MAKE THE
WORLD SEE

November 2019

Guide

Milestone XProtect Access

CCure 9000 User Manual

Prepared by:
Custom Development Americas

milestone

Table of Content

Copyright, Trademarks & Disclaimers

Copyright

Trademarks

XProtect® is a registered trademark of Milestone Systems.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

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

Disclaimer

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

Version Compatibility

Matrix

Here is the compatibility matrix between CCure 9000 and Milestone XProtect.

Please verify the version of CCure 9000 you are running against this compatibility table. Milestone always recommends that you run the latest versions of both CCure 9000 and XProtect

CCure 9000	XP 2016 R3	XP 2017 R1-R3	XP 2018 R1	XP 2018 R2	XP 2018 R3
2.70 SP2	S	S	S	T	T

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 2018 R2-R3	These versions are fully supported*

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

CCure 9000 Version details

Version	Minimum update / patch level	Version Information
CCure 9000 2.70	SP2_CU01	These versions are fully supported

Hardware Support

The following CCure 9000 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
USTAR008	iStar Ultra

Scalability

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

Cardholders

The CCure 9000 plugin supports as many cardholders as your version of XProtect supports. See XProtect documentation for the values supported by your installation.

Events Handled

Preliminary tests show a sustained rate of about 40 events per second. For more about supported events, see Milestone-ACM-CCure-9000-Events.pdf

General Description

Introduction

This document describes specifics to the XProtect Access (XPA) integration between Milestone XProtect and the CCure 9000 access control (AC) system. This integration supports the following standard XProtect Access (XPA) features:

- Retrieve configuration from the CCure 9000 AC system, e.g. doors and event types
- Receive AC event streams and state changes from the CCure 9000 system
- Get/Search cardholder information with picture association
- Create alarms in alarm manager based on AC events.
- Alarm state synchronization between XProtect and CCure 9000 when the alarm is acknowledged in XProtect.
- 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 CCure 9000 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 CCure 9000 server (Milestone.ACMServer.x64.msi)
3. The "CCure 9000 ACM Server Plugin" that runs on the CCure 9000 server (Milestone.ACMServer.CCure9k.msi)

Prerequisites

Time Synchronization

All servers (i.e. the CCure 9000 and Milestone machines) must be time-synchronized to within a couple of minutes of one another. See Kerberos V5 time skew recommendations here.

CCure 9000: Victor Web Service Installation

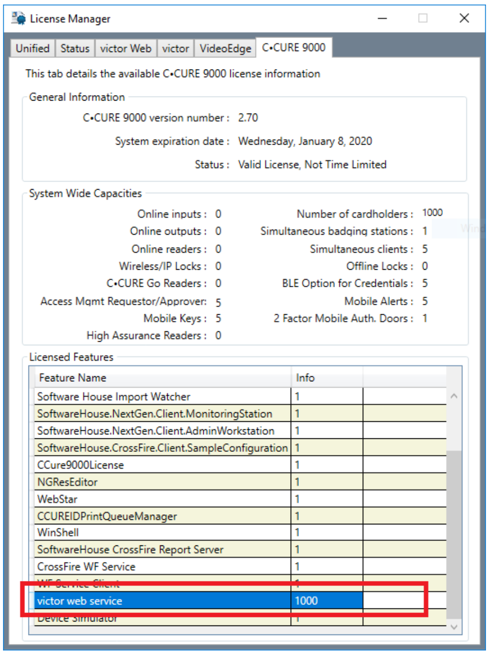
The CCure victor web service must be installed and configured on the CCure 9000 server. Please follow the Victor Web Service User Guide provided by CCure.
The CCure 9000 victor web service installer can be obtained by downloading the "CCURE 9000 v2.XX Web Service Package" through the connectedpartnerprogram.partnerproducts.com web site.

CCure 9000: Victor Web Service SSL Configuration

The SSL configuration must be set up for the CCure 9000 plugin to work (a certificate must be provided and configured in IIS for the CCure 9000 victor web service to accept secure HTTPS connections on port 443).
See page 15 of the Victor Web Service User Guide for details.

CCure 9000: Victor Web Service License

The feature "victor web service" must be licensed in CCure.



This tab details the available C•CURE 9000 license information

General Information

C•CURE 9000 version number : 2.70
System expiration date : Wednesday, January 8, 2020
Status : Valid License, Not Time Limited

System Wide Capacities

Online inputs :	0	Number of cardholders :	1000
Online outputs :	0	Simultaneous badging stations :	1
Online readers :	0	Simultaneous clients :	5
Wireless/IP Locks :	0	Offline Locks :	0
C•CURE Go Readers :	0	BLE Option for Credentials :	5
Access Mgmt Requestor/Approver:	5	Mobile Alerts :	5
Mobile Keys :	5	2 Factor Mobile Auth. Doors :	1
High Assurance Readers :	0		

Licensed Features

Feature Name	Info	
Software House Import Watcher	1	
SoftwareHouse.NextGen.Client.MonitoringStation	1	
SoftwareHouse.NextGen.Client.AdminWorkstation	1	
SoftwareHouse.CrossFire.Client.SampleConfiguration	1	
CCure9000License	1	
NGResEditor	1	
WebStar	1	
CCUREIDPrintQueueManager	1	
WinShell	1	
SoftwareHouse CrossFire Report Server	1	
CrossFire WF Service	1	
WF Service Client	1	
victor web service	1000	
Device Simulator	1	

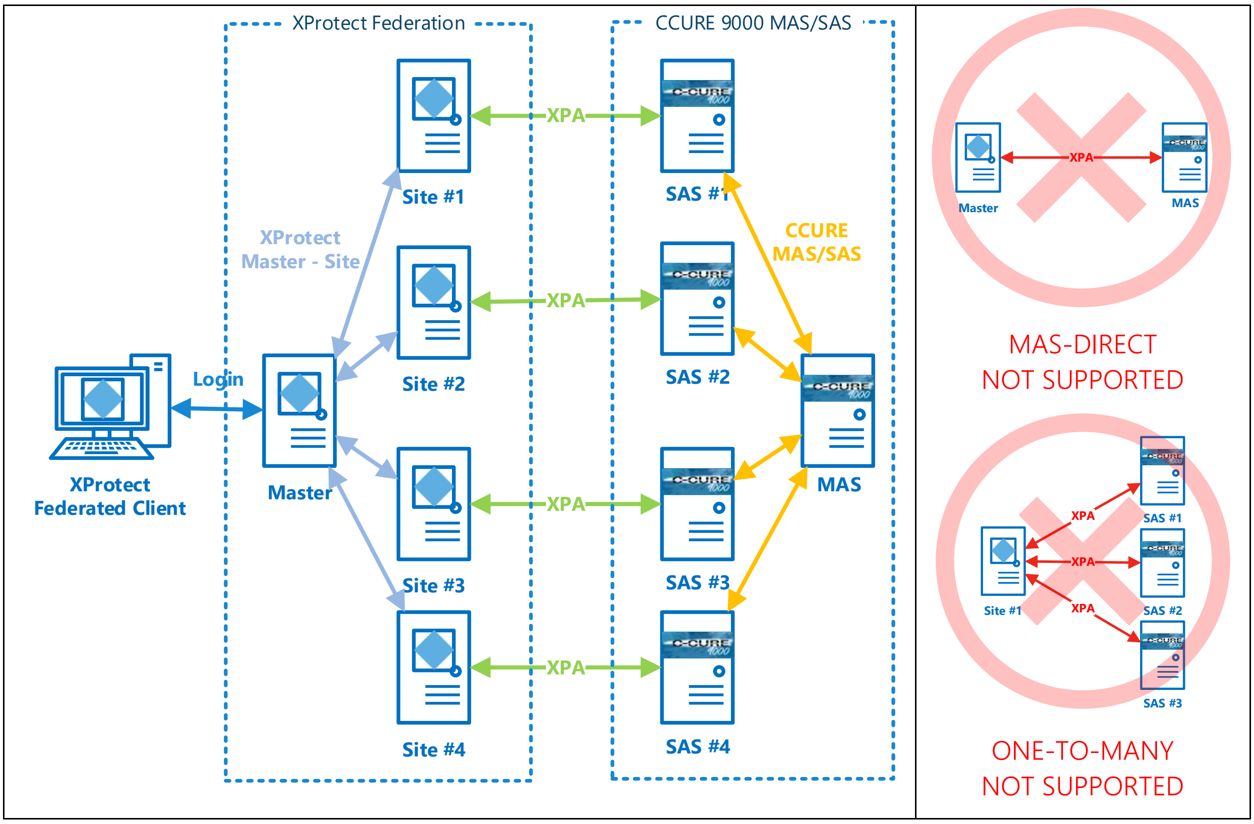
The ACM Server uses a permanent connection to CCure web service (to receive statuses and events) and uses multiple transient connections for specific user operations, such as fetching configuration and executing commands. For optimal operation of Milestone XProtect Access, the feature license activated in CCure must support enough concurrent connections to the Victor Web Service to handle the number of connected ACM Servers' permanent and transient connections.

CCure 9000: Enterprise (MAS/SAS) Configuration

If the CCure 9000 system is part of an Enterprise deployment (MAS/SAS), the Enterprise system must be correctly configured and functioning before setting up the integration. Each CCure 9000 Satellite Application Server (SAS) of an Enterprise deployment must be independently connected through XProtect Access (XPA) to each Milestone XProtect Site of a Federated system.

CCure 9000 Enterprise scenarios require that each CCure 9000 Satellite Application Server (SAS) 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 CCure 9000 Satellite Application Server (SAS) connected.

CCure 9000 Enterprise scenarios also require that *no connection* is directly made to a Master Application Server (MAS).

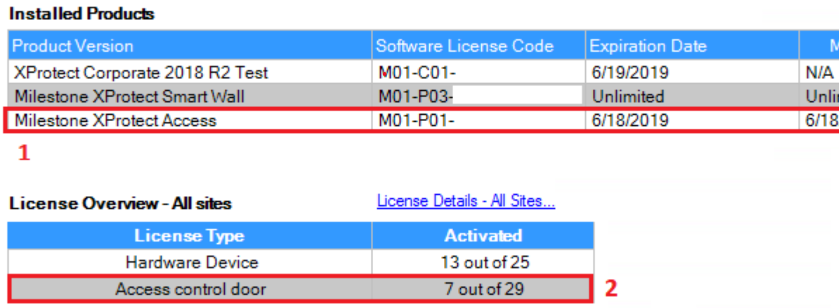


.NET Framework: Installation on CCure 9000 Server machine

.NET Framework 4.5 must be installed on the CCure 9000 server machine (dotnetfx45_full_x86_x64.exe). This is mostly for older OS editions, anything above Windows 8 and Windows 2012 Server will have it already installed as part of the OS. Milestone recommends that you use Microsoft Windows Server Editions of the OS.

Milestone XProtect®: License Options

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



Installed Products

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

1

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

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

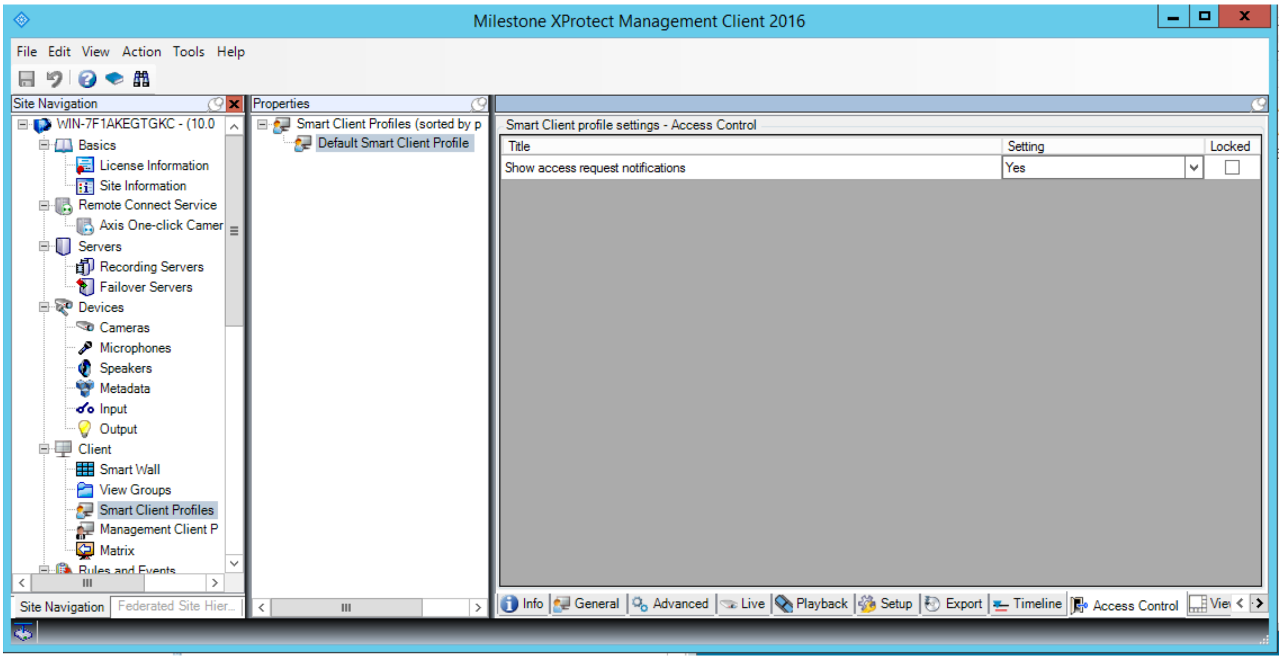
2

Milestone XProtect®: Event Server machine DNS / Name resolution

The machine running the Milestone XProtect Event Server must have network name resolution such that it can resolve the computer name of the CCure 9000 Server machine (e.g. DNS, manual host file entry, etc). The CCure 9000 Server machine must also be able to resolve the Milestone machine.

Milestone XProtect®: Smart Client Profiles

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



Smart Client profile settings - Access Control

Title	Setting	Locked
Show access request notifications	Yes	□

Installation

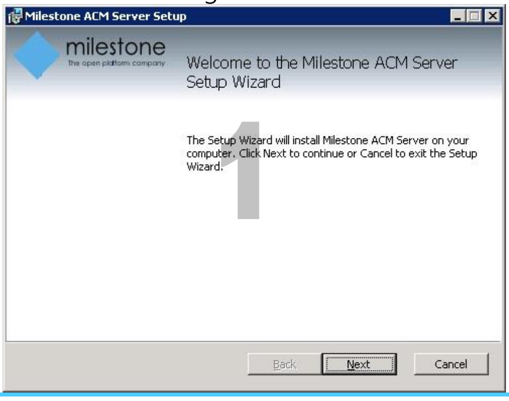
The installation package consists of three independent installers:

1. Milestone.ACMServer.x64.msi: Installer for the ACM Server
   - Installed on the CCure 9000 server machine
2. Milestone.ACMServer.CCure9k.msi: Installer for the Ccure 9000 ACM Server plugin
   - Installed on the CCure 9000 server machine, after the ACMServer.
3. Milestone.ACMServer.MipPlugin.msi: Installer for the XProtect Event Server ACM MIP Plugin
   - Installed on the XProtect Machine that hosts the Event Server Windows service

Please install them in the order specified above, following completion of the prerequisites section. It is mandatory that the *same version* of the CCure 9000 ACM integration be installed on both the XProtect and CCure 9000 machines.

ACM Server Installation

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

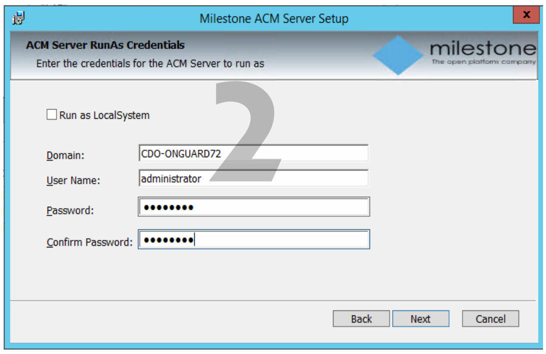


Milestone ACM Server Setup

Welcome to the Milestone ACM Server Setup Wizard

The Setup Wizard will install Milestone ACM Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Enter credentials for the ACM Server:



Milestone ACM Server Setup

ACM Server RunAs Credentials

Enter the credentials for the ACM Server to run as

☐ Run as LocalSystem

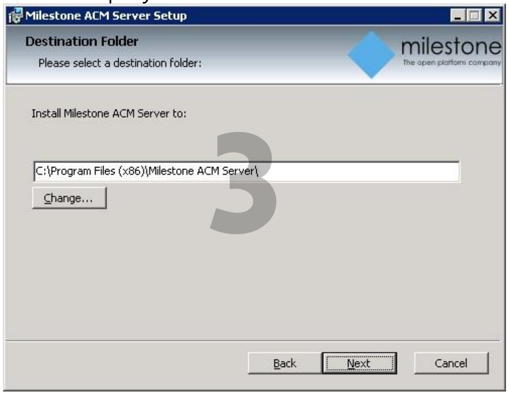
Domain: CDO-ONGUARD72

User Name: administrator

Password: ••••••••

Confirm Password: ••••••••

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



Milestone ACM Server Setup

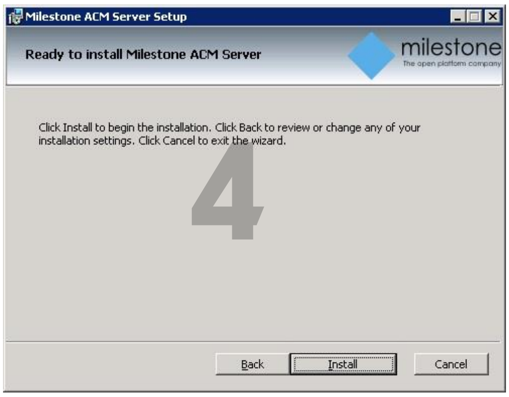
Destination Folder

Please select a destination folder:

Install Milestone ACM Server to:

C:\Program Files (x86)\Milestone ACM Server\

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

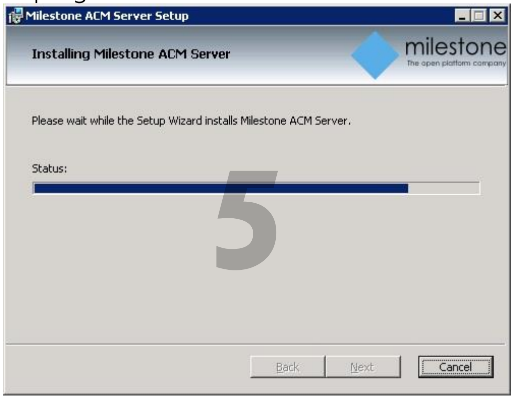


Milestone ACM Server Setup

Ready to install Milestone ACM Server

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Install progress...



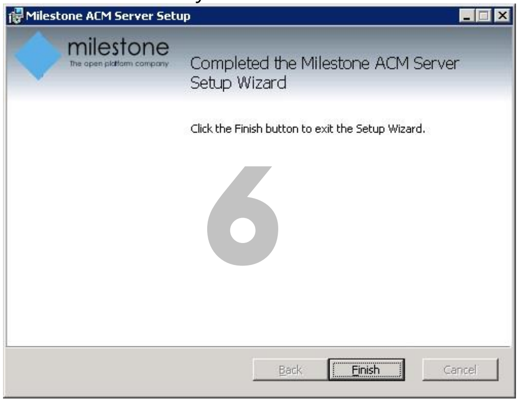
Milestone ACM Server Setup

Installing Milestone ACM Server

Please wait while the Setup Wizard installs Milestone ACM Server.

Status:

You have successfully installed the ACM Server:



Milestone ACM Server Setup

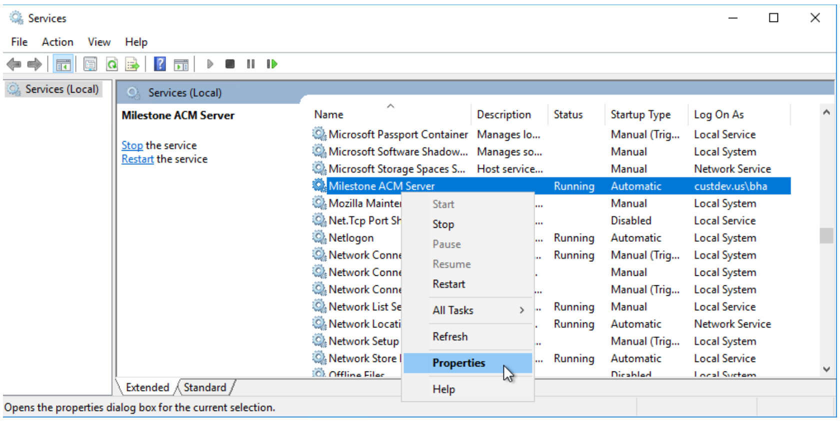
Completed the Milestone ACM Server Setup Wizard

Click the Finish button to exit the Setup Wizard.

ACM Server Credentials

If you need to verify and/or modify the credentials for the ACM Server service, do the following:

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



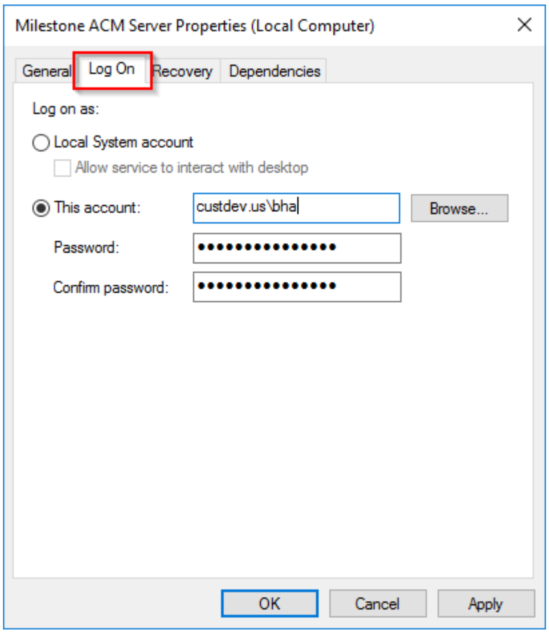
Milestone ACM Server

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Microsoft Passport Container	Manages lo...		Manual (Trig...	Local Service
Microsoft Software Shadow...	Manages so...		Manual	Local System
Microsoft Storage Spaces S...	Host service...		Manual	Network Service
Milestone ACM Server		Running	Automatic	custdev.us\bha
Mozilla Mainte	...		Manual	Local System
Net.Tcp Port Sh	...		Disabled	Local Service
Netlogon	...	Running	Automatic	Local System
Network Conne	...	Running	Manual (Trig...	Local System
Network Conne	.		Manual	Local System
Network Conne	...		Manual (Trig...	Local System
Network List Se	...	Running	Manual	Local Service
Network Locati	.	Running	Automatic	Network Service
Network Setup	...		Manual (Trig...	Local System
Network Store I	...	Running	Automatic	Local Service
Offline Files			Disabled	Local System

Opens the properties dialog box for the current selection.

2- Go to Log On tab, select "This account", and enter/change the SSO credentials that will be used for the connection to CCure 9000. 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)

Log on as:

○ Local System account

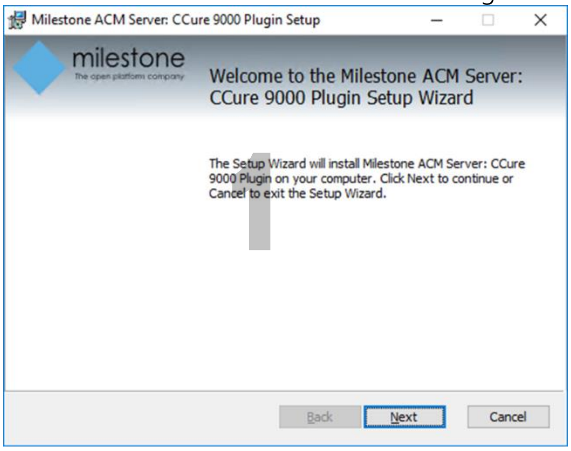
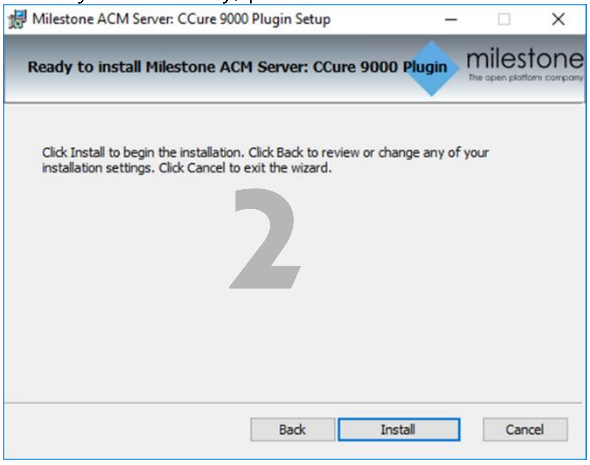
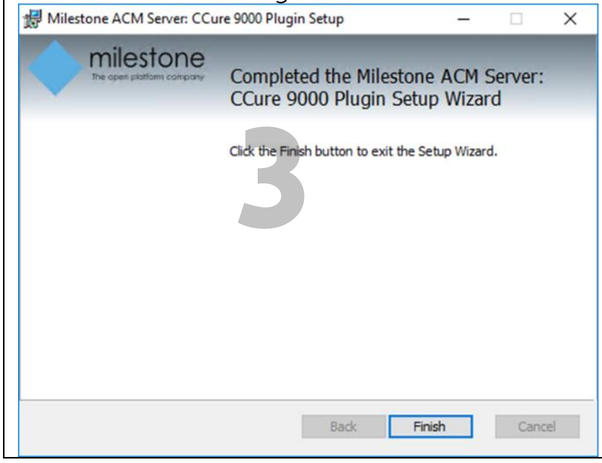
□ Allow service to interact with desktop

● This account: custdev.us\bha

Password: •••••••••••••••

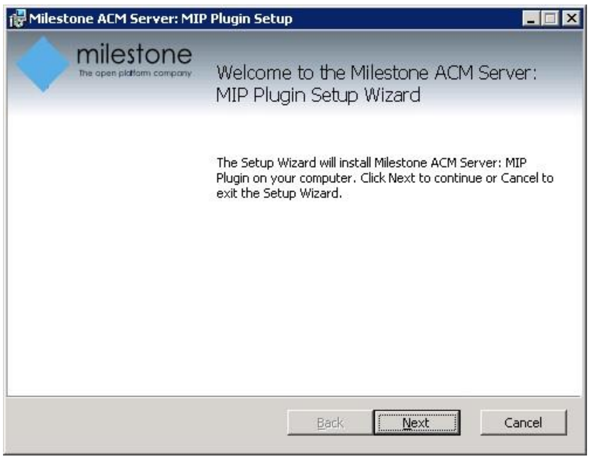
Confirm password: •••••••••••••••

ACM Server: CCure 9000 Plugin Installation

Copy the ”Milestone.ACMServer.CCure9k.msi” file to a temporay folder and double-click to install, you should see a screen similar to the following:  Milestone ACM Server: CCure 9000 Plugin Setup Welcome to the Milestone ACM Server: CCure 9000 Plugin Setup Wizard The Setup Wizard will install Milestone ACM Server: CCure 9000 Plugin on your computer. Click Next to continue or Cancel to exit the Setup Wizard. milestone The open platform company 1 Back Next Cancel The CCure 9000 plugin automatically detects the presence of both the CCure 9000 server and the pre-installed ACM Server. If either is missing it will refuse to install.	There are no configurable options in this installer. When you are ready, press install.  Milestone ACM Server: CCure 9000 Plugin Setup Ready to install Milestone ACM Server: CCure 9000 Plugin Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard. milestone The open platform company 2 Back Install Cancel
You have successfully installed the Milestone ACM Server CCure 9000 Plugin  Milestone ACM Server: CCure 9000 Plugin Setup Completed the Milestone ACM Server: CCure 9000 Plugin Setup Wizard Click the Finish button to exit the Setup Wizard. milestone The open platform company 3 Back Finish Cancel	

ACM Server: XProtect ACM MIP Plugin

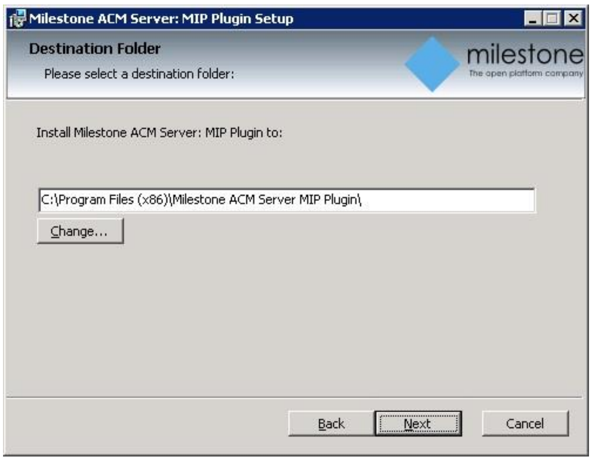
Copy the "Milestone.ACMServer.MipPlugin.msi" file to a temporary folder on the server where the XProtect Event Server is installed (in a typical deployment, this is the XProtect Management Server) and double-click to install. You should see a screen similar to the following:


Milestone ACM Server: MIP Plugin Setup
milestone
The open platform company
Back
Next
Cancel

Welcome to the Milestone ACM Server: MIP Plugin Setup Wizard

The Setup Wizard will install Milestone ACM Server: MIP Plugin on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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.


Milestone ACM Server: MIP Plugin Setup
milestone
The open platform company
Change...
Back
Next
Cancel

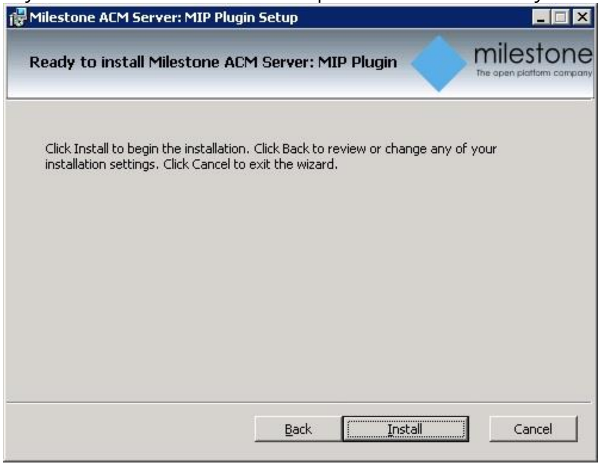
Destination Folder

Please select a destination folder:

Install Milestone ACM Server: MIP Plugin to:

C:\Program Files (x86)\Milestone ACM Server MIP Plugin\

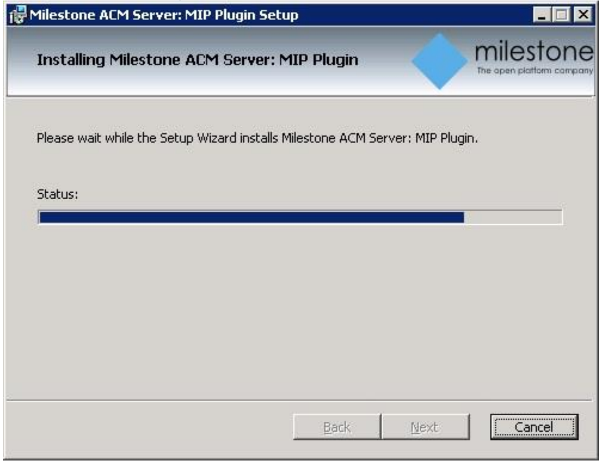
If you are satisfied with the path selection and you are ready to install press "Install"


Milestone ACM Server: MIP Plugin Setup
milestone
The open platform company
Back
Install
Cancel

Ready to install Milestone ACM Server: MIP Plugin

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Installation progress…



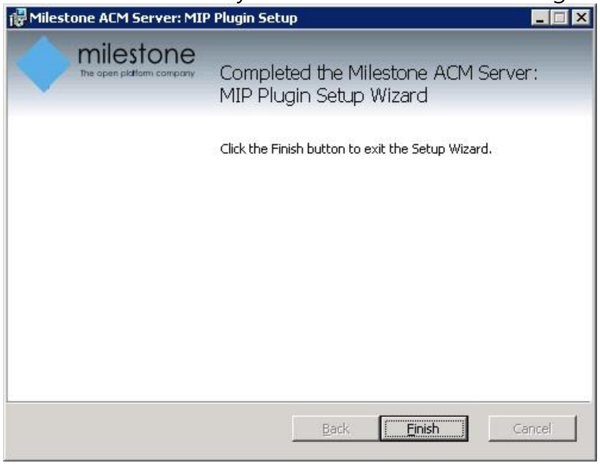
Milestone ACM Server: MIP Plugin Setup

Installing Milestone ACM Server: MIP Plugin

Please wait while the Setup Wizard installs Milestone ACM Server: MIP Plugin.

Status:

You have successfully installed the ACM MIP Plugin for ACM Server



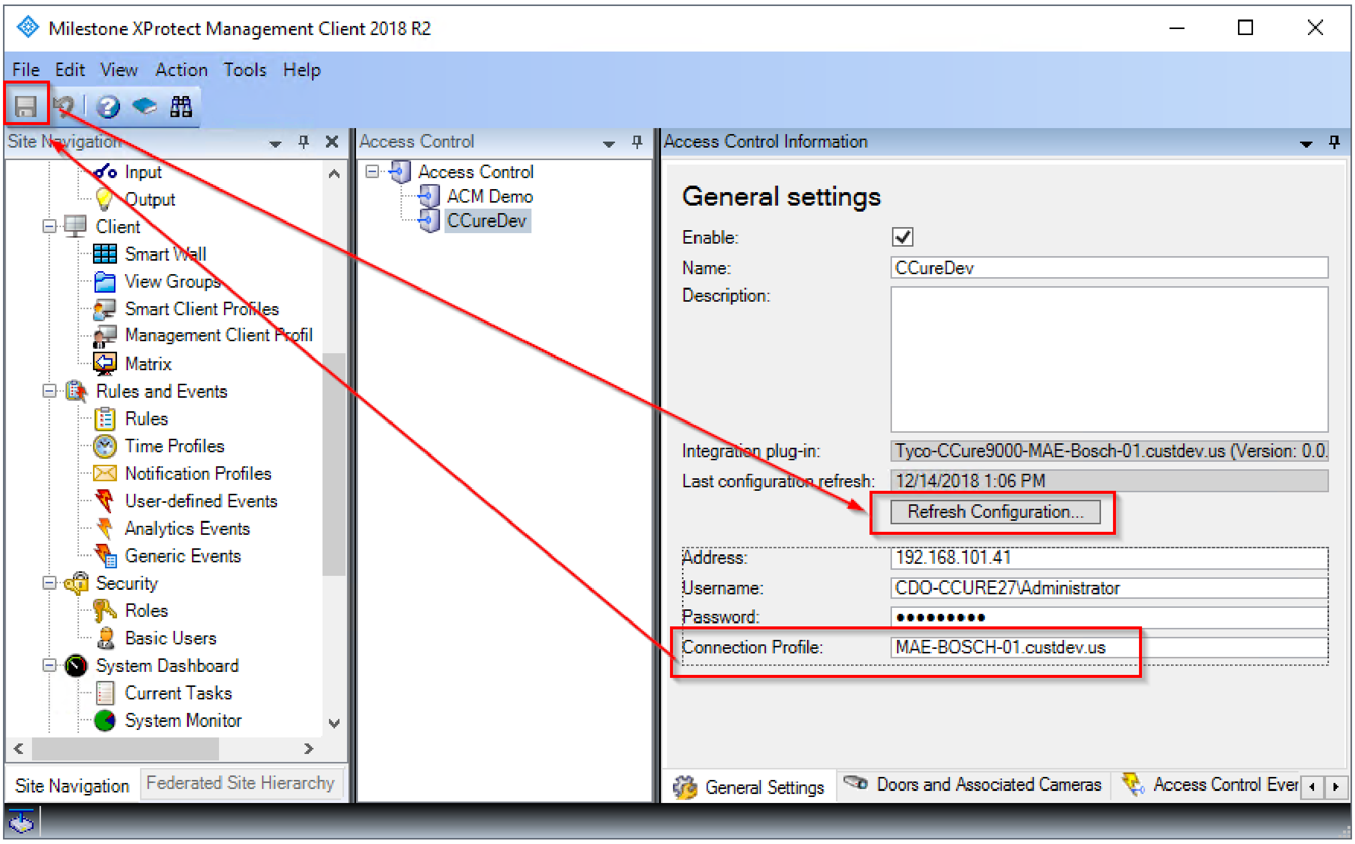
Milestone ACM Server: MIP Plugin Setup

Completed the Milestone ACM Server: MIP Plugin Setup Wizard

Click the Finish button to exit the Setup Wizard.

MIP Plugin Upgrades

- IMPORTANT – Always upgrade *both* the ACM Server and CCure 9000 ACM plugin on the CCure 9000 machine *before* upgrading the MIP Plugin. We distribute all the installers with every new CCure 9000 ACM release.
- Automatic MIP Plugin upgrades of configured and installed instances in the Management Client are supported for all versions of the CCure 9000 ACM integration.
- Simply run the MIP Plugin installer; it will upgrade any installed ACM Servers.
- After running the MIP Plugin installer, for each ACM instance in the Management Client:
  - Set the ConnectionProfileName property to the name of the ACM Server machine. Press Save to save the configuration change.
  - Click Refresh Configuration to update the configuration.



General settings

Enable: ☑

Name: CCureDev

Description:

Integration plug-in: Tyco-CCure9000-MAE-Bosch-01.custdev.us (Version: 0.0.

Last configuration refresh: 12/14/2018 1:06 PM

Address: 192.168.101.41

Username: CDO-CCURE27\Administrator

Password: •••••••••

Connection Profile: MAE-BOSCH-01.custdev.us

Upgrading will result in the following negative side-effects:

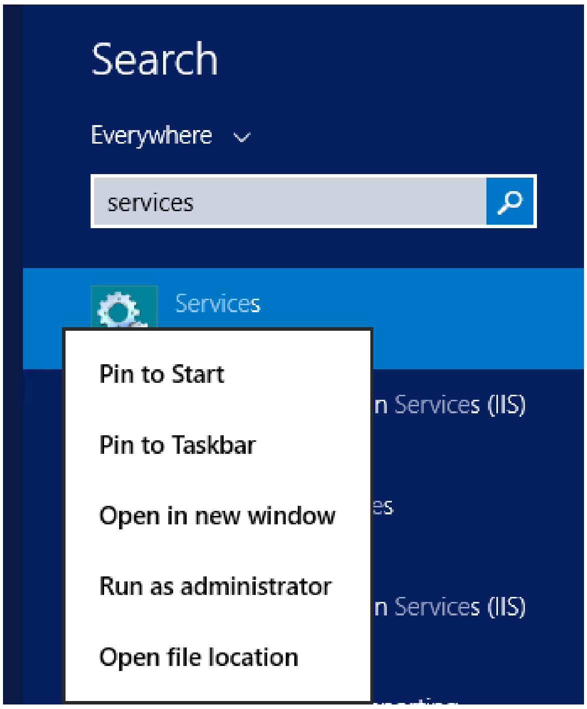
- Smart Client event history will be lost.
- Rules based off events and configured CCure 9000 hardware will no longer function. Rules based off the default access control event categories will not be affected and will continue to function.
- Custom event category assignments will be lost. The custom category will still exist; the user will just have to re-assign the category to events in the Management Client.

CCure 9000 Configuration

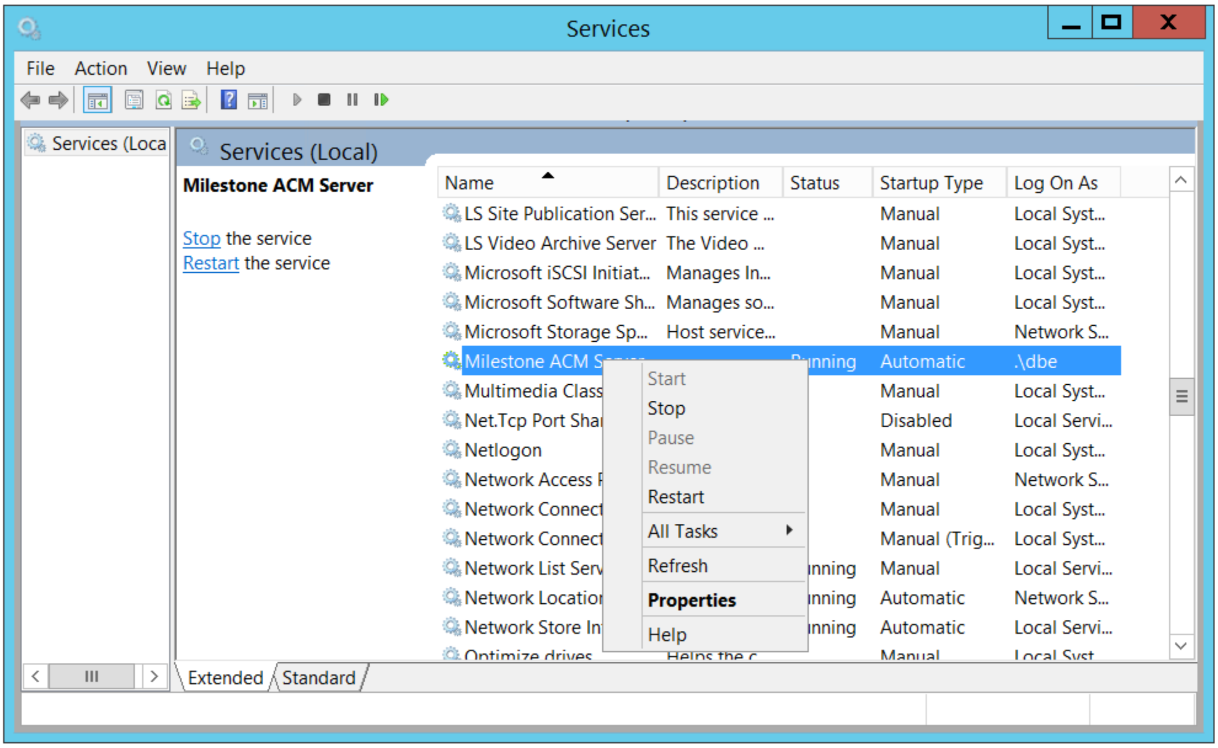
Configure to run as CCure 9000 Single-Sign-On Account

The CCure 9000 Plugin installer has already configured the ACM Server to run as the single sign-on account. You only need to do the following if you need to change the ACM Server's credentials.

On the CCure 9000 server machine, click the Windows Start menu and type "services". Right click Services and select "Run as administrator".

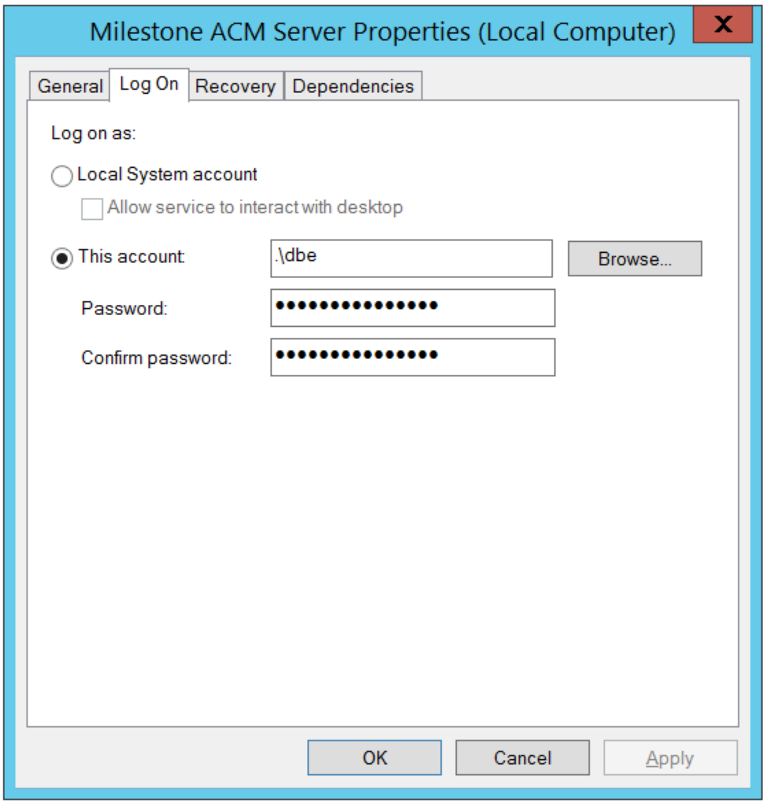


Right-click the Milestone ACM Server service and select Properties:



Name	Description	Status	Startup Type	Log On As
LS Site Publication Ser...	This service ...		Manual	Local Syst...
LS Video Archive Server	The Video ...		Manual	Local Syst...
Microsoft iSCSI Initiat...	Manages In...		Manual	Local Syst...
Microsoft Software Sh...	Manages so...		Manual	Local Syst...
Microsoft Storage Sp...	Host service...		Manual	Network S...
Milestone ACM S		Running	Automatic	.\dbe
Multimedia Class			Manual	Local Syst...
Net.Tcp Port Shar			Disabled	Local Servi...
Netlogon			Manual	Local Syst...
Network Access P			Manual	Network S...
Network Connect			Manual	Local Syst...
Network Connect			Manual (Trig...	Local Syst...
Network List Serv		nning	Manual	Local Servi...
Network Locatior		nning	Automatic	Network S...
Network Store In		nning	Automatic	Local Servi...
Optimize drives	Helps the c		Manual	Local Syst

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 CCure 9000 Directory that is configured for single sign-on (see above for configuring single sign-on).



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\dbe

Password: •••••••••••••••

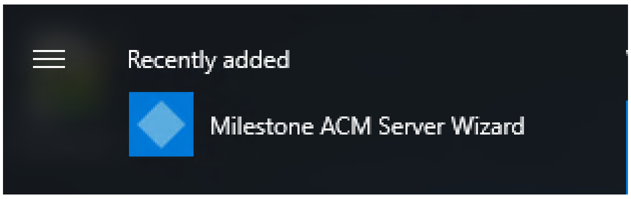
Confirm password: •••••••••••••••

IMPORTANT: Restart the Milestone ACM Server service.

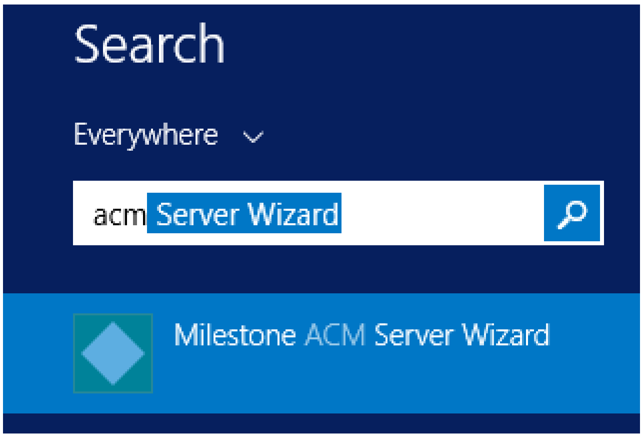
XProtect ACM MIP Plugin Configuration

ACM Server Wizard

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

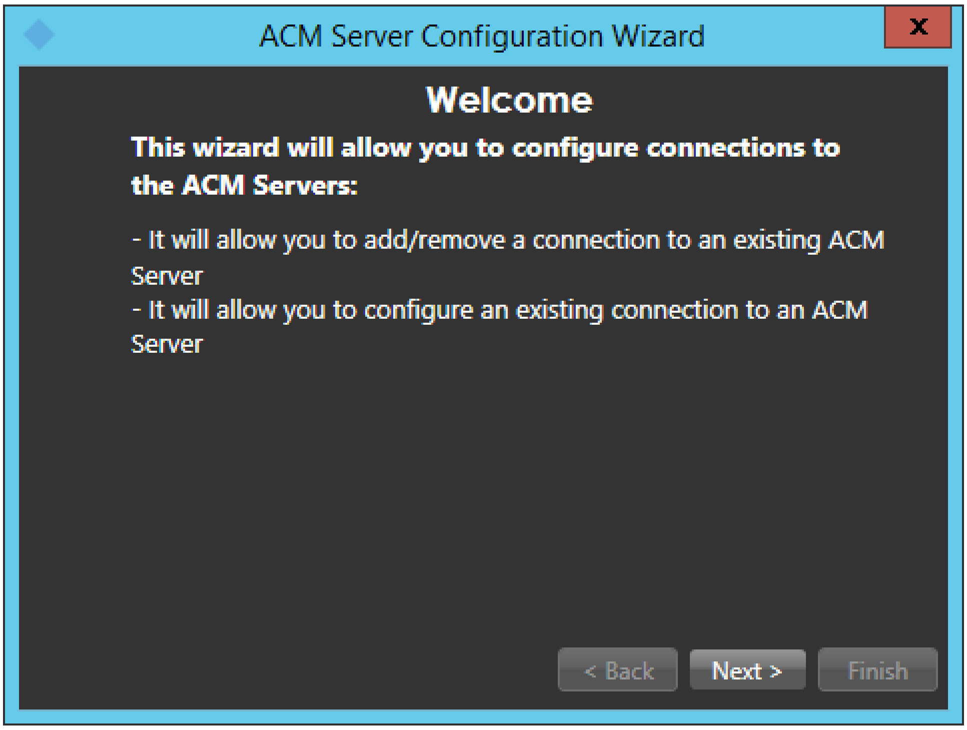


or



Installing an ACM Server

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

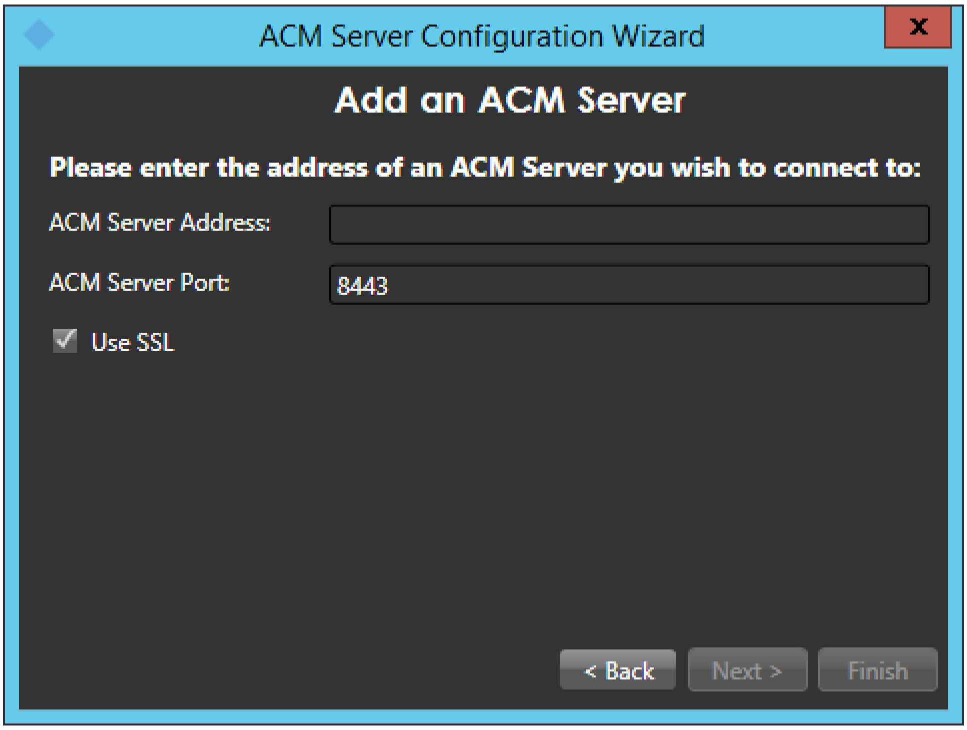


Welcome

This wizard will allow you to configure connections to the ACM Servers:

- It will allow you to add/remove a connection to an existing ACM Server
- It will allow you to configure an existing connection to an ACM Server

Once you click next, you will have to provide the IP Address / Machine name of the CCure 9000 server on which the ACM Server package was installed.



Add an ACM Server

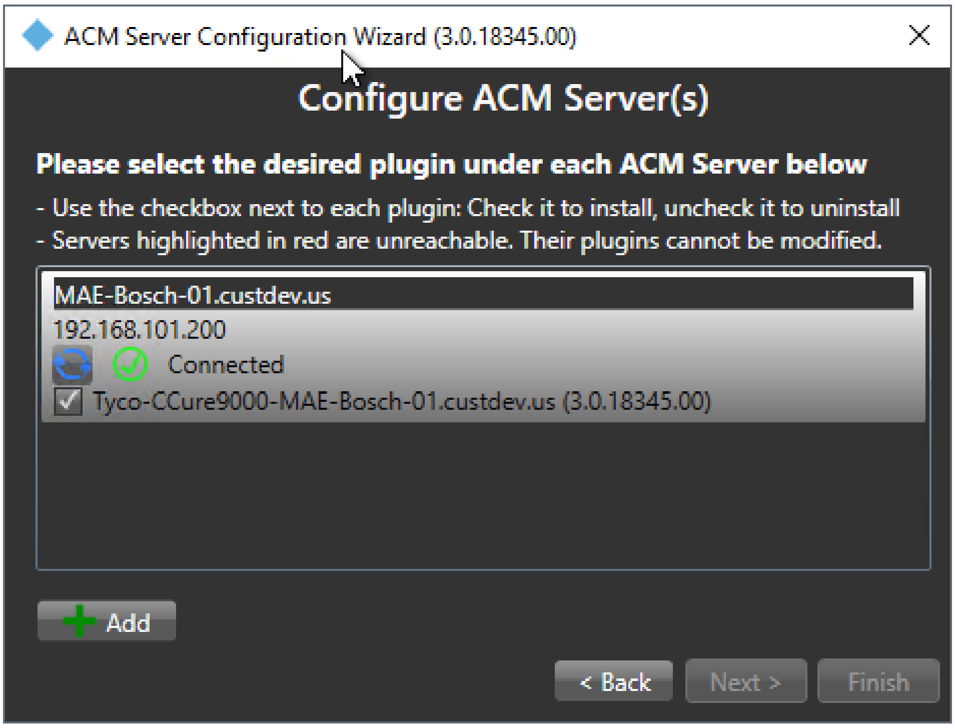
Please enter the address of an ACM Server you wish to connect to:

ACM Server Address:

ACM Server Port: 8443

☑ Use SSL

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 (3.0.18345.00)

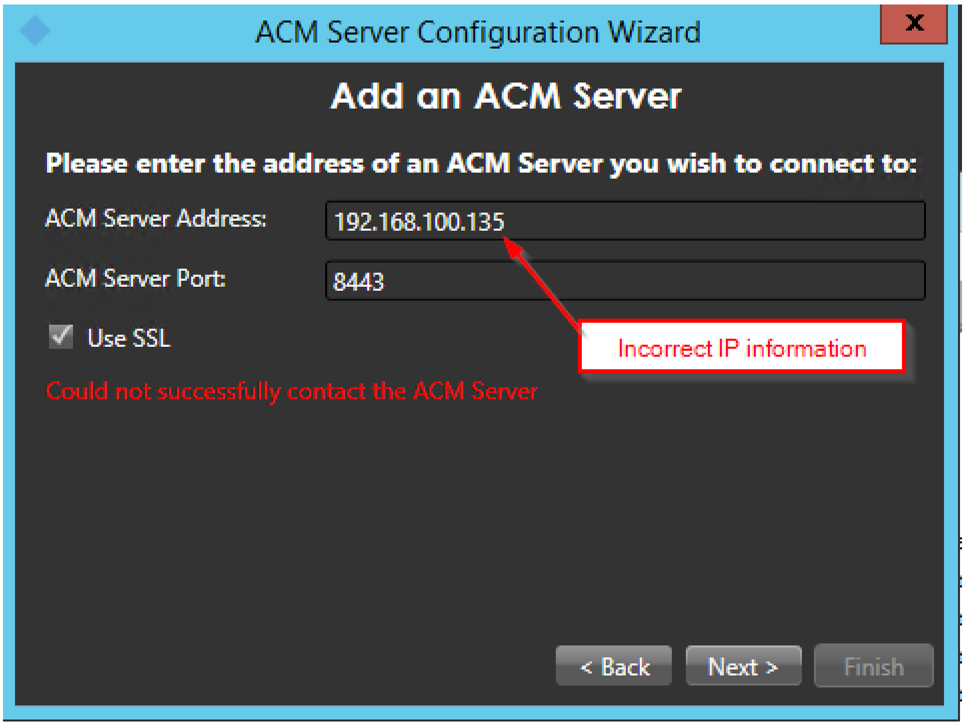
Configure ACM Server(s)

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.

MAE-Bosch-01.custdev.us
192.168.101.200
✓ Connected
☑ Tyco-CCure9000-MAE-Bosch-01.custdev.us (3.0.18345.00)

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 CCure 9000 machine is not running with sufficient administrative privileges.



ACM Server Configuration Wizard

Add an ACM Server

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

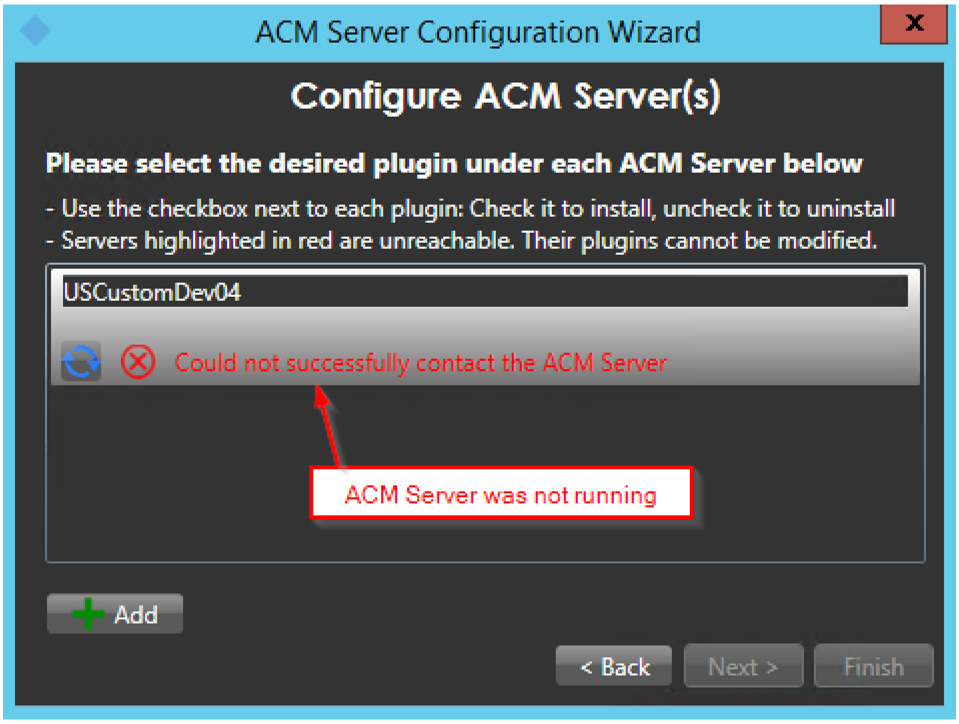
ACM Server Address: 192.168.100.135

ACM Server Port: 8443

☑ Use SSL

Incorrect IP information

Could not successfully contact the ACM Server



ACM Server Configuration Wizard

Configure ACM Server(s)

Please select the desired plugin under each ACM Server below

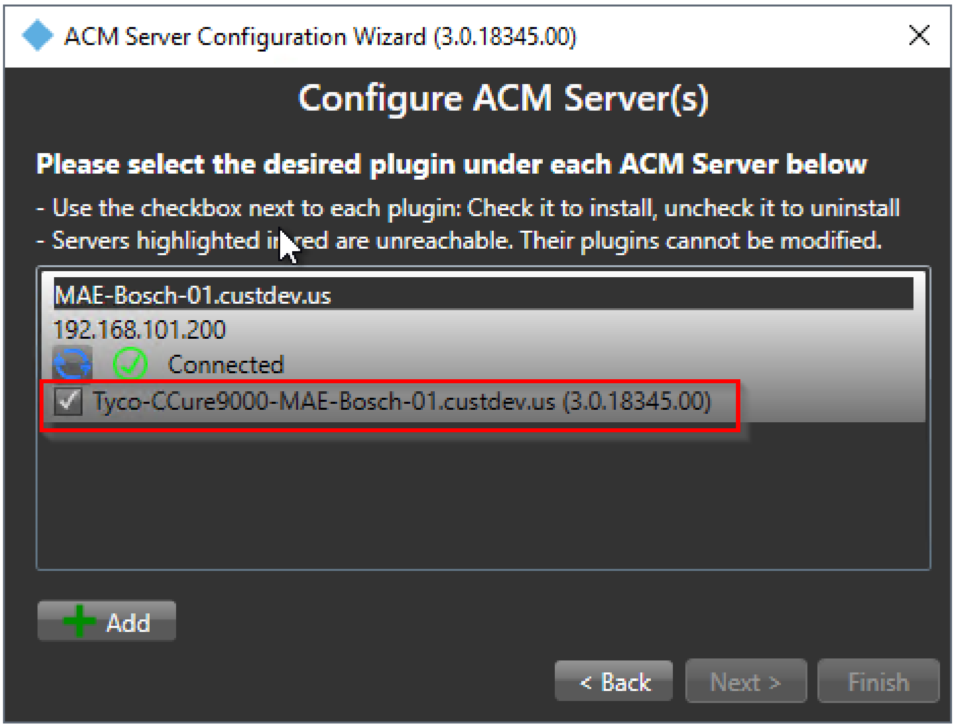
- Use the checkbox next to each plugin: Check it to install, uncheck it to uninstall
- Servers highlighted in red are unreachable. Their plugins cannot be modified.

USCustomDev04

Could not successfully contact the ACM Server

ACM Server was not running

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 CCure 9000.



ACM Server Configuration Wizard (3.0.18345.00)

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.

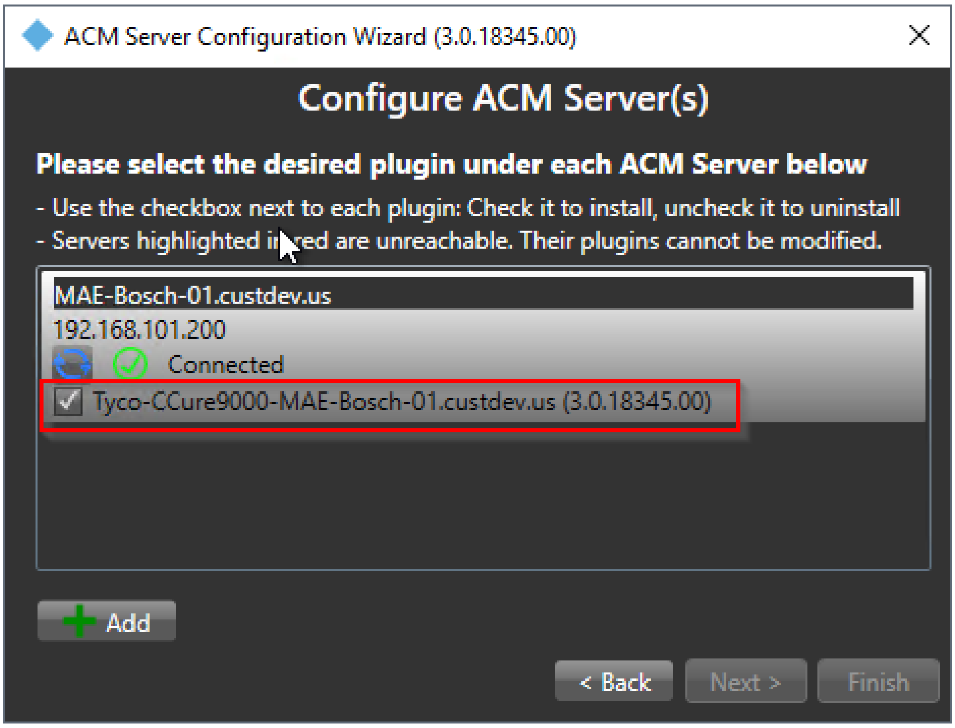
MAE-Bosch-01.custdev.us

192.168.101.200

Connected

☑ Tyco-CCure9000-MAE-Bosch-01.custdev.us (3.0.18345.00)

Check the box marked below and press next to install a MIP plugin on this host to connect to the CCure 9000 server identified.



ACM Server Configuration Wizard (3.0.18345.00)

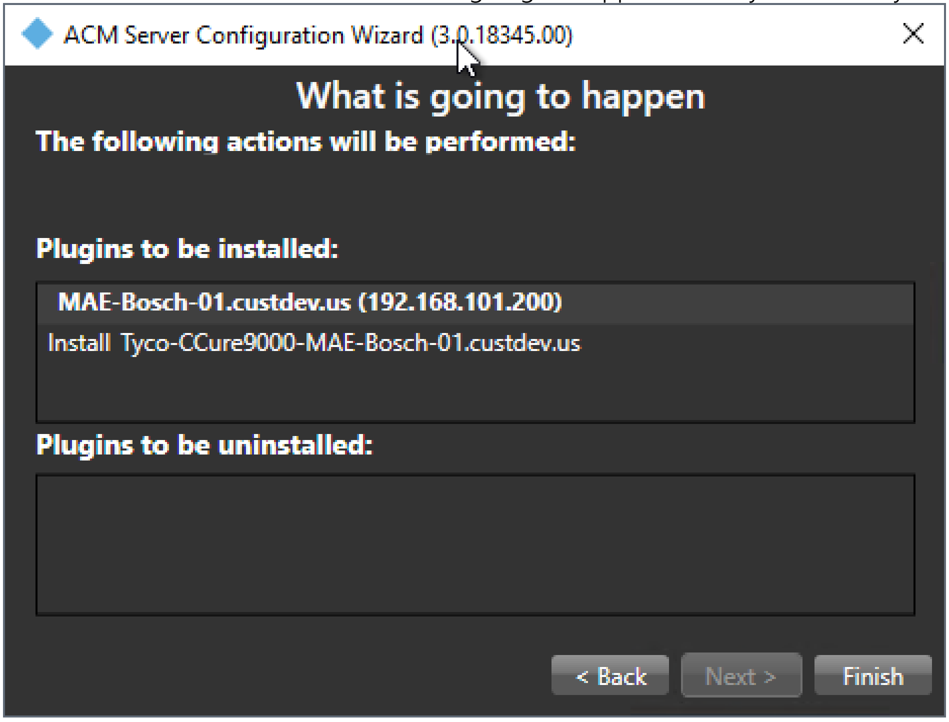
Configure ACM Server(s)

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.

MAE-Bosch-01.custdev.us
192.168.101.200
Connected
☑ Tyco-CCure9000-MAE-Bosch-01.custdev.us (3.0.18345.00)

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



ACM Server Configuration Wizard (3.0.18345.00)

What is going to happen

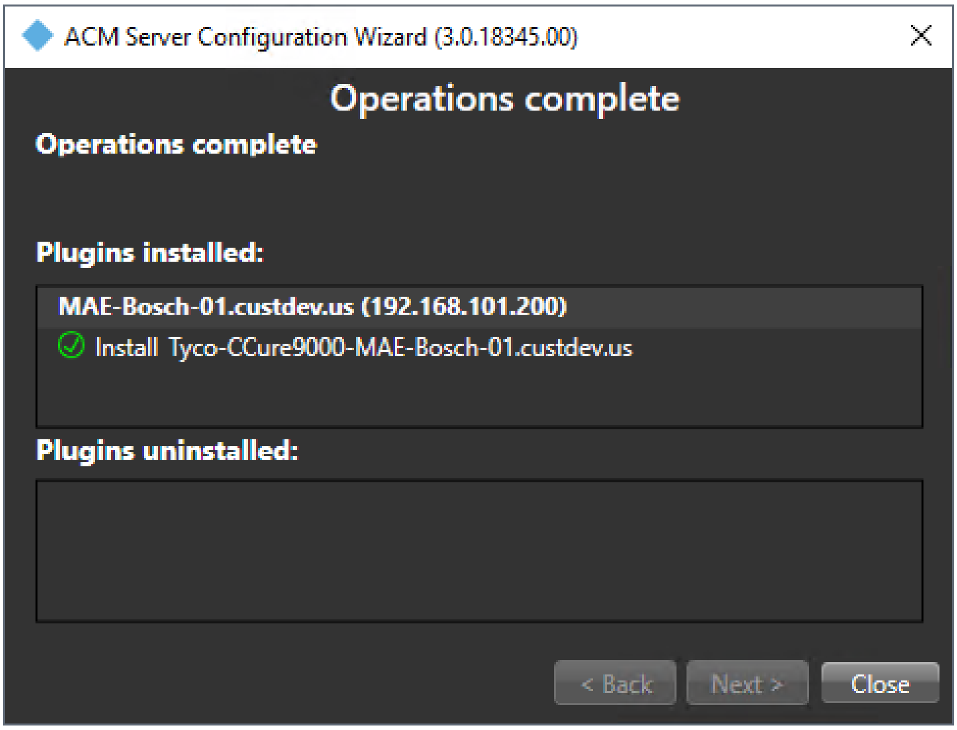
The following actions will be performed:

Plugins to be installed:

MAE-Bosch-01.custdev.us (192.168.101.200)
Install Tyco-CCure9000-MAE-Bosch-01.custdev.us

Plugins to be uninstalled:

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



Operations complete

Operations complete

Plugins installed:

MAE-Bosch-01.custdev.us (192.168.101.200)

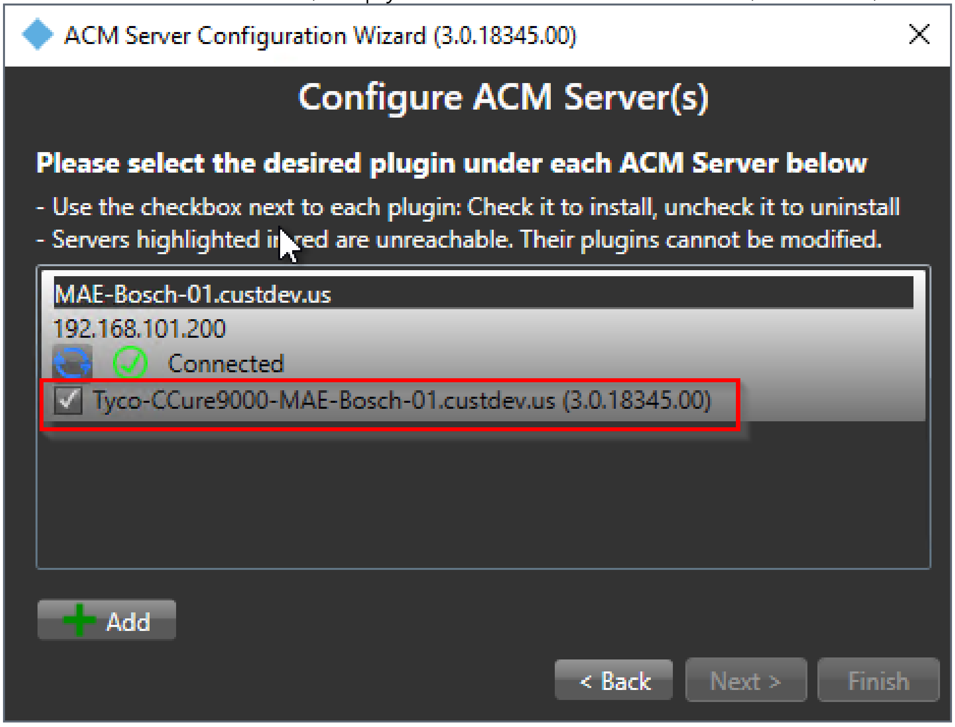
✓ Install Tyco-CCure9000-MAE-Bosch-01.custdev.us

Plugins uninstalled:

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.



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.

MAE-Bosch-01.custdev.us

192.168.101.200

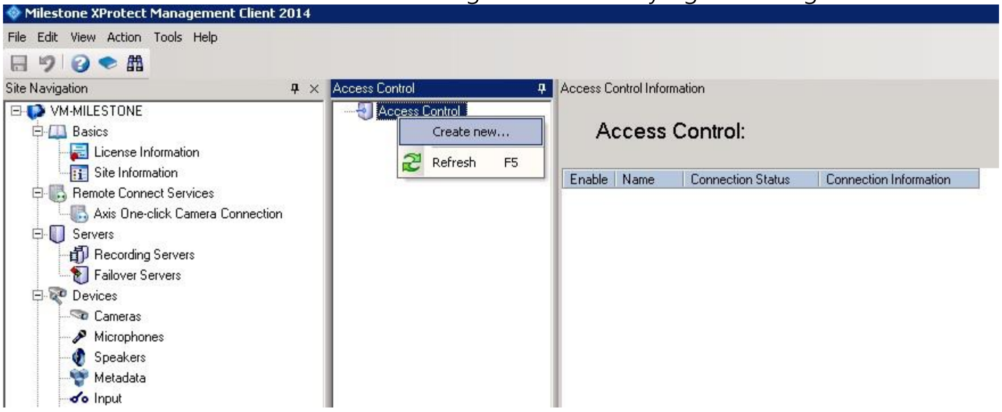
✓ Connected

☑ Tyco-CCure9000-MAE-Bosch-01.custdev.us (3.0.18345.00)

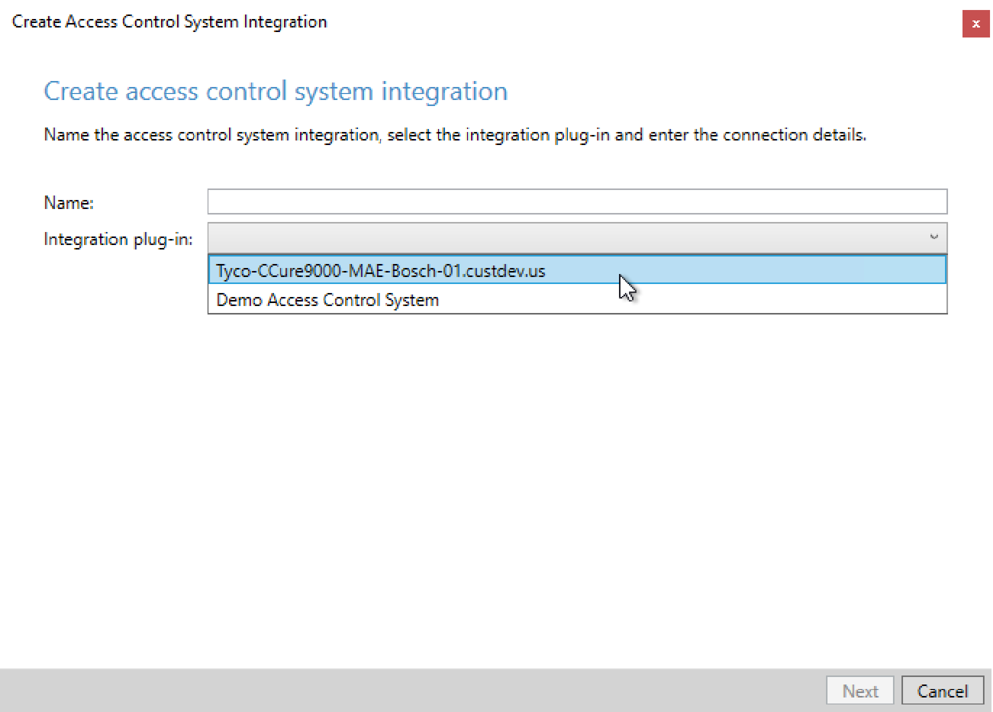
XProtect Management Client Configuration

XProtect Management Client

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



This will pop up a wizard to step you through the access control instance creation process. Type a name for the instance of the plugin you wish to create and select from the drop-down box the integration plug-in. Note that you will find a plugin named Tyco-CCure-9000-{ServerName} where {ServerName} is the name of the machine where CCure 9000 and ACM Server are installed.



Create Access Control System Integration

Create access control system integration

Name the access control system integration, select the integration plug-in and enter the connection details.

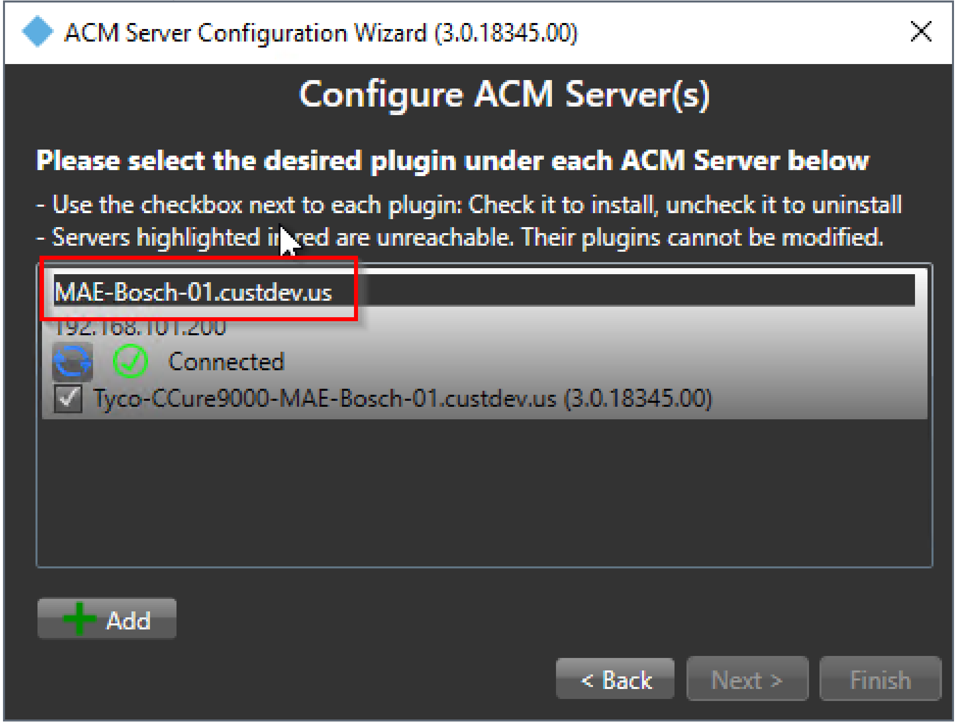
Name:

Integration plug-in:

Tyco-CCure9000-MAE-Bosch-01.custdev.us
Demo Access Control System
Next
Cancel

After selecting the plugin, you will have to provide credentials and parameters to configure the connection to the CCure 9000 database server.

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 (3.0.18345.00)

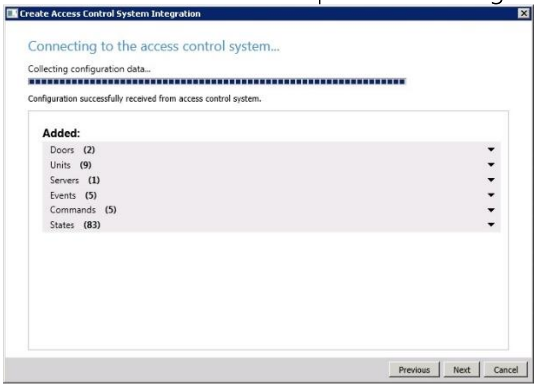
Configure ACM Server(s)

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.

MAE-Bosch-01.custdev.us
192.168.101.200
Connected
☑ Tyco-CCure9000-MAE-Bosch-01.custdev.us (3.0.18345.00)

The wizard will now fetch the configuration of the CCure 9000 AC system into Milestone.
The screen below is an example of the configuration found on the server:



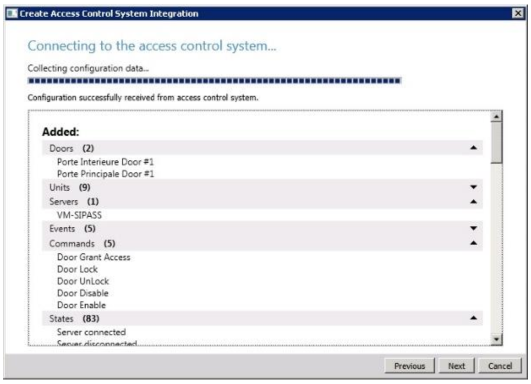
Create Access Control System Integration

Connecting to the access control system...

Collecting configuration data...

Configuration successfully received from access control system.

Added:
Doors (2)
Units (9)
Servers (1)
Events (5)
Commands (5)
States (83)



Create Access Control System Integration

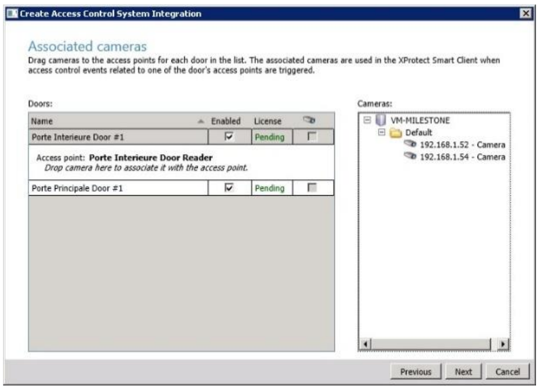
Connecting to the access control system...

Collecting configuration data...

Configuration successfully received from access control system.

Added:
Doors (2)
Porte Interieure Door #1
Porte Principale Door #1
Units (9)
Servers (1)
VM-SIPASS
Events (5)
Commands (5)
Door Grant Access
Door Lock
Door UnLock
Door Disable
Door Enable
States (83)
Server connected
Server disconnected

On this screen an association must 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.



Create Access Control System Integration

Associated cameras

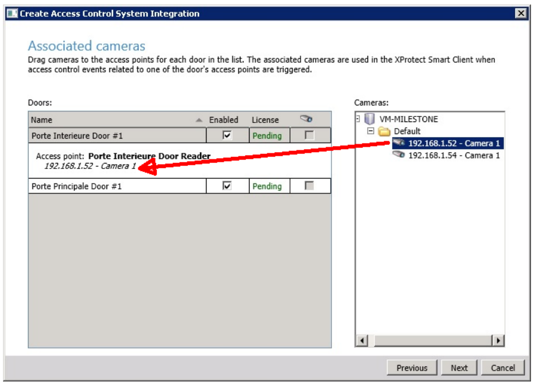
Drag cameras to the access points for each door in the list. The associated cameras are used in the XProtect Smart Client when access control events related to one of the door's access points are triggered.

Doors:

Name	Enabled	License	
Porte Interieure Door #1	☑	Pending	☐
Access point: **Porte Interieure Door Reader** *Drop camera here to associate it with the access point.*			
Porte Principale Door #1	☑	Pending	☐

Cameras:

- VM-MILESTONE
  - Default
    - 192.168.1.52 - Camera
    - 192.168.1.54 - Camera



Create Access Control System Integration

Associated cameras

Drag cameras to the access points for each door in the list. The associated cameras are used in the XProtect Smart Client when access control events related to one of the door's access points are triggered.

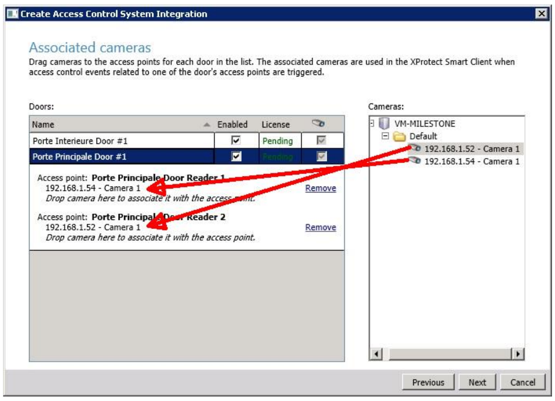
Doors:

Name	Enabled	License	
Porte Interieure Door #1	☑	Pending	☐
Access point: **Porte Interieure Door Reader** *192.168.1.52 - Camera 1*			
Porte Principale Door #1	☑	Pending	☐

Cameras:

- VM-MILESTONE
  - Default
    - 192.168.1.52 - Camera 1
    - 192.168.1.54 - Camera 1

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:



Create Access Control System Integration

Associated cameras

Drag cameras to the access points for each door in the list. The associated cameras are used in the XProtect Smart Client when access control events related to one of the door's access points are triggered.

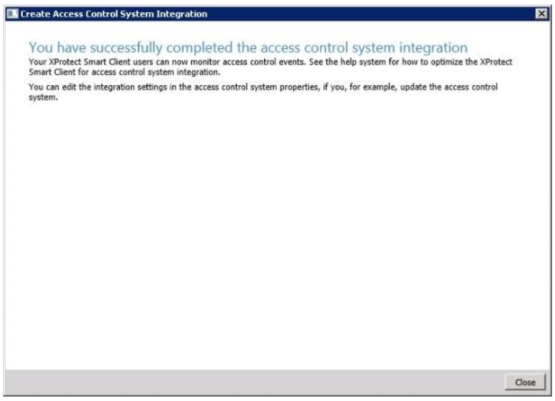
Doors:

Name	Enabled	License	
Porte Interieure Door #1	☑	Pending	☑
Porte Principale Door #1	☑	Pending	☑
Access point: **Porte Principale Door Reader 1** 192.168.1.54 - Camera 1 *Drop camera here to associate it with the access point.*			Remove
Access point: **Porte Principale Door Reader 2** 192.168.1.52 - Camera 1 *Drop camera here to associate it with the access point.*			Remove

Cameras:

- VM-MILESTONE
  - Default
    - 192.168.1.52 - Camera 1
    - 192.168.1.54 - Camera 1

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



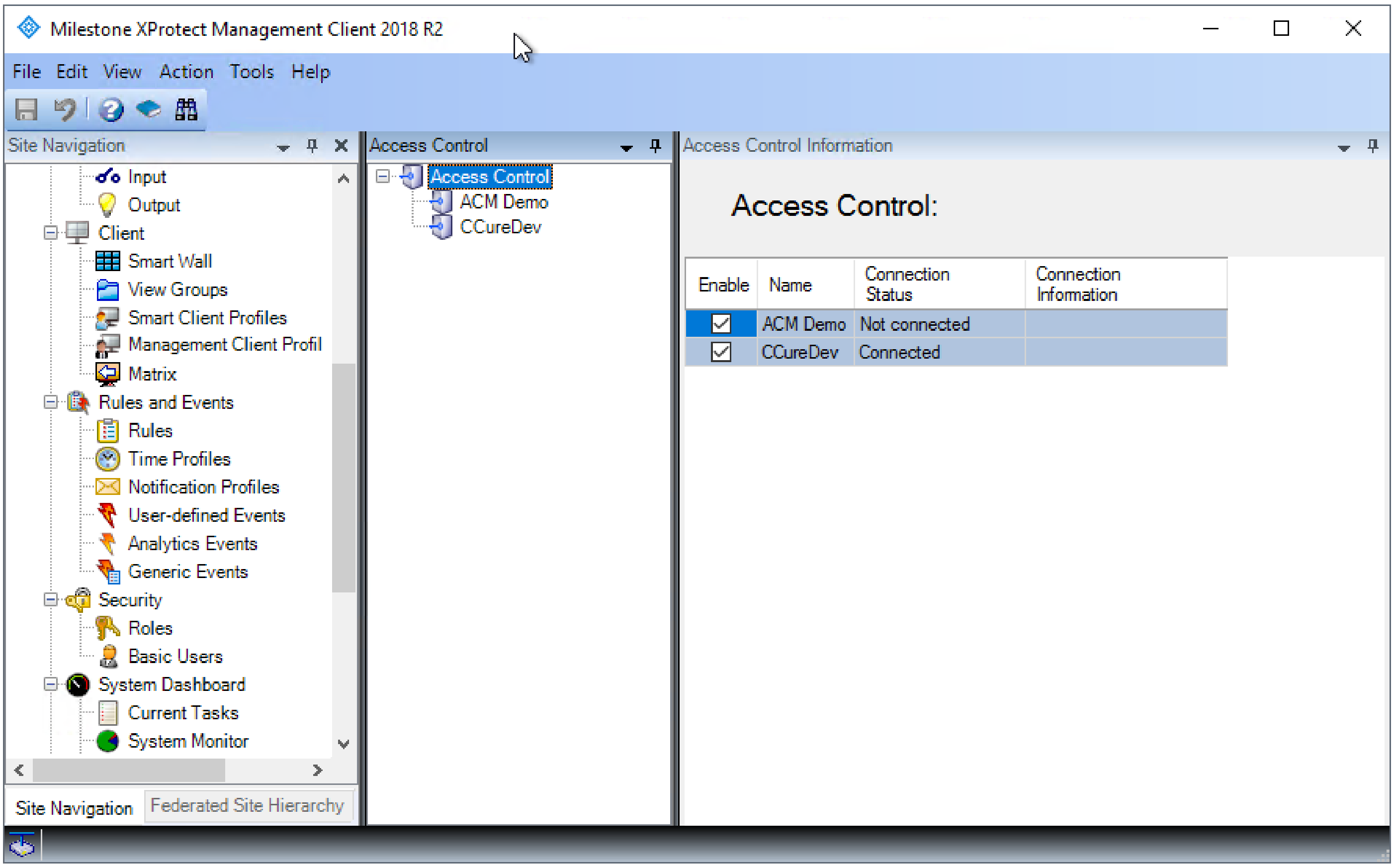
Create Access Control System Integration

You have successfully completed the access control system integration

Your XProtect Smart Client users can now monitor access control events. See the help system for how to optimize the XProtect Smart Client for access control system integration.

You can edit the integration settings in the access control system properties, if you, for example, update the access control system.

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



Access Control:

Enable	Name	Connection Status	Connection Information
☑	ACM Demo	Not connected	
☑	CCureDev	Connected	

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.

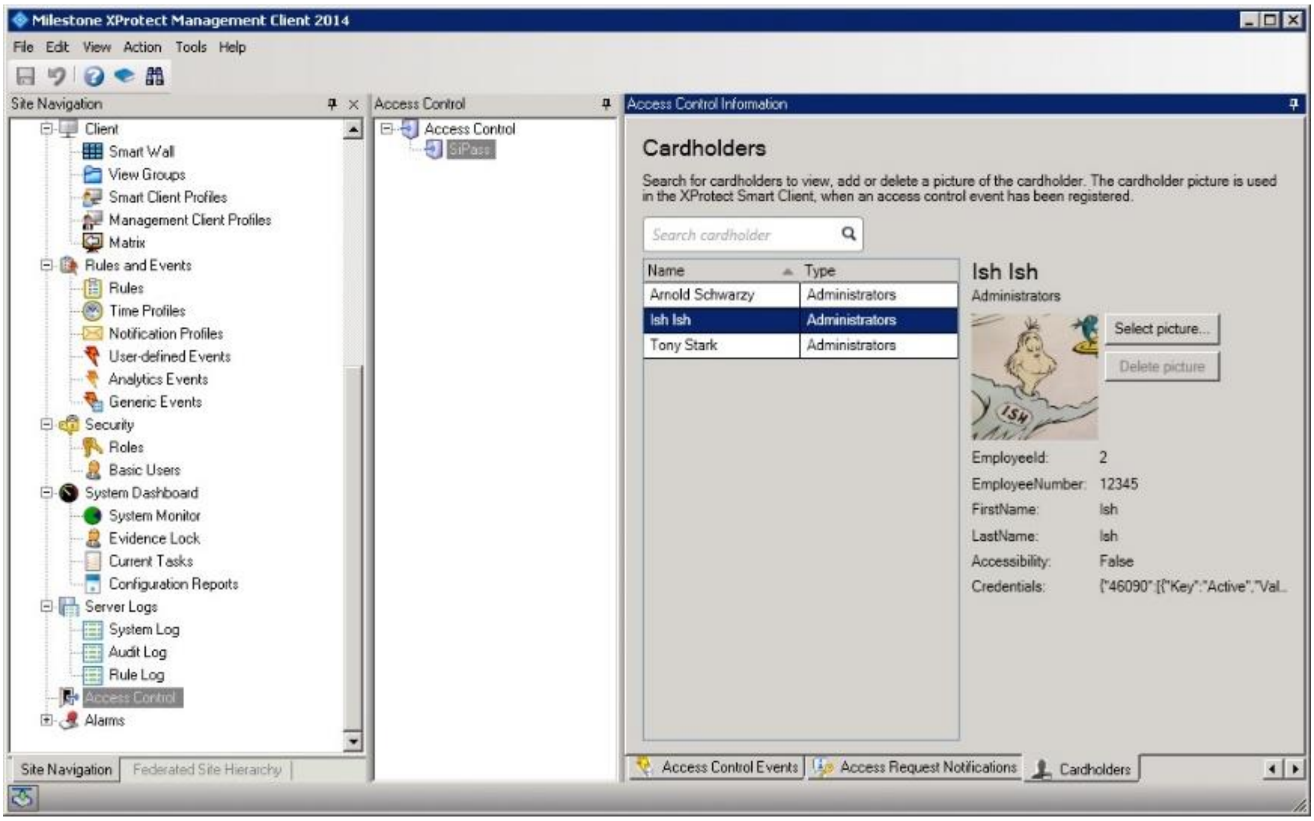
An access control plugin must specifically support personalized login. The CCure 9000 ACM plugin does NOT support it.

Common Actions

Searching for cardholders

Only “active” cardholders are downloaded from the CCure 9000 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 CCure 9000 system through the management client interface:



Cardholders

Search for cardholders to view, add or delete a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered.

Name	Type
Arnold Schwarzy	Administrators
Ish Ish	Administrators
Tony Stark	Administrators

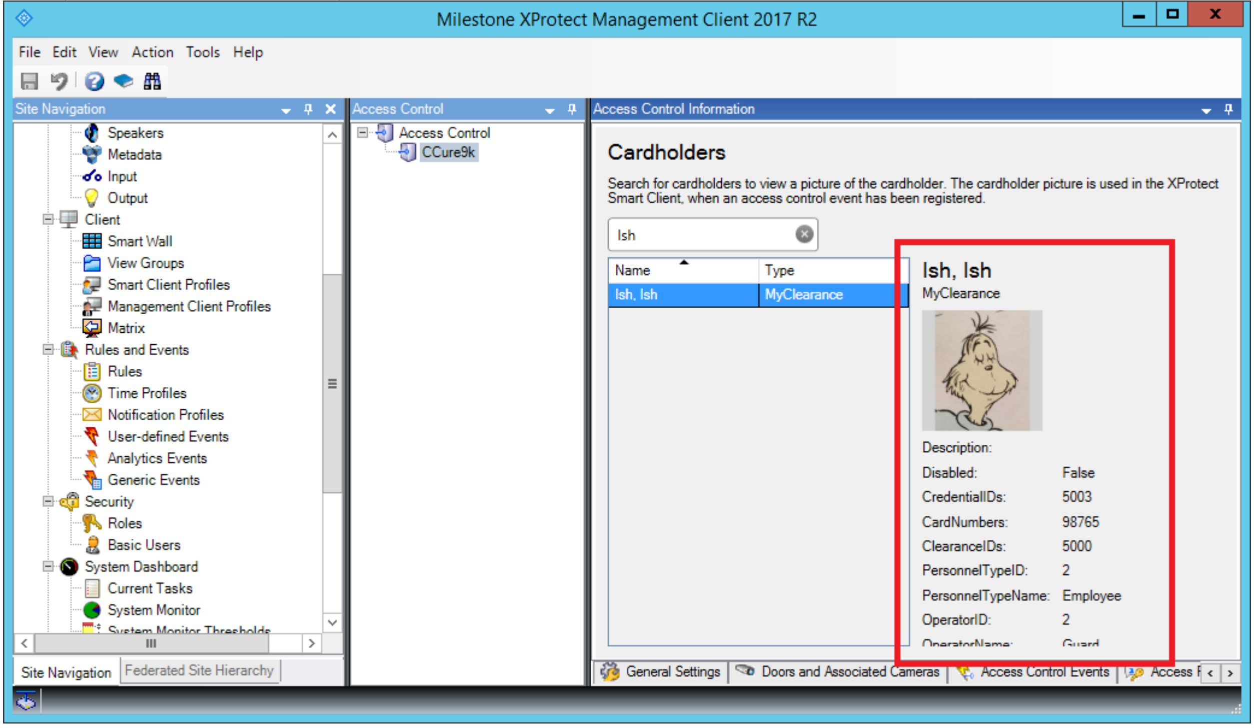
Ish Ish
Administrators

EmployeeId:	2
EmployeeNumber:	12345
FirstName:	Ish
LastName:	Ish
Accessibility:	False
Credentials:	{"46090":[{"Key":"Active","Val...

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.



Cardholders

Search for cardholders to view a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an access control event has been registered.

Ish

Name	Type
Ish, Ish	MyClearance

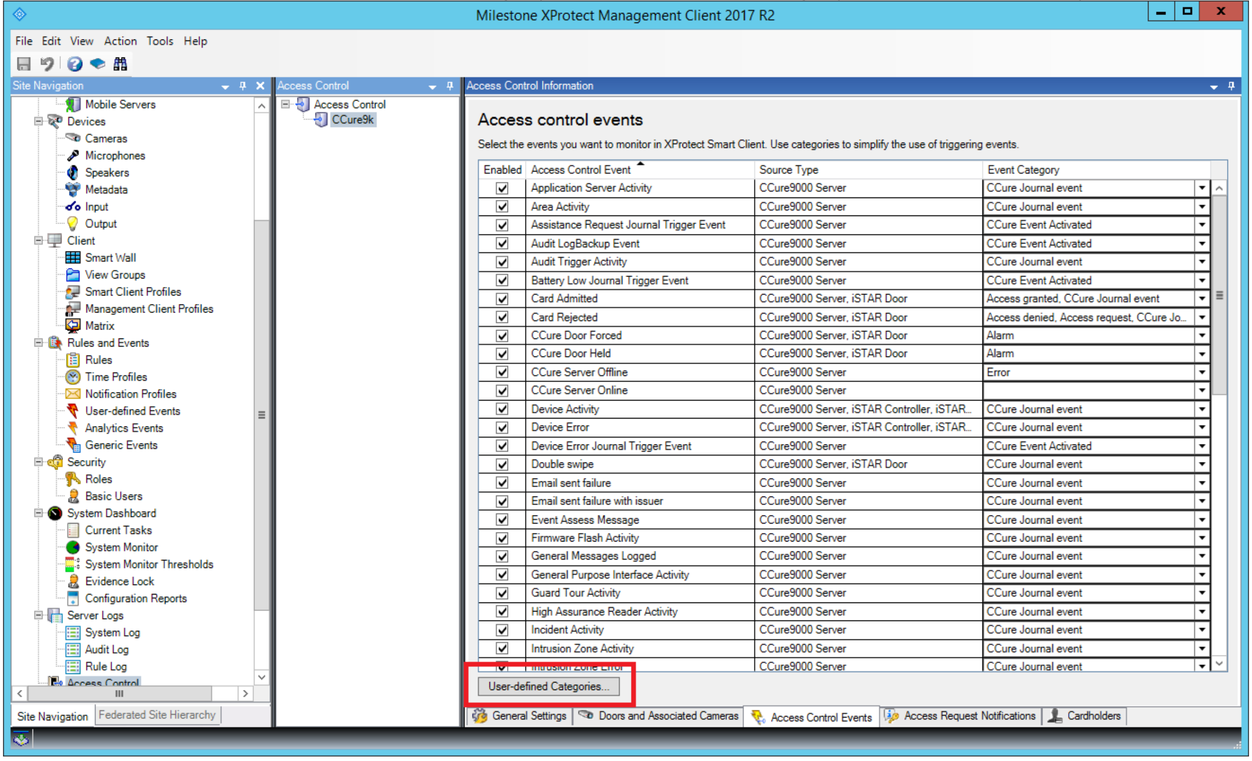
Ish, Ish

MyClearance

Description:	
Disabled:	False
CredentialIDs:	5003
CardNumbers:	98765
ClearanceIDs:	5000
PersonnelTypeID:	2
PersonnelTypeName:	Employee
OperatorID:	2
OperatorName:	Guard

Defining alarms based on CCure 9000 events

To define alarms based on CCure 9000 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:

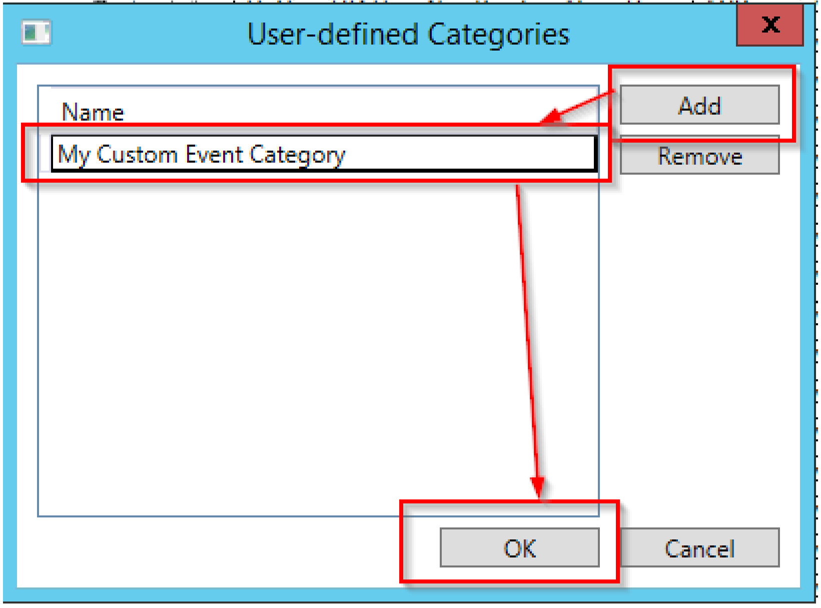


Access control events

Select the events you want to monitor in XProtect Smart Client. Use categories to simplify the use of triggering events.

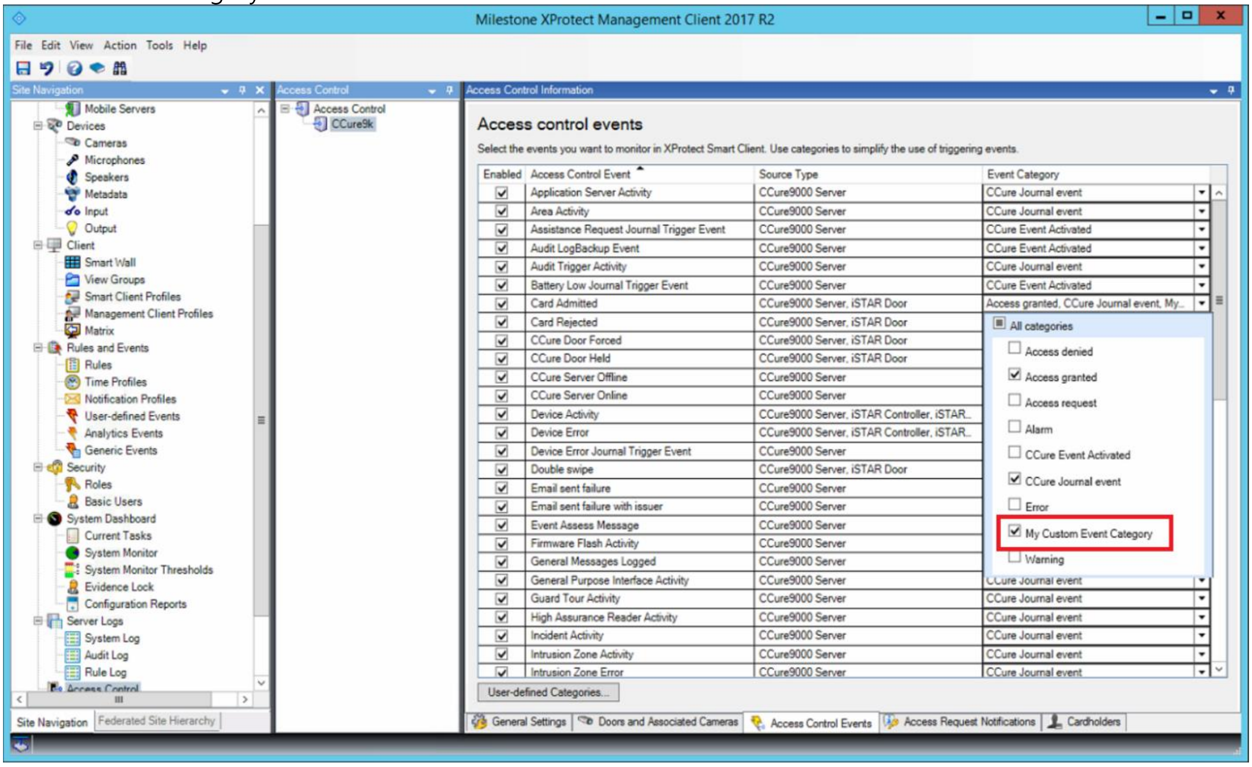
Enabled	Access Control Event	Source Type	Event Category
☑	Application Server Activity	CCure9000 Server	CCure Journal event
☑	Area Activity	CCure9000 Server	CCure Journal event
☑	Assistance Request Journal Trigger Event	CCure9000 Server	CCure Event Activated
☑	Audit LogBackup Event	CCure9000 Server	CCure Event Activated
☑	Audit Trigger Activity	CCure9000 Server	CCure Journal event
☑	Battery Low Journal Trigger Event	CCure9000 Server	CCure Event Activated
☑	Card Admitted	CCure9000 Server, iSTAR Door	Access granted, CCure Journal event
☑	Card Rejected	CCure9000 Server, iSTAR Door	Access denied, Access request, CCure Jo...
☑	CCure Door Forced	CCure9000 Server, iSTAR Door	Alarm
☑	CCure Door Held	CCure9000 Server, iSTAR Door	Alarm
☑	CCure Server Offline	CCure9000 Server	Error
☑	CCure Server Online	CCure9000 Server	
☑	Device Activity	CCure9000 Server, iSTAR Controller, iSTAR...	CCure Journal event
☑	Device Error	CCure9000 Server, iSTAR Controller, iSTAR...	CCure Journal event
☑	Device Error Journal Trigger Event	CCure9000 Server	CCure Event Activated
☑	Double swipe	CCure9000 Server, iSTAR Door	CCure Journal event
☑	Email sent failure	CCure9000 Server	CCure Journal event
☑	Email sent failure with issuer	CCure9000 Server	CCure Journal event
☑	Event Assess Message	CCure9000 Server	CCure Journal event
☑	Firmware Flash Activity	CCure9000 Server	CCure Journal event
☑	General Messages Logged	CCure9000 Server	CCure Journal event
☑	General Purpose Interface Activity	CCure9000 Server	CCure Journal event
☑	Guard Tour Activity	CCure9000 Server	CCure Journal event
☑	High Assurance Reader Activity	CCure9000 Server	CCure Journal event
☑	Incident Activity	CCure9000 Server	CCure Journal event
☑	Intrusion Zone Activity	CCure9000 Server	CCure Journal event
☑	Intrusion Zone Error	CCure9000 Server	CCure Journal event

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



My Custom Event Category

Associate the category with one of the CCure 9000 AC events:



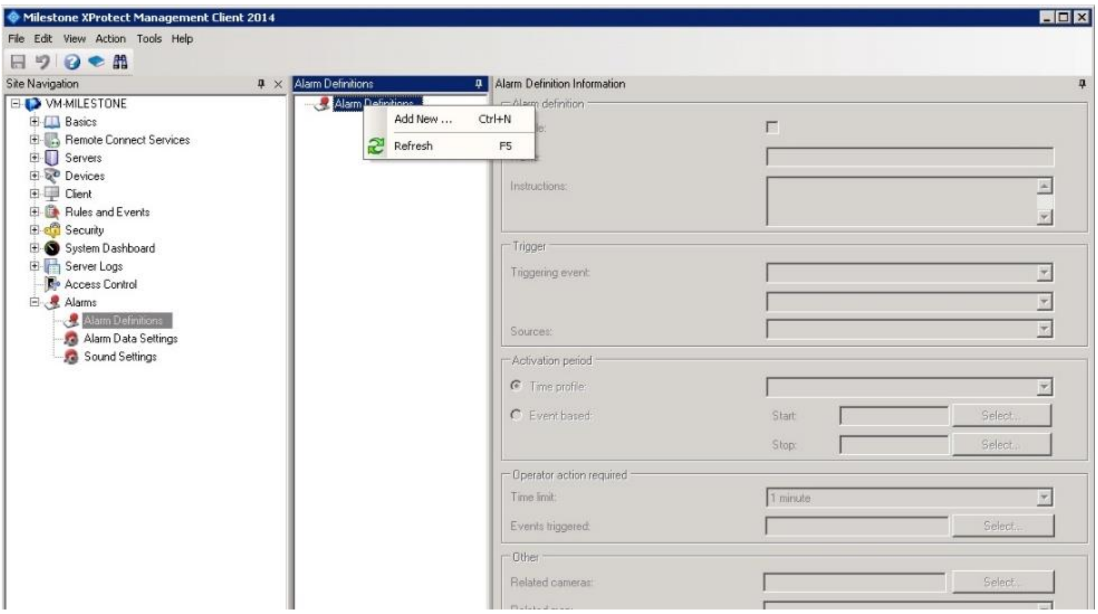
Access control events

Select the events you want to monitor in XProtect Smart Client. Use categories to simplify the use of triggering events.

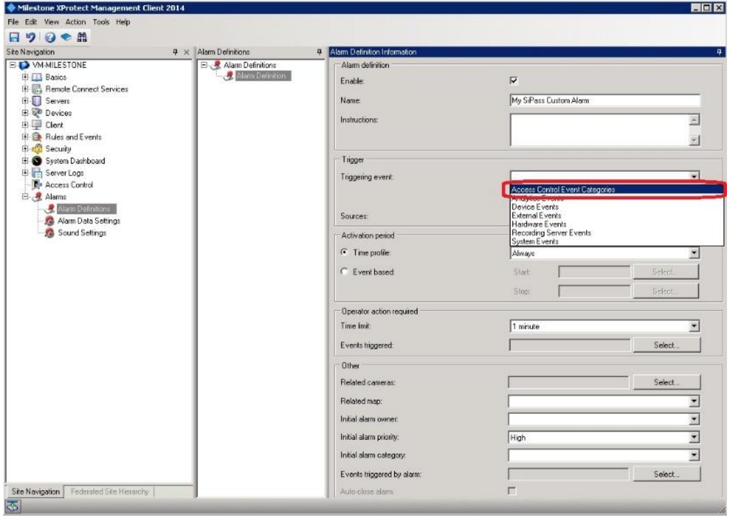
Enabled	Access Control Event	Source Type	Event Category
☑	Application Server Activity	CCure9000 Server	CCure Journal event
☑	Area Activity	CCure9000 Server	CCure Journal event
☑	Assistance Request Journal Trigger Event	CCure9000 Server	CCure Event Activated
☑	Audit LogBackup Event	CCure9000 Server	CCure Event Activated
☑	Audit Trigger Activity	CCure9000 Server	CCure Journal event
☑	Battery Low Journal Trigger Event	CCure9000 Server	CCure Event Activated
☑	Card Admitted	CCure9000 Server, iSTAR Door	Access granted, CCure Journal event, My...
☑	Card Rejected	CCure9000 Server, iSTAR Door	
☑	CCure Door Forced	CCure9000 Server, iSTAR Door	
☑	CCure Door Held	CCure9000 Server, iSTAR Door	
☑	CCure Server Offline	CCure9000 Server	
☑	CCure Server Online	CCure9000 Server	
☑	Device Activity	CCure9000 Server, iSTAR Controller, iSTAR...	
☑	Device Error	CCure9000 Server, iSTAR Controller, iSTAR...	
☑	Device Error Journal Trigger Event	CCure9000 Server	
☑	Double swipe	CCure9000 Server, iSTAR Door	
☑	Email sent failure	CCure9000 Server	
☑	Email sent failure with issuer	CCure9000 Server	
☑	Event Assess Message	CCure9000 Server	
☑	Firmware Flash Activity	CCure9000 Server	
☑	General Messages Logged	CCure9000 Server	
☑	General Purpose Interface Activity	CCure9000 Server	CCure Journal event
☑	Guard Tour Activity	CCure9000 Server	CCure Journal event
☑	High Assurance Reader Activity	CCure9000 Server	CCure Journal event
☑	Incident Activity	CCure9000 Server	CCure Journal event
☑	Intrusion Zone Activity	CCure9000 Server	CCure Journal event
☑	Intrusion Zone Error	CCure9000 Server	CCure Journal event

- ▣ All categories
- ☐ Access denied
- ☑ Access granted
- ☐ Access request
- ☐ Alarm
- ☐ CCure Event Activated
- ☑ CCure Journal event
- ☐ Error
- ☑ My Custom Event Category
- ☐ Warning

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

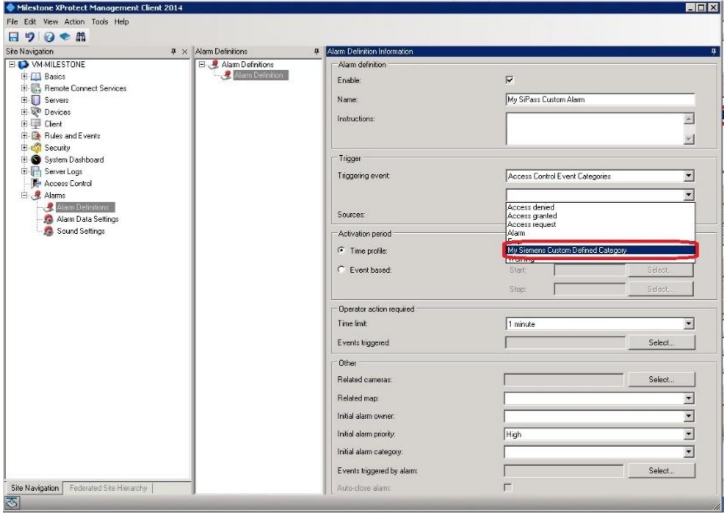


Name the alarm a pertinent name and select Access Control Event Categories in the Triggering event dropdown:



Enable: ☑
Name: My SiPass Custom Alarm
Time profile: Always
Time limit: 1 minute
Initial alarm priority: High

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



Alarm definition

Enable: ☑

Name: My SiPass Custom Alarm

Instructions:

Trigger

Triggering event: Access Control Event Categories

Access denied
Access granted
Access request
Alarm
My Siemens Custom Defined Category

Sources:

Activation period

● Time profile:

○ Event based: Start: Stop:

Operator action required

Time limit: 1 minute

Events triggered:

Other

Related cameras:

Related map:

Initial alarm owner:

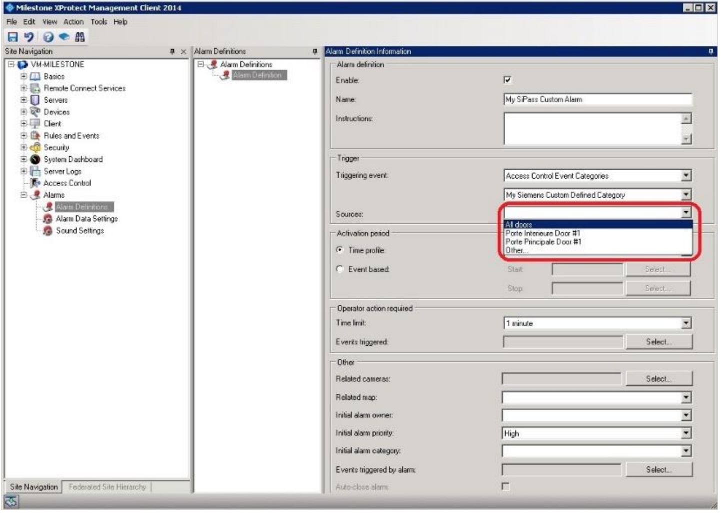
Initial alarm priority: High

Initial alarm category:

Events triggered by alarm:

Auto-close alarm: □

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



Alarm definition

Enable: ☑

Name: My SiPass Custom Alarm

Instructions:

Trigger

Triggering event: Access Control Event Categories

My Siemens Custom Defined Category

Sources:

All doors
Porte Interieure Door #1
Porte Principale Door #1
Other...

Activation period

● Time profile:

○ Event based: Start: Stop:

Operator action required

Time limit: 1 minute

Events triggered:

Other

Related cameras:

Related map:

Initial alarm owner:

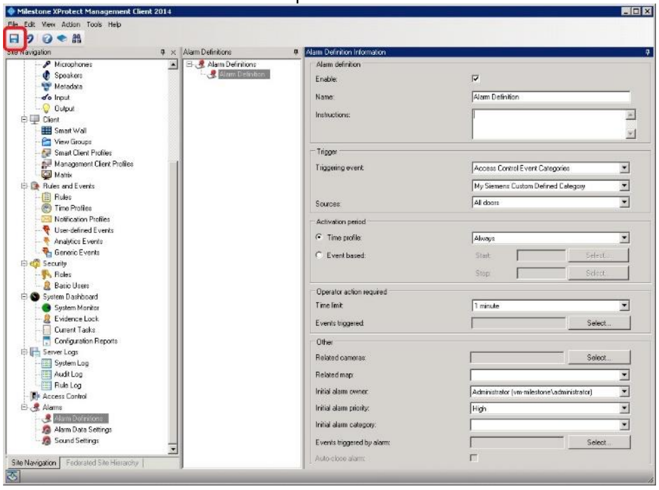
Initial alarm priority: High

Initial alarm category:

Events triggered by alarm:

Auto-close alarm: □

Select all the other alarm parameters and save:



Alarm definition

Enable: ☑

Name: Alarm Definition

Instructions:

Trigger

Triggering event: Access Control Event Categories

My Siemens Custom Defined Category

Sources: All doors

Activation period

● Time profile: Always

○ Event based: Start: Stop:

Operator action required

Time limit: 1 minute

Events triggered:

Other

Related cameras:

Related map:

Initial alarm owner: Administrator (vm-milestone\administrator)

Initial alarm priority: High

Initial alarm category:

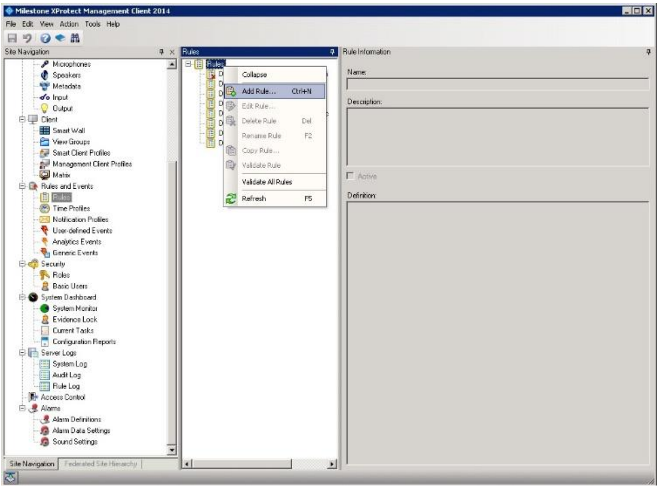
Events triggered by alarm:

Auto-close alarm: □

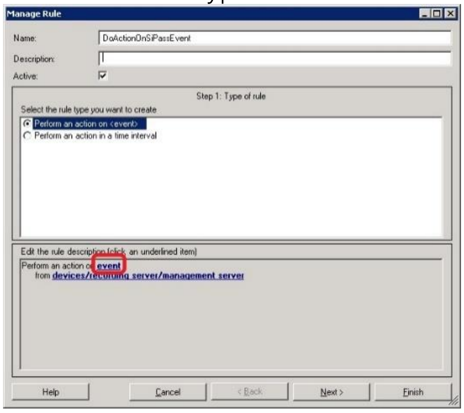
Alarms acknowledged in Milestone are acknowledged in CCure 9000.

Defining rules based on CCure 9000 events

To define rules in Milestone based on CCure 9000 events, create a rule in the Rules tab:



Select the event hyperlink:



Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 1: Type of rule

Select the rule type you want to create

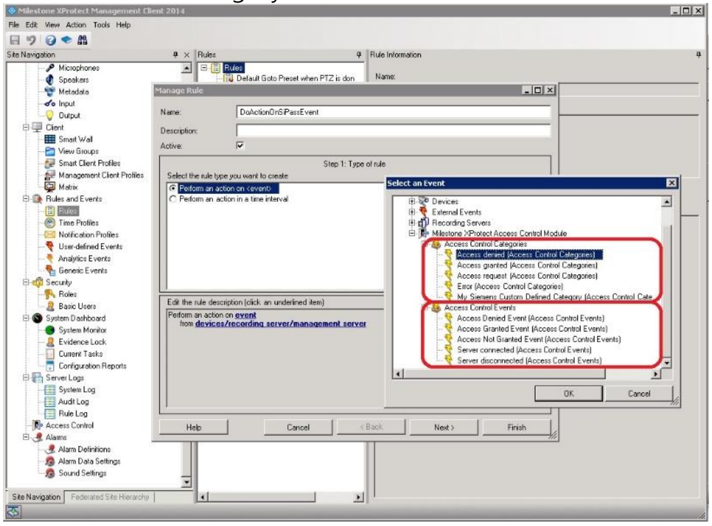
● Perform an action on <event>

○ Perform an action in a time interval

Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

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



Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 1: Type of rule

Select the rule type you want to create

● Perform an action on <event>

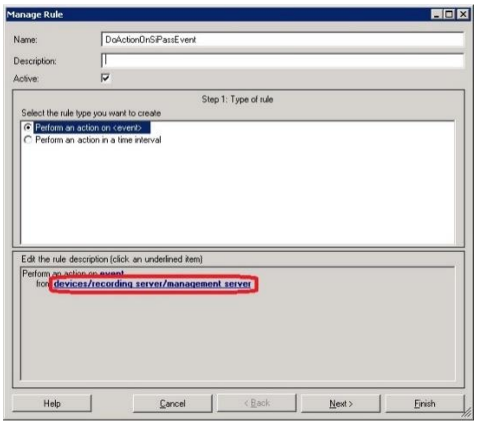
○ Perform an action in a time interval

Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server

Devices
External Events
Recording Servers
Milestone XProtect Access Control Module
Access Control Categories
Access denied (Access Control Categories)
Access granted (Access Control Categories)
Access request (Access Control Categories)
Error (Access Control Categories)
My Siemens Custom Defined Category (Access Control Cate
Access Control Events
Access Denied Event (Access Control Events)
Access Granted Event (Access Control Events)
Access Not Granted Event (Access Control Events)
Server connected (Access Control Events)
Server disconnected (Access Control Events)

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


Manage Rule

Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 1: Type of rule

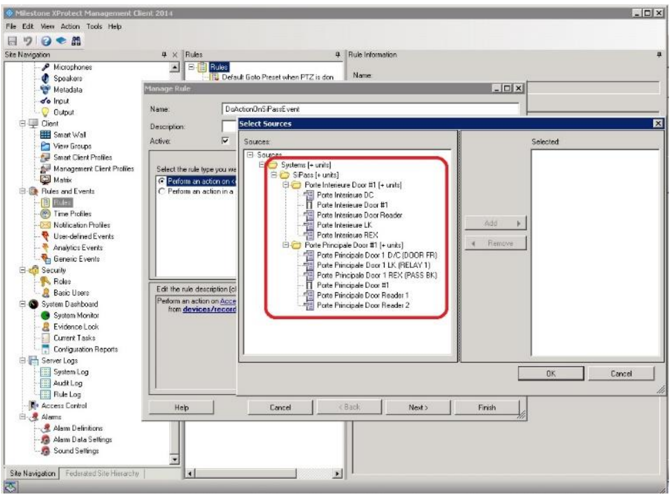
Select the rule type you want to create

● Perform an action on <event>

○ Perform an action in a time interval

Edit the rule description (click an underlined item)

Perform an action on event
from devices/recording server/management server


Milestone XProtect Management Client 2014

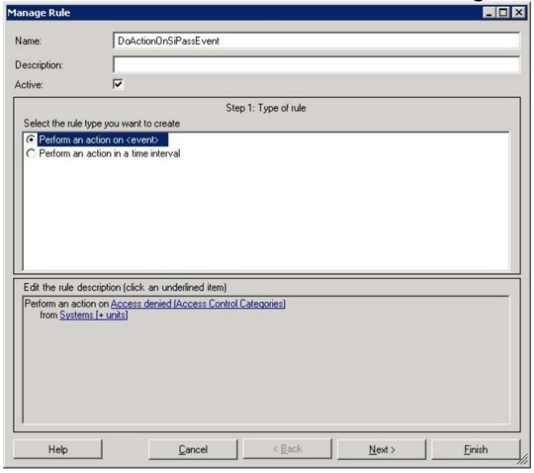
Select Sources

Sources:

- Sources
  - Systems [+ units]
    - SiPass [+ units]
      - Porte Interieure Door #1 [+ units]
        - Porte Interieure DC
        - Porte Interieure Door #1
        - Porte Interieure Door Reader
        - Porte Interieure LK
        - Porte Interieure REX
      - Porte Principale Door #1 [+ units]
        - Porte Principale Door 1 D/C (DOOR FR)
        - Porte Principale Door 1 LK (RELAY 1)
        - Porte Principale Door 1 REX (PASS BK)
        - Porte Principale Door #1
        - Porte Principale Door Reader 1
        - Porte Principale Door Reader 2

Selected:

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


Manage Rule

Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 1: Type of rule

Select the rule type you want to create

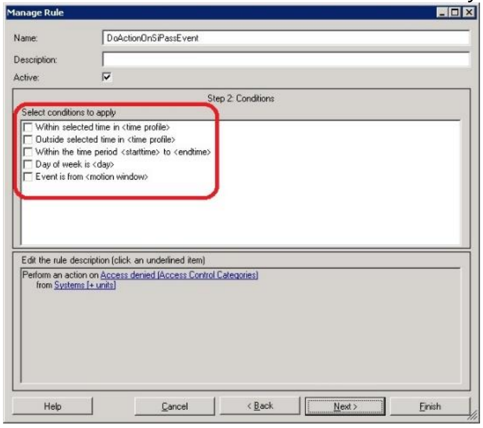
● Perform an action on <event>

○ Perform an action in a time interval

Edit the rule description (click an underlined item)

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

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


Manage Rule

Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 2: Conditions

Select conditions to apply

☐ Within selected time in <time profile>

☐ Outside selected time in <time profile>

☐ Within the time period <starttime> to <endtime>

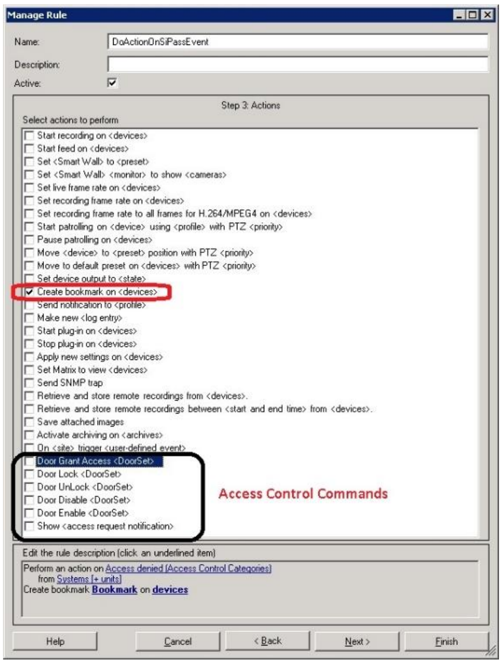
☐ Day of week is <day>

☐ Event is from <motion window>

Edit the rule description (click an underlined item)

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

Select the action that will be executed when the CCure 9000 event occurs. Notice that AC commands can be used as actions based on any events that come into Milestone:



Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 3: Actions

Select actions to perform

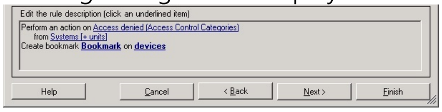
- ☐ Start recording on <devices>
- ☐ Start feed on <devices>
- ☐ Set <Smart Wall> to <preset>
- ☐ Set <Smart Wall> <monitor> to show <cameras>
- ☐ Set live frame rate on <devices>
- ☐ Set recording frame rate on <devices>
- ☐ Set recording frame rate to all frames for H.264/MPEG4 on <devices>
- ☐ Start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

Access Control Commands

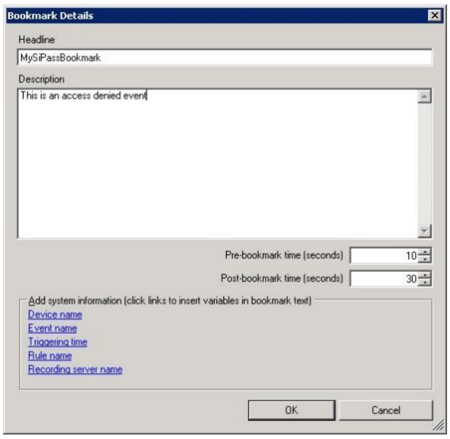
Edit the rule description (click an underlined item)

Perform an action on Access denied (Access Control Categories)
from Systems [+ units]
Create bookmark **Bookmark** on **devices**

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)

Perform an action on Access denied (Access Control Categories)
from Systems [+ units]
Create bookmark **Bookmark** on **devices**



Headline: MySiPassBookmark

Description: This is an access denied event

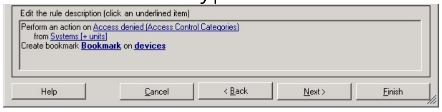
Pre-bookmark time (seconds): 10

Post-bookmark time (seconds): 30

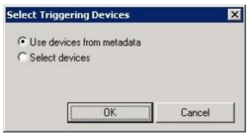
Add system information (click links to insert variables in bookmark text)

Device name
Event name
Triggering time
Rule name
Recording server name

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

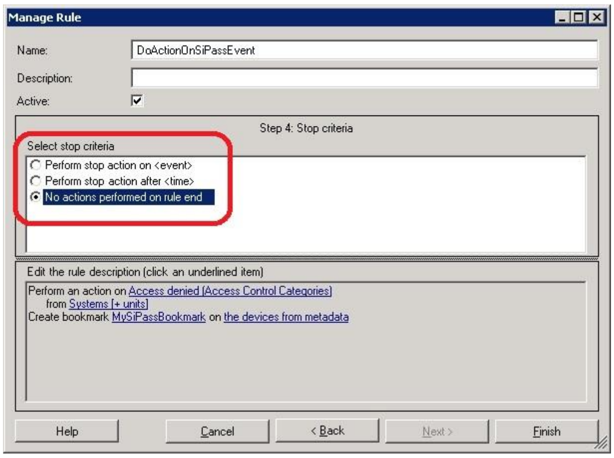

Edit the rule description (click an underlined item)

Perform an action on Access denied (Access Control Categories)
from Systems [+ units]
Create bookmark **Bookmark** on **devices**



● Use devices from metadata
○ Select devices

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



Manage Rule

Name: DoActionOnSiPassEvent

Description:

Active: ☑

Step 4: Stop criteria

Select stop criteria

○ Perform stop action on <event>
○ Perform stop action after <time>
● No actions performed on rule end

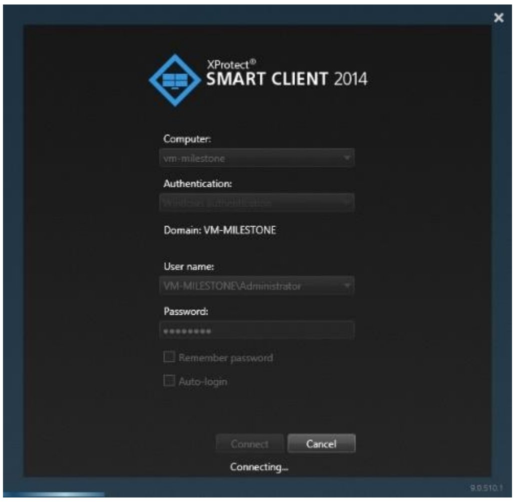
Edit the rule description (click an underlined item)

Perform an action on Access denied [Access Control Categories]
from Systems [+ units]
Create bookmark MySiPassBookmark on the devices from metadata

Click finish and the rule is set.

XProtect® Smart Client Maps

It is possible to put doors and CCure 9000 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:



Computer: vm-milestone

Authentication: Windows authentication

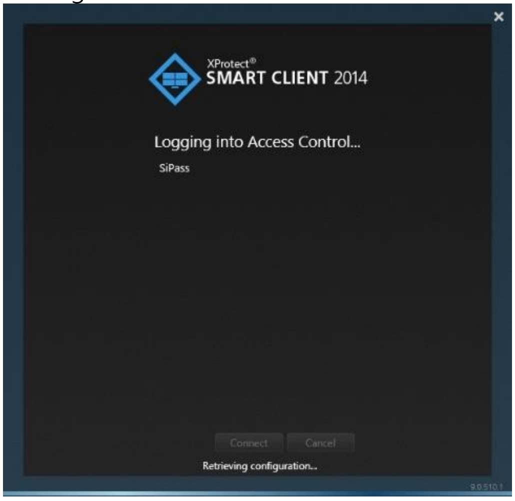
Domain: VM-MILESTONE

User name: VM-MILESTONE\Administrator

Password: ••••••••

□ Remember password
□ Auto-login

Connecting...

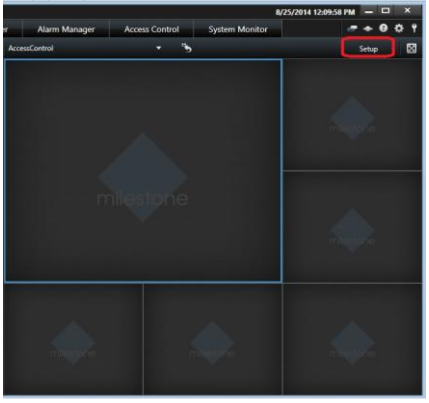


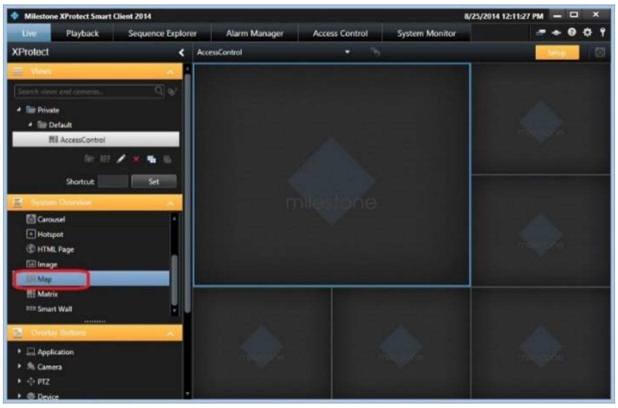
Logging into Access Control...

SiPass

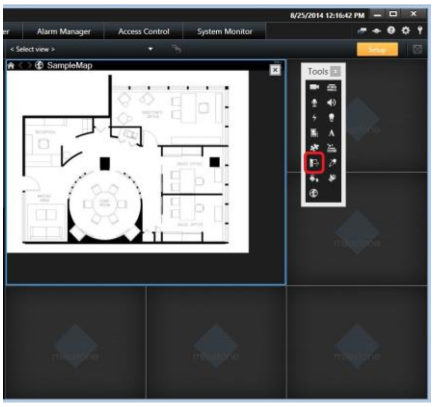
Retrieving configuration...

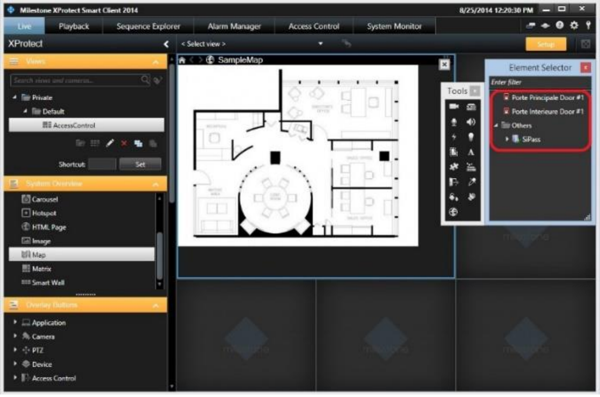
Use an existing view, go into setup mode by pressing the setup button in red below and create a map by dragging it onto a tile once in setup mode.



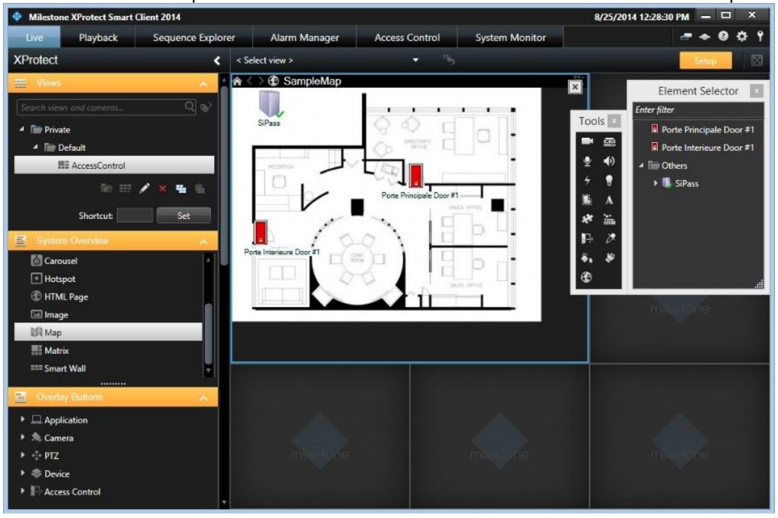


Select the access control button on the map overview and drag doors from the Element Selector to the map



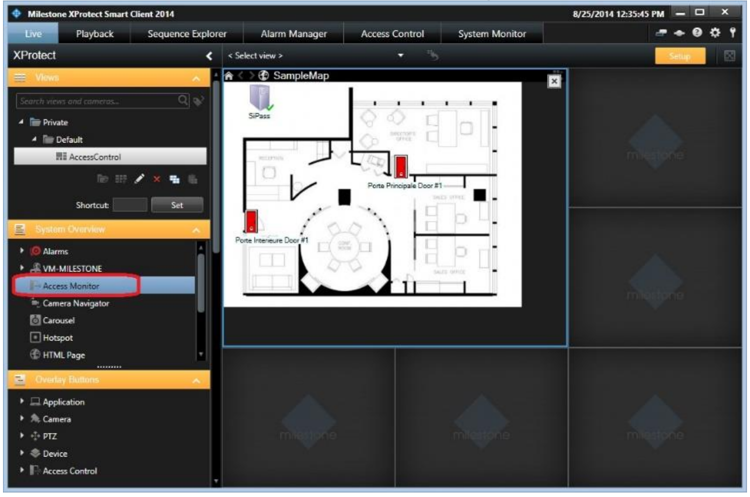


The finalized map with the doors and server added in this example will look like this:

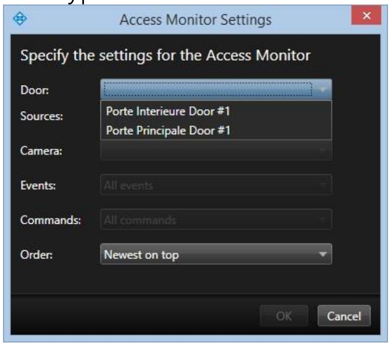


XProtect® Access Monitor tiles

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:


Access Monitor Settings

Specify the settings for the Access Monitor

Door:

Sources:

Porte Interieure Door #1

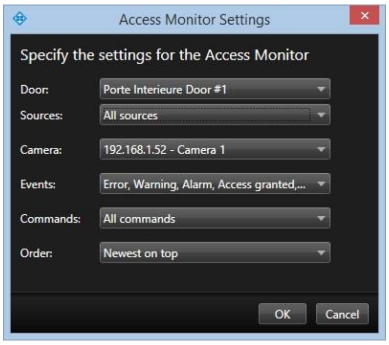
Porte Principale Door #1

Camera:

Events: All events

Commands: All commands

Order: Newest on top


Access Monitor Settings

Specify the settings for the Access Monitor

Door: Porte Interieure Door #1

Sources: All sources

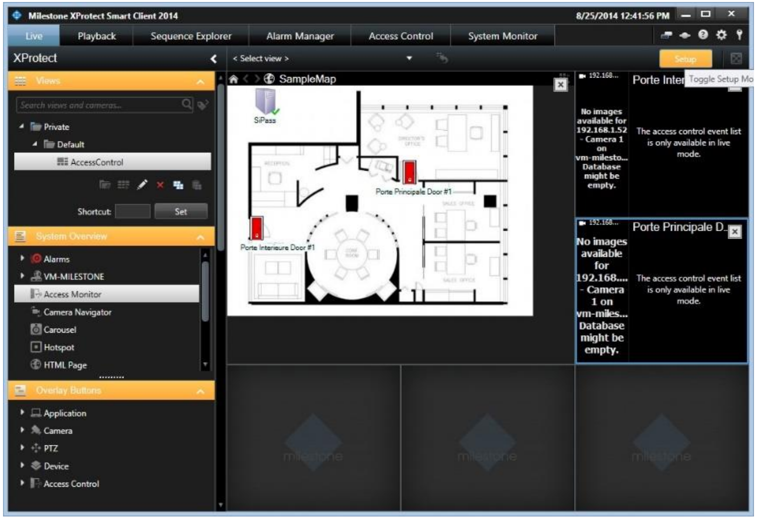
Camera: 192.168.1.52 - Camera 1

Events: Error, Warning, Alarm, Access granted,...

Commands: All commands

Order: Newest on top

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



No images available for 192.168.1.52 - Camera 1 on vm-milesto... Database might be empty.

The access control event list is only available in live mode.

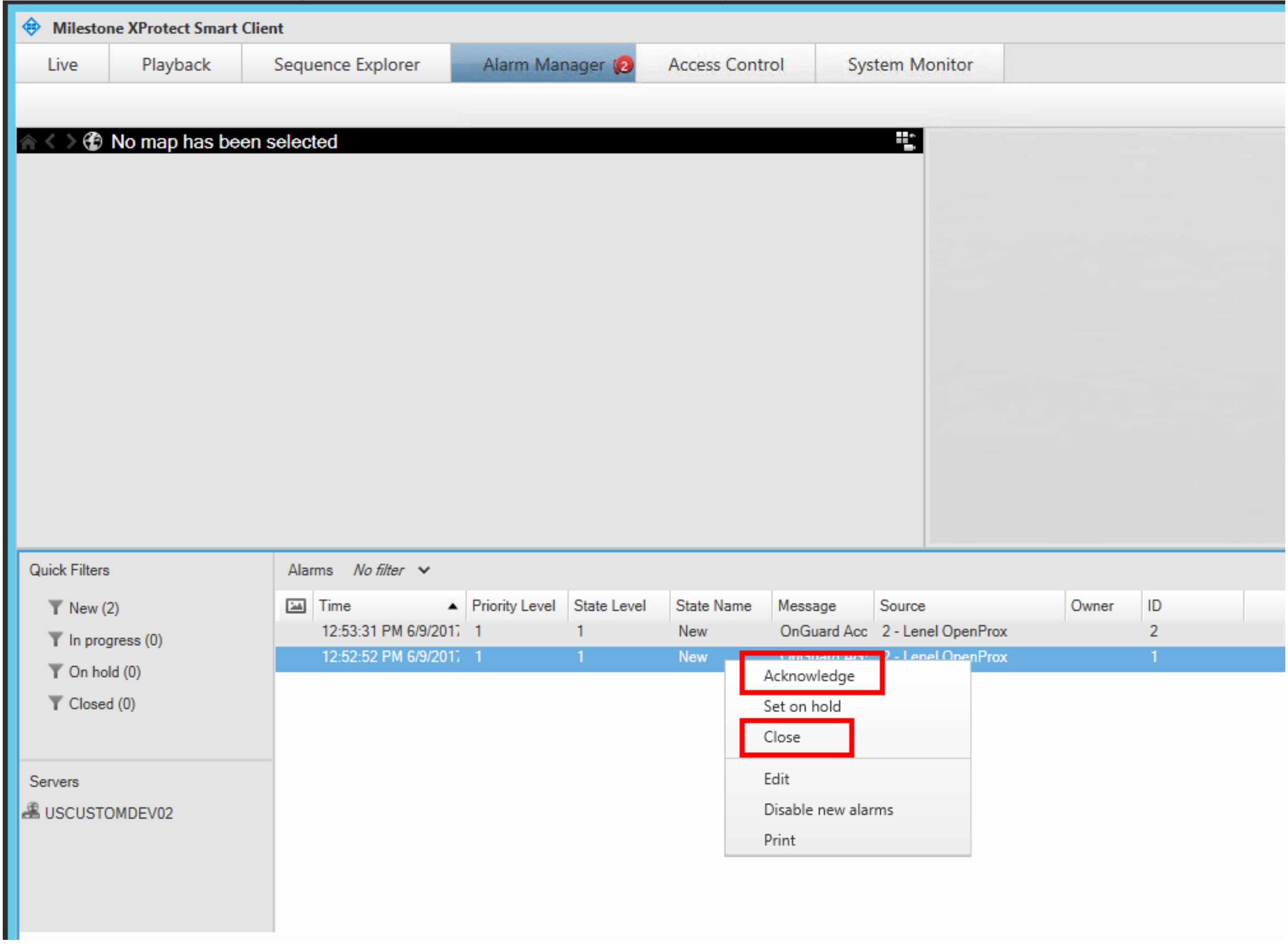
No images available for 192.168.... - Camera 1 on vm-miles... Database might be empty.

The access control event list is only available in live mode.

Alarm Acknowledgment

Alarm acknowledgment from XProtect to CCure 9000 is implemented. In XProtect versions earlier than 2016 R3, you can still perform alarm acknowledgment in XProtect, but it will not be propagated to CCure 9000. Alarm acknowledgment from CCure 9000 to XProtect is not implemented due to the lack of such functionality in CCure 9000.

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 CCure 9000.



Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
12:53:31 PM 6/9/201	1	1	New	OnGuard Acc	2 - Lenel OpenProx		2
12:52:52 PM 6/9/201	1	1	New	[illegible]	2 - Lenel OpenProx		1

NOTE – As mentioned above, selecting either Acknowledge or Close will cause the alarm to be acknowledged in CCure 9000 and removed from CCure 9000'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 CCure 9000. The reason is simple – the alarm was removed from CCure 9000'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.

Logging

By default the debug logs are enabled on both the Milestone event server plugin and the CCure 9000 server but they are at a reduced log level (Info). They can be increased for diagnostics purposes to Debug (or even Trace) but be aware that this change causes more information to be logged using more disk space and possibly slowing down operations on busy servers. DO NOT LEAVE logging at Debug levels for extended periods of time for performance reasons. It should only be used for diagnostics purposes and put back to Info afterwards.

Gathering the logs

Milestone Event Server side

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

CCure 9000 Server side

5. On the machine running the CCure 9000 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 CCure 9000 server go to X:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\logs, where X: is the drive where windows is installed
8. Create a zip file of the contents of that whole folder and name it MilestoneACMServerServiceLogs.zip
9. On the machine running the CCure 9000 server go to: X:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\CCure9kAcmServerPlugin\logs
10. Create a zip file of the contents of that whole folder and name it CCure9000AcmServerPluginLogs.zip

Changing logging level

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

Milestone Event Server side

1. On the machine running the Milestone Event Server go to x:\ProgramData\VideoOS\ACMServerPlugin, where X: is the drive where Windows is installed
2. There should be subfolders that use a unique identifier (GUID) something like "4c53f6e5-e951-1616-83f0-e44fb813e451". For each of these folders do the following:

a. Find a file named “ACMServerPluginNLog.xml”, open it with a text editor like notepad
b. The second to last line in the file is like this “<logger name="*" minlevel="Info" writeTo="mainlog" />”
c. Change the “Info” to “Debug” or “Trace” in that line and save the file.
d. Depending on the OS you are running you may have to save the file to the desktop and copy it back to that folder because windows permissions will not let you save a file there directly.

CCure 9000 Server side

1. On the CCure 9000 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=" CCure9kAcmServerPlugin.*"", and “<logger name=" Milestone.CCure9k.Client.*"”.
   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 CCure 9000 server machine go to x:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService. X: would be the drive where windows is installed.
   a. Find a file named “VideoOSACMServerNLog.xml”, open it with a text editor like notepad
   b. The second to last line in the file is like this “<logger name="*" minlevel="Info" writeTo="mainlog" />”
   c. Change the “Info” to “Debug” or “Trace” in that line and save the file.

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

Troubleshooting Guide

Symptom: CCure 9000 loses communication with the access control hardware

Communication can be lost for the following reasons:

1) Firewall blocking the traffic

Symptom: XProtect® Smart Client shows a System Error event with StateCode: LicensedQuantityReached when sending commands to CCure 9000

Make sure you only connect to the CCure 9000 server with one ACM server. Connecting with multiple ACM servers is not supported.

Symptom: 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.

Symptom: CCure 9000 ACM instance is not displayed in the XProtect® Management Client

If XProtect is unable to communicate with the CCure 9000ACM 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 CCure 9000 is running successfully. This may require restarting services.
- Start the Milestone ACM Service
- Start the Milestone Event Server, and wait for it to come to ready
- Start the Management Client

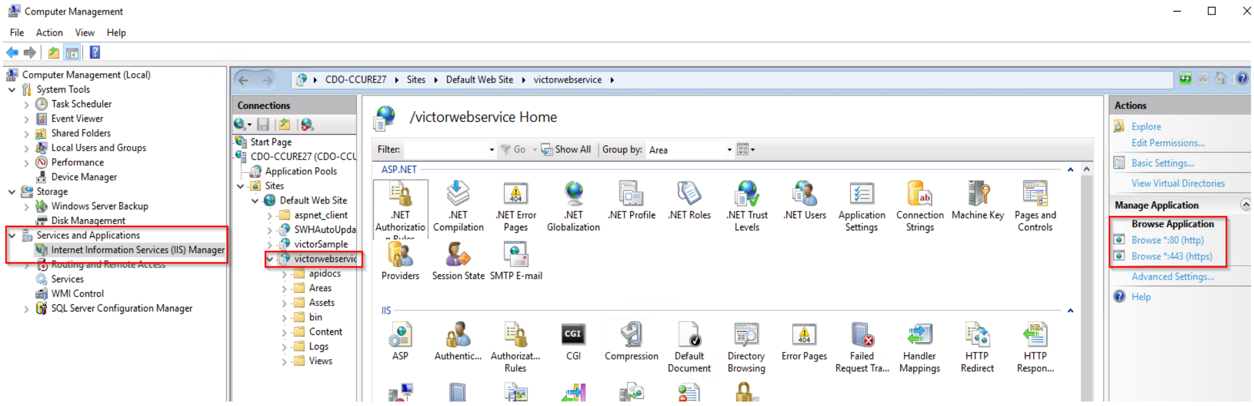
Symptom: CCure 9000 ACM looking for secured connection with XProtect®

Check the SSL configuration for the CCure 9000 plugin:
A certificate must be provided and configured in IIS for the CCure 9000 Victor web service to accept secure HTTPS connection on port 443. From the CCure Server open a browser window. Cut and Paste this URL to review IIS and SSL encryption:

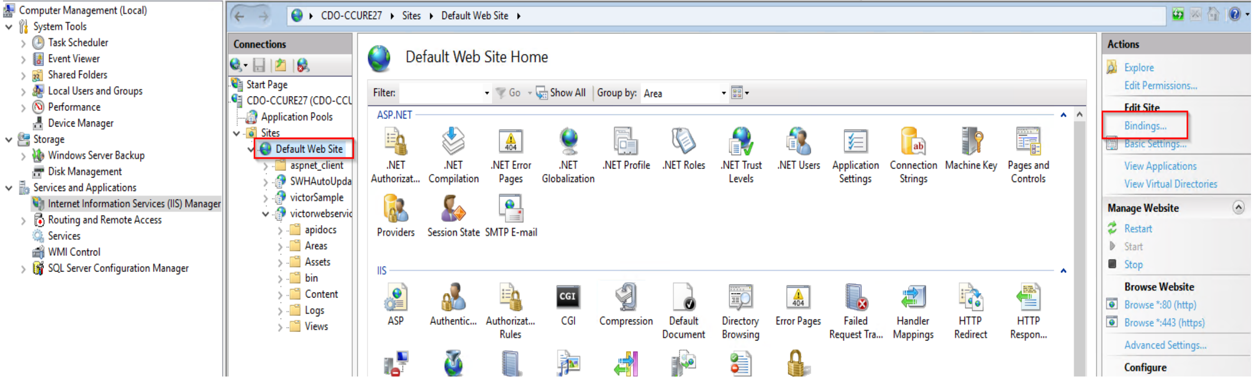
https://www.swhouse.com/products/CCURE_9000.aspx
Look under "Manuals"

To check if the Port number needs to be setup for HTTPS on the XProtect Server:

Go to Start, Windows Administrative Tools, Computer Management.
In Computer Management, Select Services and Applications, Internal Information Services (IIS) Manager.
Click on Browse *.443 to validate if HTTPS is working. It will try to login with TLS onto a secure website. If it's blocked then that port is not setup.

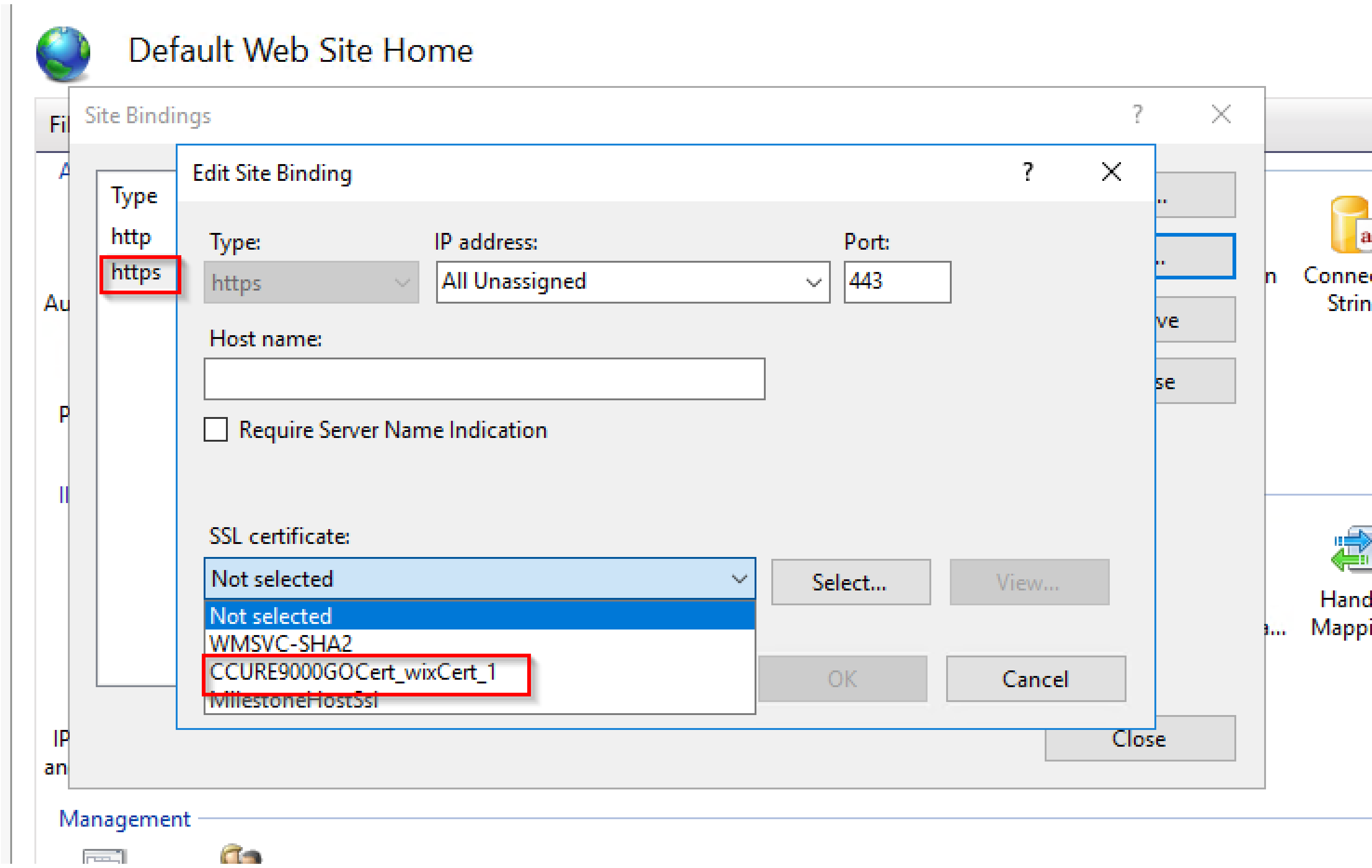


To setup HTTPS on Port 443, Go to “Default Web Site” and click on” Bindings”….



Then click on Type HTTPS and Edit.

Click on SSL certificate and Select it the appropriate certificate. The certificate allows access to Secured ports.



Type: https

IP address: All Unassigned

Port: 443

Host name:

☐ Require Server Name Indication

SSL certificate: Not selected

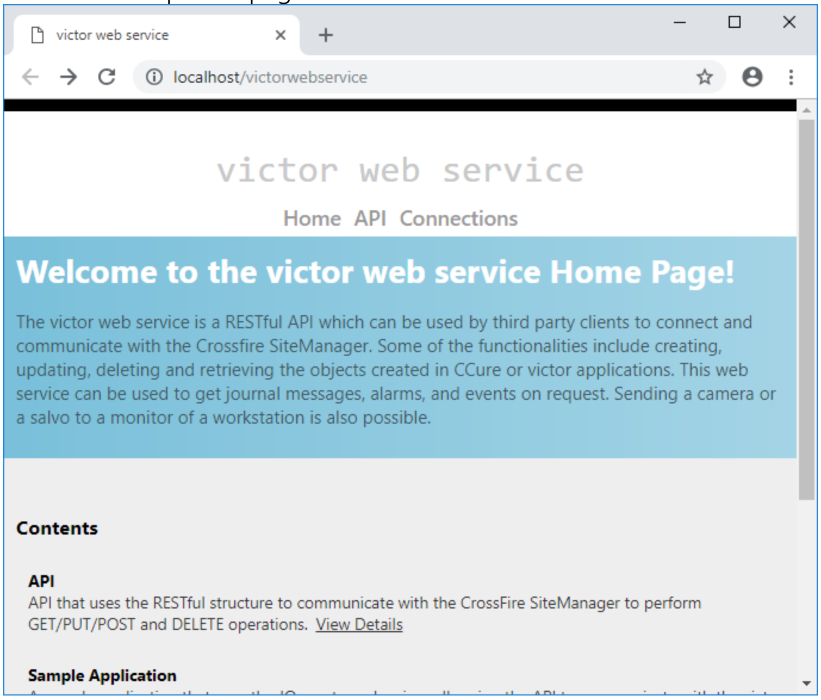
Not selected
WMSVC-SHA2
CCURE9000GOCert_wixCert_1
MilestoneHostSsl

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

Symptom: CCure 9000 ACM instance cannot communicate with CCure 9000

If XProtect is unable to authenticate or communicate with CCure 9000, there might be a problem with the CCure 9000 victor web service application pool. Do the following steps to make sure the CCure 9000 victor web service is correctly started and accepts requests.

- On the CCure 9000 machine, open a web browser and go the address below: http://localhost/victorwebservice/
- Make sure it opens a page similar to the one below:



Welcome to the victor web service Home Page!

The victor web service is a RESTful API which can be used by third party clients to connect and communicate with the Crossfire SiteManager. Some of the functionalities include creating, updating, deleting and retrieving the objects created in CCure or victor applications. This web service can be used to get journal messages, alarms, and events on request. Sending a camera or a salvo to a monitor of a workstation is also possible.

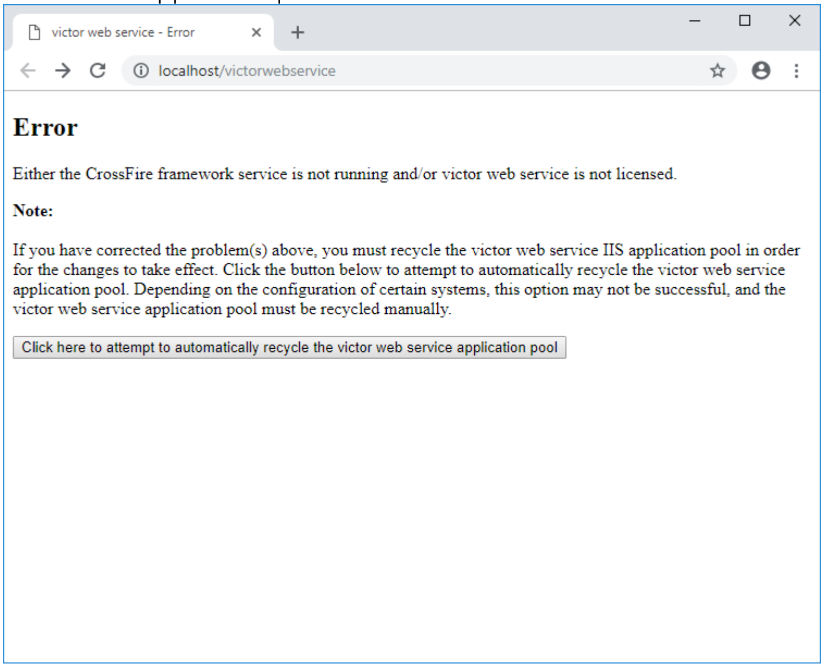
Contents

API

API that uses the RESTful structure to communicate with the CrossFire SiteManager to perform GET/PUT/POST and DELETE operations. View Details

Sample Application

- If an Error page similar to the one below is displayed instead, click the button to recycle the victor web service application pool.



Error

Either the CrossFire framework service is not running and/or victor web service is not licensed.

Note:

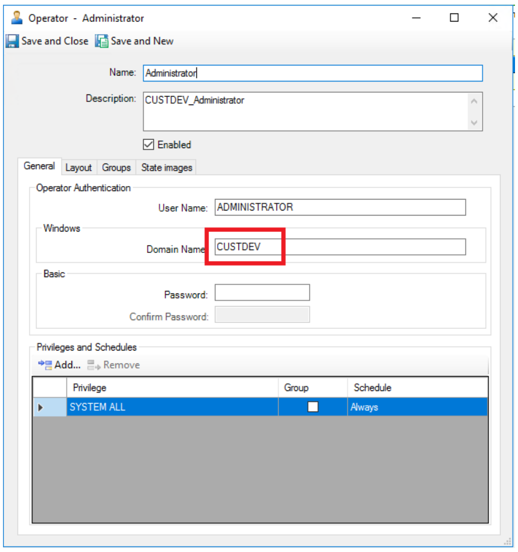
If you have corrected the problem(s) above, you must recycle the victor web service IIS application pool in order for the changes to take effect. Click the button below to attempt to automatically recycle the victor web service application pool. Depending on the configuration of certain systems, this option may not be successful, and the victor web service application pool must be recycled manually.

Click here to attempt to automatically recycle the victor web service application pool

Symptom: Login fails with CCure 9000 when using a multi-parts domain user

It appears that the default Operator created when installing CCure 9000 will only retain the first part of a multi-parts domain name.

For example, if CCure 9000 is installed using the Administrator user on the *CUSTDEV.US* domain, only the *CUSTDEV* part will be kept in the Operator definition (the *.US* part will be lost). Trying to login using the full domain name won't work (as shown in the images below). The same domain name must be used in both places for login to succeed (including or excluding the multiple parts of the domain).



Operator - Administrator

Save and Close | Save and New

Name: Administrator

Description: CUSTDEV_Administrator

☑ Enabled

General | Layout | Groups | State images

Operator Authentication

User Name: ADMINISTRATOR

Windows

Domain Name: CUSTDEV

Basic

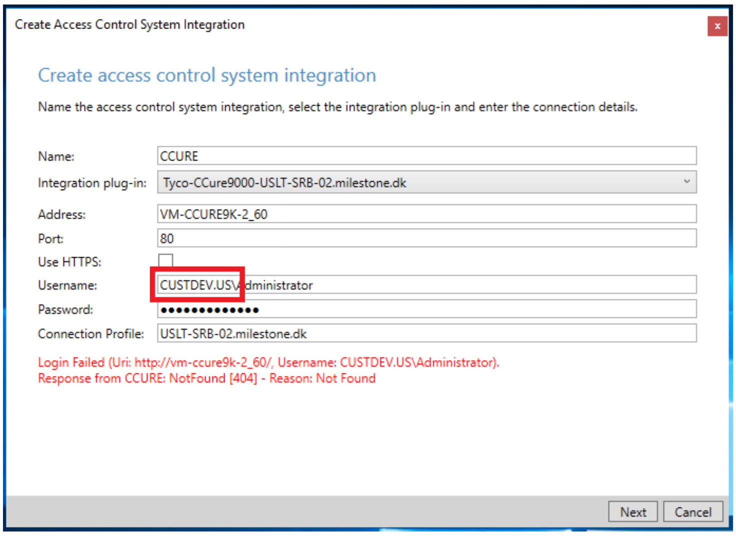
Password:

Confirm Password:

Privileges and Schedules

Add... Remove

Privilege	Group	Schedule
SYSTEM ALL	□	Always



Create Access Control System Integration

Create access control system integration

Name the access control system integration, select the integration plug-in and enter the connection details.

Name: CCURE

Integration plug-in: Tyco-CCure9000-USLT-SRB-02.milestone.dk

Address: VM-CCURE9K-2_60

Port: 80

Use HTTPS: □

Username: CUSTDEV.US\Administrator

Password: •••••••••••••

Connection Profile: USLT-SRB-02.milestone.dk

Login Failed (Uri: http://vm-ccure9k-2_60/, Username: CUSTDEV.US\Administrator).
Response from CCURE: NotFound [404] - Reason: Not Found

All other support issues

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

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.