231.2, 1.0.19231.02)
	Last configuration refresh:	8/20/2019 12:22 PM
		Refresh Configuration
	On any tax login any size di	
	Operator login required.	
	Connection Profile:	BHA-APROTECT-A.custdev.us
	Database - Host:	192.168.109.31
	Database - Instance:	
	Database - Name:	AccessControl
	Database - User:	88
	Database - Password:	
	Database - Integrated Security:	
	Access Type:	OpenAccess v
	OpenAccess - Host:	192.168.109.31
	OpenAccess - Port:	8080
	OpenAccess - Directory:	custdev.us
	OpenAccess - User:	xtian
	OpenAccess - Password:	••••••
	OpenAccess - Page Size:	100
	Options - Event Batch Size:	50
I I I		



Smart Client Personalized Login

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

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

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

	×
Milestone XProtect® SMART CLIENT 2017 R3	
Log into access control	
Lenel ACM	
User name:	
sa 🔻	
Password:	
Remember password	
Auto-login	
Connect Skip	
	11.3.5240.1

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



Milestone XProtect® SMART CLIENT 2017 R3	×
Log into access control Lenel ACM User name: bogus Password: Password: Auto-login	
Connect Skip Suser validation failed. Invalid user credentials.	11.3.5240.1

If you click Skip, the Smart Client is opened without using personalized login.

If the credentials are successfully validated, the Smart Client will load a personalized configuration from that access control instance. This personalized configuration is used by the Smart Client to filter entities viewed/operated on in the Smart Client. For example:

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

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

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

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



will only be visible if the underlying device is in their personalized configuration, then users can only acknowledge alarms related to hardware they can see.

OnGuard does not support personalized command execution. That is, a user can execute any applicable commands on any devices that are visible to that user.

Refreshing the Personalized Configurations

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

Access Control 🚽 👎	Access Control Information	
Access Control	General settings	
	Enable:	\checkmark
	Name:	log
	Description:	
	Integration plug-in:	OnGuard-OnGuardAcmServer (Version: 1.0.19231.2, 1.0.19231.02)
	Last configuration refresh:	0/20/2010 12:22 PM
		Refresh Configuration
	Operator login required:	
	Connection Profile:	BHA-XPROTECT-A.custdev.us
	Database - Host:	192.168.109.31
	Database - Instance:	
	Database - Name:	AccessControl
	Database - User:	sa
	Database - Password:	•••••
	Database - Integrated Security:	
	Access Type:	OpenAccess v
	OpenAccess - Host:	192.168.109.31
	OpenAccess - Port:	8080
	OpenAccess - Directory:	custdev.us
	OpenAccess - User:	xtian
	OpenAccess - Password:	•••••
	OpenAccess - Page Size:	100
	Options - Event Batch Size:	50
I	• • • • •·	

The personalized configuration cache is cleared upon Event Server restart.

If there is a running Smart Client using a personalized configuration, after the configuration is updated, you may see the following message in the Smart Client. Simply log back in to get the updated personalized configuration:

🔶 Milestor	ne XProtect Smart	Client			4/1	12/2018 9:15:15 AM 🗕 🗖 🗙
Live	Playback	Sequence Explorer	Alarm Manager	Access Control	System Monitor	₽ + 0 ☆ ₽ १
					Acce	ess control administration
9:14:23 AM	The access cor	ntrol system 'Lenel ACM' has been	disabled. Log into XProtect Sm	art Client again to enable the a	access control system.	4 V
L	_					
Events	Doors Cardh	nolders				
Search d	loors	Q				
Door 🔻	All states 🔻 Al	Il doors 🔻				

milestone

Common Actions

Editing OnGuard Event Types

The OnGuard event types are originally read from the OnGuard database Event table. After initially reading from the database, the event types are stored in a comma-delimited disk file located at

C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\Eve ntTypes.csv on the OnGuard machine.

The columns are: Id, Type, SubType, Description, Name, HardwareType, AllowDoorAnimation The rows are sorted by Type, then SubType.

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

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

An example from the file is shown below:

1,0,0,Access Granted,granted_access_granted,0x000000FF,True

2,0,1,Access Granted on Facility Code,granted_facilitycode,0x000000FF,True

3,0,2,Access Granted No Entry Made,granted_noentrymade,0x000000FF,False

4,0,3,Access Granted on Facility Code| No Entry Made,granted_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 OnGuard.

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

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

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



Searching for cardholders

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

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



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

Cardholder Properties:

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



milestone

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

The OnGuard ACM plugin manages a configuration file

3

C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\OnGuardAcmServer\Cre dHolderProps.dat. This configuration file is created the first-time credential holders are fetched. By default, it includes *all* cardholder fields.

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

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



CredHolderProps.dat - Notepad –		×
File Edit Format View Help		
// This file lists the card holder properties to be displayed in XProtect. // The properties will be displayed in the order listed in this file. // Each property may be optionally followed by a comma and the label to display within XProtect	t.	~
FIRSTNAME,First Name LASTNAME,Last Name LASTCHANGED,Last Modified SSNO,Identification Number ALLOWEDVISITORS,Allowed Visitors		
// Possible properties include the following:		
//ADDR1 //ALLOWEDVISITORS //BDATE //BUILDING //CITY //DEPT //DEPT //DEPT //EXT //FIRSTNAME //FIRSTNAME //FLOOR //LASTCHANGED //LASTCHANGED //LASTCHANGED //LASTNAME //LOCATION //MIDNAME //OPHONE //PHONE //PHONE //SNO //STATE //TITLE //TITLE		
ζ		>

Defining alarms based on OnGuard events

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





♦	Milestone XProtect Management Client 2017 R3	– – X
File Edit View Action Tools Help		
	Access Castel Information	
Site Navigation • Access Control	Access Control mature	• *
Access Cont	Access control events	
License Information		
Site Information	Select the events you want to monitor in XProtect Smart Client. Use categories to simplify the use of triggering events.	
Remote Connect Services	Enabled Access Control Event Source Type Event Category	
Axis One-click Camera Connection	OnGuard 24 Hour Alarm ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	▼ ^
E Servers	OnGuard 24 Hour Alarm Restore ACServer, AlarmPanel, Door, Input, Output. Alarm, OnGuard Trouble	•
Recording Servers	OnGuard 24 Hour Auto Test ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	•
Failover Servers	OnGuard 24 Hour Non-Burglary Alarm ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	•
Mobile Servers	OnGuard 24 Hour Non-Burglary Alarm Res ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	-
E 10 Devices	OnGuard 24 Hour Report Closed ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	-
Cameras	OnGuard 24 Hour Report Open ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	•
P Microphones	OnGuard 24 Hour Zone Bypassed ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	-
Metadata =	OnGuard 24 Hour Zone Unbypassed ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	•
	OnGuard 30 Minutes Since Fallback Com ACServer, AlarmPanel, Door, Input, Output OnGuard System	•
Q Output	OnGuard 32 Hour Event Log Marker ACServer, AlarmPanel, Door, Input, Output Alarm, OnGuard Trouble	•
E E Client	OnGuard Abort ACServer, AlarmPanel, Door, Input, Output OnGuard System	-
Smart Wall	OnGuard AC Battery Fail ACServer, AlarmPanel, Door, Input, Output OnGuard System	•
- 🗁 View Groups	OnGuard AC Restore ACServer, AlarmPanel, Door, Input, Output OnGuard System	-
- 🐙 Smart Client Profiles	OnGuard AC Trouble ACServer, AlarmPanel, Door, Input, Output OnGuard System	•
Management Client Profiles	OnGuard Accepted Biometric Score ACServer, AlarmPanel, Door, Input, Output OnGuard Biometric	•
Matrix	OnGuard Access Closed ACServer, AlarmPanel, Door, Input, Output OnGuard System	•
Rules and Events	OnGuard Access Code Used ACServer, AlarmPanel, Door, Input, Output OnGuard System	-
- E Rules	OnGuard Access Denied ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
Ime Profiles	OnGuard Access Denied (access_denied ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
Notification Profiles	OnGuard Access Denied : AAM Timeout ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
Analytice Events	OnGuard Access Denied : AAM Validation ACServer, AlarmPanel, Door, Input, Output Access denied, Access request,	OnGua 🔻
Generic Events	OnGuard Access Denied Door Secured ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
⊟ construction and a second s	OnGuard Access Denied Interlock ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
Roles	OnGuard Access Denied Passback ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
Basic Users	OnGuard Access Denied to Destination Flo ACServer, AlarmPanel, Door, Input, Output Access denied, Access request.	OnGua 🔻
🗉 🕥 System Dashboard	OnGuard Access Denied Unauthorized Ar ACServer, AlarmPanel, Door, Input, Output Access denied, Access request,	OnGua 🔻
Current Tasks	OnGuard Access Denied Unauthorized Ent ACServer, AlarmPanel, Door, Input, Output Access denied, Access request,	OnGua 🔻
System Monitor	OnGuard Access Denied Unauthorized Ti ACServer, AlarmPanel, Door, Input, Output Access denied, Access request,	OnGua 🔻 🗸
System Monitor Thresholds		
< III >		
Site Navigation Federated Site Hierarchy	👸 General Settings 🔊 Doors and Associated Cameras 🎅 Access Control Events 🤴 Access Request Notifications 🗼 Cardhold	s ivate Wir
		a to System in

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



Associate the category with one of the OnGuard AC events:



cess Cor	ntrol Information		
Acces	as control events		
Select the	a events you want to monitor in XProtect Smart I	Client Lise categories to simplify the use of trig	gering events
		client. Use categories to simplify the use of thig	
Enabled	Access Control Event	Source Type	Event Category
<u> </u>	OnGuard 24 Hour Alarm	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
 	OnGuard 24 Hour Alarm Restore	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
 Image: A start of the start of	OnGuard 24 Hour Auto Test	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard 24 Hour Non-Burglary Alarm	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard 24 Hour Non-Burglary Alarm Res	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
>	OnGuard 24 Hour Report Closed	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard 24 Hour Report Open	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard 24 Hour Zone Bypassed	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard 24 Hour Zone Unbypassed	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard 30 Minutes Since Fallback Com	ACServer, AlarmPanel, Door, Input, Output	OnGuard System
~	OnGuard 32 Hour Event Log Marker	ACServer, AlarmPanel, Door, Input, Output	Alarm, OnGuard Trouble
~	OnGuard Abort	ACServer, AlarmPanel, Door, Input, Output	OnGuard System
~	OnGuard AC Battery Fail	ACServer, AlarmPanel, Door, Input, Output	OnGuard System
~	OnGuard AC Restore	ACServer, AlarmPanel, Door, Input, Output	OnGuard System
~	OnGuard AC Trouble	ACServer, AlarmPanel, Door, Input, Output	OnGuard System
	OnGuard Accepted Biometric Score	ACServer, AlarmPanel, Door, Input, Output,	OnGuard Biometric
	OnGuard Access Closed	ACServer AlarmPanel Door Input Output	My Custom Event Category, OnGuard S
	OnGuard Access Code Used	ACServer AlarmPanel Door Input Output	
	OnGuard Access Denied	ACServer AlarmPanel Door Input Output	All categories
	OnGuard Access Denied (access denied	ACServer AlarmPanel Door Input Output	Access denied
	OnGuard Access Denied (access_denied	ACServer AlarmPanel Door Input Output	
	OnGuard Access Denied : AAM Validation	ACServer AlarmPanel Door Input Output	
	OnGuard Access Denied Door Secured	ACServer AlarmPanel Door Input Output	Access request
<u> </u>	OnGuard Access Denied Door Secured	ACServer, AlarmPanel, Deer, Input, Output.	
•	OnGuard Access Denied Interlock	ACServer, AlarmPanel, Door, Input, Output	
▼	Or Guard Access Denied to Destination Fla	ACServer, Alarm anel, Door, Input, Output	
	Origuard Access Denied to Destination Plo	ACServer, AlarmPanel, Door, Input, Output	My Custom Event Category
	Unguard Access Denied Unauthorized Ar	ACServer, AlarmPanel, Door, Input, Output	
	Unguard Access Denied Unauthorized Ent	ACServer, AlarmPanel, Door, Input, Output	OnGuard Access Denied
~	UnGuard Access Denied Unauthorized Ti	ACServer, AlarmPanel, Door, Input, Output	OnGuard Access Granted
User-d	efined Categories		OnGuard Area APB
诸 Gener	al Settings 🤝 Doors and Associated Cameras	Recess Control Events 1 Access Re	
-		The recease control Events	OnGuard Asset Activa

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



File Edit View Action Tools Help					
Site Navigation	4 × Alarm Definitions		Alarm Definition Information		ą
VM-MILESTONE Basics	Alarm Defi	Add New	Ctrl+N s:	Г	
Gervers Servers Devices	2	Refresh	F5	[
E I Client E Alles and Events			Instructions:		×
🗄 😳 Security 🗄 🕥 System Dashboard			Trigger		
E Gerver Logs			Triggering event:		¥
E Alarms					¥.
			Sources:		Ŧ
- 5 Sound Settings			Activation period		
			C Time profile		¥
			C Event based:	Start	Select
				Stop:	Select.
			Operator action required		
			Time limit:	1 minute	<u>*</u>
			Events triggered:		Select
			Other		
			Related cameras:		Select.

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

filestone XProtect Management Client 2014		
Edit View Action Tools Help		
Navisation A X Alam Definitions	a Alam Detrotion Internation	
VM-MILESTONE	tions Alam definition	
🗄 🛄 Basics 🔤 🖓 🔝 🔤	Enable	2
B B Remote Connect Services	Marrie	Mr. C. Proc. Contem Mann
B 20 Devices	Prane.	program association and an
B 🖳 Clert	Instructions:	<u>^</u>
B Rules and Events		<u>×</u>
B System Dashboard	Tripger	
🖲 🔚 Server Logs	Triggering event:	
P Access Control		Access Control Event Categories
- Alatan Definitions	200000	Device Events
Alarm Data Settings	Sources:	Haidware Events
- 19 Sound Settings	Activation period	Hecolding Server Events System Events
	Time profile	Always
	C Event based	Stat: Select.
		Stop: Seirct.
	Drevator action required	
	Time Init:	1 minute *
	Events trimmed	
	Evens of Meren	3000.
	Other	
	Fielated cameras:	Select .
	Fielated map:	
	Initial alarm owner:	<u> </u>
	Initial alarm priority:	High
	Initial alarm category	
	Events himmed he alarm	Select

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





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

Prinestone Aprocect Management C	ment 2014		
He Edit View Action Tools Help			
te Navigation	# × Alam Definitions	Alam Definition Information	
W MILESTONE	🛛 👷 Alam Definitions	Alarm definition	
B C Basics	- 🧏 Alarm Definition	Enable	A
Remote Connect Services		Name:	My SiPass Custon Alam
Devices		Instructions	
B Clerk		modeline	
B G Security			1
🖲 🕥 System Dashboard		Trigger	
B Server Logs		Triggering event:	Access Control Event Categories
B 🛃 Alams			My Siemens Custom Defined Category
ASam Definitions		Sources:	
Sound Settings		Activation period	Al dore Pote Intereste Dore #1
		G. Time coolie	Porte Principale Door #1
		C Sandhard	
		 Event based. 	Stat Deel.
			Stop. Select.
		Operator action required	
		Time limit	1 minute
		Events triggered	Select.
		Other	
		Related cameras:	Select
		Related map:	
		Initial alarm owner:	-
		Initial alarm priority:	Hish
		Initial alarm category	
		Events timesed by show	
		s reasoning feed by alamit	Senot.
Re Havgauth Foderaled Site Hitrachy		1 1 www.core.alam	



Alarms acknowledged in Milestone are acknowledged in OnGuard.



Defining rules based on OnGuard events

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



Select the event hyperlink:

Vame:)escription:	DoActionUnSite	'assEvent		
escription:				
ather	1			
CUVD.	N			
		Ste	p 1: Type of rule	
Select the rule ty	pe you want to create	e.		
Perform an a	ction on <event></event>			
C Perform an a	ction in a time interval	<u>U</u>		
D the side day	whether failed are used	And Annual Contracts		
Edit the rule des	cription leack an unde	snined itemj		
from device	not event	Imanagemen	nt server	
HOIN MEYICE	server and server	Zindridutenies	a server	

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.



- IDI XI

	DoActionOnSiPassEvent		
scription:	1		
tive:	5		
	St	ep 1: Type of rule	
elect the rule I	ype you want to create		
Perform an	action on Kevenb		
Perform an	action in a time interval		
dit the rule de	scription (click an underlined item)		
dit the rule de erform an acti	scription (click: an underlined item)		
dit the rule de erform on acti fron devic	scription (click an underlined item) as as event es/recording server/manageme	ant server	
dit the rule de leform on acti fron devic	scription (click. an underlined item) on on exemp es/recording.server/manageme	ont server	
dit the rule de renform an acti fron dervic	scription (click, an underlined item) an cin exampt es/seconding_serves/managemi	ant server	
dit the rule de ferform as acti fron <mark>dervic</mark>	scription (click an underlined item) an on exeant estimoording server/manageme	ant source	
dit the rule de ferform on activ fron devic	scripton (click: an underlined item) an on a weet as /recording: server/manageme	ant server	
dit the rule de ferform on acti fron <mark>dervice</mark>	scription (click. an undefined item) on conservent es /necording.server/manageme	ant sorver	
dit the rule de ferform an activity fron device	scripton (click an undefined item) or on avant as / necording_server/manageme	2NL BOLVOY	



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

lame:	DoActionOnSiPas	ssEvent	
escription:			
ictive:	N		
		Step 1: Type of rule	
Edit the rule de	scription (click an underli	ined item)	
Edit the rule de Perform an acti from <u>System</u>	scription (click an underli on on <u>Access denied (Acc</u> is (+ units)	ined ikem) cess Control Categories)	

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.

tamo.	D oActionOnSiPassEvent	
escription:		
ctive:	N	
	Step 2: Conditions	
Select condition	ns to apply	
Within sele	cted time in <time profile=""></time>	
Dutside sel	ected time in <time profile=""></time>	
Day of wee	k is (dau)	
Event is fro	m <motion window=""></motion>	
10		
Edit the rule de	sciplion (slick an undefined Rem)	
Edit the rule de from Suster	scopton (dck an underlined item) on on Access Gened Access Control Categories)	_
Edit the rule de Perform an acti from <u>Syster</u>	scription (click an underfined item) on on Access denied (Access Control Categories) is Le units)	_
Edit the rule de Perform an act from <u>Syster</u>	escliption (click an underlined item) on on Access Genied (Access Control Calegories) si I- units)	_
Edit the rule de Perform an acti from <u>Syster</u>	scopion (clok an undefined Rem) on on access demind faccess Control Categories) is L-unita)	_
Edit the rule de Perform an acti from <u>Syster</u>	scolption (click an underfined item) on on <u>Access Gened (Access Control Categories)</u> si L wint)	_
Edit the rule de Perform an act from <u>Syster</u>	scopion (slok an undefined Beni) on on Access Genied Recess Control Categories) al Cuenza)	
Edit the rule de Perform an acti from <u>Syster</u>	scoption (click an undefined item) on on <u>access denied (access Control Categories)</u> is 1 - write)	
Edit the rule de Perform an acti from <u>Syster</u>	scopton (dick. en underlined item) on on <u>Access Gened</u> (Access Control Caleozoies) ei L- Junzi)	

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



łame:	DoActionOnSiPassEve	nt		
escription:				
ctive:	R			
		Chan D. Antinan		
Calact actions to	parform	Step 3: Actions		
Stat coord	penom			
Start feed or	(devices)			
Set (Smart)	(all) to coreceth			
Set (Smart)	Vally cooperation to show coa	maran \		
C Cat live from	valis chiormons to show cou	100000		
Cat we man	frame rate an colorinary			
C Set recording	frame rate to all former for	1 DEA MIDE C A an Administra		
C Start patrolla	a on (device) using (profile	with PTZ (minitus)		
E Pause patrol	ing on (device) using (prome	2 WHITE TA Sprinky?		
E Mause paulo	ing on coevices?	DTZ (miniho		
Move (devi	set to chresels position with	DTZ (pilony)		
Cat device	aut preset on cuevices? with	F12 (priority)		
Set device t	uipui io (siale)			
Cleate DODK	naik un cuevices?			
E Maha nounca	nuerto «prome»			
Charle new C	og entrys			
Chan plug-in	un (devices)			
Stop plug-in	un (devices)			
Cat Matrix Is	sungs on (devices)			
Card Child	view (devices)			
Dehister of	uap Labora annala annaidheac fear			
Debieve and	store remote recordings nor	i (devices).	in a star from the	
Course work	store remote recordings be	ween statt and end times r	IOM (Devices).	
Save attach	sd images			
Activate arci	iving on (archives)			
Un cares en	adel (user-defined event)			
Door Grant A	ccess (DeerSet)			
Door Lock C	Joorsep			
Door UnLoc	DesiGeb	Access Control	Commands	
Door Disable	DesiGette			
Door Enable	(Doorset)			
Show <acce< td=""><td>ss request notrication></td><td></td><td></td><td></td></acce<>	ss request notrication>			
C.D.H	which are to find a second of the of the	tend .		
Edit the fulle des	cription (click an underlined i	iem)		
Perform an actic	n on Access denied (Access	Control Categories]		
Create bookman	Bookmark on devices			
	NS 52		a	
	0.1		1.100000	1000

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 underlined item)	Bookmark Details
Perform an action on Access denied (Access Control Categories) from Surtem le units) Deste bookmark Bookmark on devices	Headine McClassReadwork
	myoir asso bukinan.
	Description
Help Lancel (Back Next)	This is an access denied event
	Pre-bookmark time (seconds)
	1 oscood mark une (seconda)
	Add system information (click links to insert variables in bookmark iteel) <u>Device name Event name Isopering line Bule name Recording server name </u>
	OK Cancel

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

E dit her uke description (olick) an underland ken) Perform an okon o <u>ccess devel devices Control Categores</u>) from <u>Statemen</u> , undel Deate bookmark <u>Beekmark</u> on <u>devices</u>	Select Triggering Devices X C Use devices from metadata C Select devices
Hep Cancel (Back Next) Finish	Cancel

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



lame:	DoActio	onOnSiPassEvent			
escription:					
Active:	V				
		-	Step 4: Stop criteria		
Select stop crite	eria				
C Perform stop	o action on Kev	ent>			8
C Perform stop	action after <t< p=""></t<>	ime>			
No actions	performed on ru	le end			
-					
-					
Edit the rule de	scription (click -	an underlined item)		
Edit the rule de Perform an activ	scription (click on on <u>Access d</u>	an underlined item enied (Access Cor) Itrol Categories)		
Edit the rule de Perform an acti from <u>System</u>	scription (click - on on <u>Access d</u> is (+ units)	an underlined item enied (Access Cor) Itrol Categories)		
Edit the rule de Perform an acti from <u>System</u> Create bookma	scription (click + on on <u>Access d</u> is <u>(+ units)</u> rk <u>MySiPassBoo</u>	an underlined item enied (Access Cor okmark on <u>the dev</u>) Itrol Categories) ices from metadata		
Edit the rule de Perform an acti from <u>System</u> Create bookma	scription (click - on on <u>Access d</u> is (+ units) ik <u>MySiPassBo</u> r	an underlined item enied (Access Cor okmark on <u>the dev</u>) trol Categories) ices from metadata		
Edit the rule de Perform an acti from <u>System</u> Create bookma	scription (click - on on <u>Access d</u> i <u>s (+ units)</u> ik <u>MySiPassBor</u>	an underlined item enied (Access Cor okmark on <u>the dev</u>) Itrol Categories) ices from metadata		
Edit the rule de Perform an acti from <u>System</u> Create bookma	scription (click - on on <u>Access d</u> is <u>1+ units]</u> ik <u>MySiPassBor</u>	an underlined item enied (Access Cor okmark on the dev) trol Categories) ices from metadata		
Edit the rule de Perform an acti from <u>System</u> Create bookma	scription (click , on on <u>Access d</u> s (+ units) rk <u>MySiPassBor</u>	an underlined item enied (Access Cor okmark on the dev) Irrol Categories) ices from metadata		
Edit the rule de Perform an acti from <u>System</u> Create bookma	scription (click , on on <u>Access d</u> is <u>I + units</u> rk <u>MySiPassBoo</u>	an underlined item enied (Access Cor akmark on the dev) Irrol Categories) ices from metadata	1 Days	

Click finish and the rule is set.

XProtect® Smart Client Maps

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



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





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





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



XProtect® Access Monitor tiles

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





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



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



Alarm Acknowledgment

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



Alarm acknowledgment is done in the XProtect Smart Client's Alarm Manager tab. If you right-click an alarm, and select either Acknowledge or Close, the alarm will be acknowledged in OnGuard.

🔶 Mileston	e XProtect Smart Clier	nt								
Live	Playback	Sequence Explorer	Alarm Man	ager 😥	Access Con	trol Sys	tem Monitor			
1 🚯 « > 🔊	No map has been s	selected								
Quick Filters		Alarms No filter 🗸								
T New (2))	🖼 Time 🔺	Priority Level	State Level	State Name	Message	Source	Owner	ID	
T In progr	ress (0)	12:53:31 PM 6/9/2017	1	1	New	OnGuard Acc	2 - Lenel OpenProx		2	
T On hold	I (0)	12:52:52 PM 6/9/2017	1	1	New	Acknowledge	2 - Lenel OpenProx		1	
T Closed	(0)				-	Set on hold	-			
						Close				
Servers						Edit				
a uscusto	MDEV02					Disable new alar	rms			
						Print				

NOTE – As mentioned above, selecting either Acknowledge or Close will cause the alarm to be acknowledged in OnGuard 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 OnGuard. 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.

Fetching OnGuard event types

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



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

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

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

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

Defining cardholder properties to display in Milestone XProtect

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

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

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

FIRSTNAME, First Name

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

The bottom of the file contains the fields detected in the integration at the time of installation, for your convenience.

Once the file has been modified, save and close it. Restart the Milestone ACM Server. Then, restart the Milestone Event Server for the changes to take effect.

Logging

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



periods of time for performance reasons. It should only be used for diagnostics purposes and put back to Info afterwards.

Gathering the logs

Milestone Event Server side

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

OnGuard Server side

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

Changing logging level

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

Milestone Event Server side

- 1. On the machine running the Milestone Event Server go to x:\ProgramData\VideoOS\ACMServer-Plugin, where X: is the drive where Windows is installed
- 2. There should be subfolders that use a unique identifier (GUID) something like "4c53f6e5-e951-1616-83f0-e44fb813e451". For each of these folders do the following:
 - a. Find a file named "ACMServerPluginNLog.xml", open it with a text editor like notepad
 - b. The second to last line in the file is like this "<logger name="*" minlevel="Info" writeTo="mainlog" />"
 - c. Change the "Info" to "Debug" or "Trace" in that line and save the file.
 - d. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.



OnGuard Server side

- 1. On the OnGuard server machine go to x:\ProgramData\VideoOS\ServiceHost. X: would be the drive where windows is installed.
 - a. Find a file named "ServiceHostNLog.xml", open it with a text editor like notepad
 - b. Near the bottom of the file, find the lines starting with "<logger name="*"", "<logger name="lenel.*"", and "<logger name="OnGuard.*"".
 - c. Change the "minlevel" attribute values in those lines from their current values to "Debug" or "Trace" and save the file.
 - d. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.
- 2. On the OnGuard server machine go to x:\ProgramData\VideoOS\ServiceHost\Services\VideoOSAC-MServerService. X: would be the drive where windows is installed.
 - a. Find a file named "VideoOSACMServerNLog.xml", open it with a text editor like notepad
 - b. The second to last line in the file is like this "<logger name="*" minlevel="Info" writeTo="mainlog" />"
 - c. Change the "Info" to "Debug" or "Trace" in that line and save the file.

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

Troubleshooting Guide

OnGuard loses communication with the access control hardware

Communication can be lost for the following reasons:

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

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

The OnGuard ACM plugin runs in the ACM Server service. That service must be running in the security context of a local machine admin user which is linked to a OnGuard Directory that is configured for single sign-on. See <u>Configure OnGuard for Single Sign-On</u> and <u>ACM Server: Configure to RunAs OnGuard Single-Sign-on Account</u> above for details.

If the ACM Server is not running in the required security context, the OnGuard ACM plugin log (see log locations <u>below</u>) will show lines similar to the following:

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



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

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

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

If you don't see these lines, or you expect a communication failure between the Evert Server MIP plugin and OnGuard ACM plugin, take a look at your firewall settings, rules, etc. You may need to adjust them to allow communication.

Note that, by default, the ACM Server's web service uses HTTPS on port 8443. You may have configured your ACM Server differently (see <u>ACM Server: XProtect ACM MIP Plugin</u> 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 <u>Configure SQL Server for Connections</u> for properly configuring the SQL Server supporting your OnGuard installation.

Failure to connect to SQL Server

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



Access Control 🗸 🗸 👎	Access Control Information		• 9
Access Control	General settings		
	Enable:	\checkmark	
	Name:	log	
	Description:		
	Integration plug-in:	OnGuard-OnGuardAcmServer (Version: 1.0.19231.2, 1.0.19231.02)	
	Last configuration refresh:	8/20/2019 12:22 PM	
	_	Refresh Configuration	
	Operator login required:		
	Connection Profile:	BHA-XPROTECT-A.custdev.us	^
	Database - Host:	192.168.109.31	
	Database - Instance:		
	Database - Name:	AccessControl	
	Database - User:	\$8	
	Database - Password		
	Database - Integrated Security:		
	Access Type:	OpenAccess v	
	OpenAccess - Host:	192.168.109.31	
	OpenAccess - Port:	8080	
	OpenAccess - Directory:	custdev.us	
	OpenAccess - User:	xtian	
	OpenAccess - Password:	•••••	
	OpenAccess - Page Size:	100	
	Options - Event Batch Size:	50	
1	. . .		~

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 <u>enabled software events in OnGuard</u>.

Optimizing Event Processing Performance

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

- Debug log level should be set to "Info". The "debug" or "trace" settings write too much data to the event log affecting overall performance.
- Adjust the following ACM instance settings (see Milestone Management Client Configuration):
 - ReaderPollingInterval Set this to a large number (e.g. 60). Frequently reading reader information can have a large impact on overall performance.
 - CardHolderProcessSleepInterval Set this to a large number (e.g. 60). Frequently reading cardholder information can have a large impact on overall performance.
 - EventProcessBatchSize Only applies to OnGuard versions less than 7.4. Tailor this value as needed. The larger the number, the more events processed in one batch. Note that a larger number doesn't



always result in better performance because, depending on the rate of events coming in, more time could be spent waiting for events than processing them.

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

No matter what settings you adjust, all raw events received from OnGuard get sent to XProtect. If DoProcessStateChanges is enabled, for every raw event received from OnGuard, the OnGuard ACM integration will create corresponding "state change" events. If the raw event is for a "parent" device (e.g. panel, door, I/O control module), and if the DoEventPropagation setting is enabled, state change events may also be created for child devices (e.g. reader, inputs, outputs). When added together, state change and propagated state change events add a large number of events to be sent to XProtect. Therefore, if you're only interested in optimizing raw OnGuard event processing, disabling

DoProcessStateChanges will result in better performance as it drastically reduces the number of events sent to XProtect. However, XProtect Smart Client map icons won't display status changes since no state change events get sent to XProtect.

On one of the Milestone test systems, we achieved almost real time firing of OnGuard events to XProtect with all the default settings except:

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

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

Refreshing cardholders

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



The OnGuard ACM integration downloads cardholders from OnGuard at the following times:

- 1) When the ACM Server is started.
- 2) When the CardHolderProcessSleepInterval (see <u>Milestone Management Client Configuration</u>) occurs.
- When XProtect Management Client property values change (see <u>Milestone Management Client Con-</u> <u>figuration</u>) are saved.

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

WMI related errors

If you're getting WMI-related errors in the OnGuard ACM log files, they're typically due to the OnGuard Single Sign-On (SSO) user. The SSO user may not be set up correctly, may be missing some permissions, etc. A workaround to verify that the errors are indeed due to SSO user permissions, is to change the currently configured OnGuard SSO user to the built-in "System Account" user. This built-in user has all possible permissions within OnGuard.

Steps:

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

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

OnGuard OpenAccess connectivity

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

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

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

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

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

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



OnGuard ACM integration flooding user transaction report

Milestone's XProtect system requests the current states of OnGuard hardware at various times throughout the life of the application. As prescribed by the OnGuard integration documentation (for both DataConduit and OpenAccess), to get the current state of a hardware device, the integration must update the hardware status on the parent panel, then query for the device state.

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

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

Customers making use of OnGuard's built-in "User Transaction" report from OnGuard's Sys Admin + Reports will see these *many* transactions from the OnGuard ACM integration under the SSO user in the report. Because there's so many of these transactions, some customers feel that the OnGuard ACM integration makes this report useless. Per OnGuard, it's not possible to filter the User Transaction report to omit the SSO user.

The only options that customers have are:

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

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

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

If XProtect is unable to communicate with the OnGuard ACM instance, the instance will not appear in the Access Control section of the Management Client. Do the following steps in the following order:

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

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

LS OpenAccess service automatically stops seconds after starting

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

workaround is to switch the Single Sign-On user to be a local windows account, and adjust the services to use this same login as mentioned above in <u>Refreshing the Personalized Configurations</u>. For questions and information concerning a fix for this issue, please contact Lenel support for information regarding this bug at <u>oaap@lenel.com</u>. Reference Lenel Bug DE40122.

milestone

I/Os connected to OSDP readers are no longer detected

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) where I/Os connected to OSDP readers are no detected in the Milestone ACM Server integration.

For questions and information concerning a fix for this issue, please contact Lenel support for information regarding this bug at oaap@lenel.com. Reference Lenel Bug DE40122.

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

This is a known issue with OnGuard 7.4 Update 1 (7.4.457.69) running in an Enterprise configuration where devices do not send events through OpenAccess to the Milestone ACM Server integration. For questions and information concerning a fix for this issue, please contact Lenel support for information regarding this bug at opan@lenel.com. Reference Lenel Bug DE40122.

All other support issues

For issues not covered in this guide, please contact Milestone Support at <u>support@milestone.us</u>, or by phone at 503-350-1100.

Known issues

- This ACM integration was only tested against the MIP SDK 2017. The MIP SDK is backwards-compatible; so it is assumed that the ACM integration will work with MIP SDK 2016 and 2014.
- This ACM integration has only been tested when running the OnGuard and Milestone systems on Windows Server 2012 R2 and Windows Server 2016.
- This ACM integration is currently coded to only work with a OnGuard system using SQL Server as its database. Oracle integration has not been implemented yet.
- Only United States English installers are available.
- OnGuard doesn't model doors; they work only with readers. But Milestone ACM requires doors to be modelled. Therefore, the OnGuard plugin creates virtual doors based on reader properties (i.e. panel id, panel address, reader number, etc). Currently, the virtual door names are based on the first reader that has a non-empty display name. So if that reader is named "reader 1", that's what the door will be named. This may not be intuitive when viewed in the XProtect Management or Smart Client applications' hardware hierarchy.
- When creating a new ACM instance on the Access Control tab in the XProtect Management Client, especially when creating the first instance, it may take 1 or 2 clicks of the Next button in the wizard before configuration is successfully fetched from the OnGuard system.
- See the negative side-effects of <u>upgrading</u>.



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.