MAKE THE
WORLD SEE

April 21

Milestone Systems

CCure 9000 XProtect Access

User Guide

milestone

Contents

Copyright, Trademarks & Disclaimers

Trademarks

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.

Version Compatibility

Integration with CCure 9000 Access Control system is supported with all XProtect VMS products which can support MIP integrations and with a rules system that supports the XPA suite of functionality. XProtect products which are tested and supported include the following releases of XProtect Professional+, Expert and Corporate.

CCure 9000	XProtect 2018			XProtect 2019			XProtect 2020		
	R1	R2	R3	R1	R2	R3	R1	R2	R3
2.70	S	S	S	T	T	S	S	S	T
2.80	S	S	S	T	T	T	T	S	S
2.90	S	S	S	S	S	T	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 Free Editions Essential+ are NOT supported.

⚠ 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 Versions:

All updates and patches for CCure 9000 access control systems should not impact compatibility with the XProtect Access integration. If a minimum update or patch is documented, it will be listed here. If no minimum update or patch is listed, then all available updates and patches should be assumed to be compatible.

Version	Minimum update / patch level	Version Information
2.70	SP3_CU01	The Personalized Login feature will only work if CCure 9000 with SP3 CU1 or higher is installed.
2.80	-	-
2.90	-	-

Hardware Support

The following CCure 9000 panels have been tested and are known to be supported.

Panel Model	Description
USTAR008	iStar Ultra

⚠ 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

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 XPA integration should support any number of cardholders. However, XProtect Access has officially supported limitations for many system parameters.   You can find those "limitations" listed in the most recent version of the XProtect Access Specification Sheet.

Events Handled

Preliminary tests show a sustained rate of about 40 events per second.

General Description

Introduction

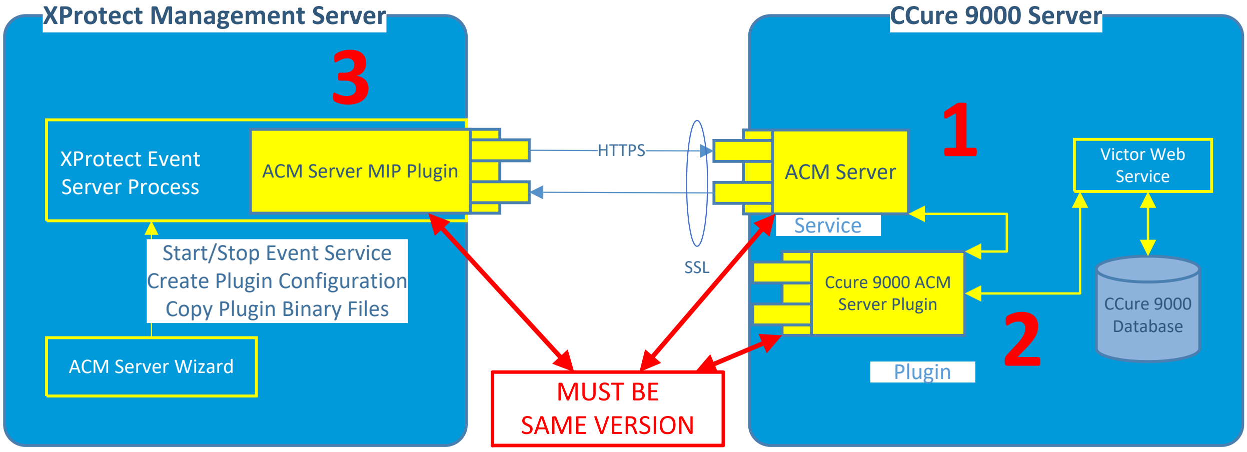
This document describes specifics to the XProtect Access (XPA) integration between Milestone XProtect and the CCure 9000 access control (AC) system. This integration supports the following standard XProtect Access (XPA) features:

- Retrieve and refresh configuration from the CCure 9000 AC system, e.g. doors and event types
- Receive AC event streams and hardware state changes from the CCure 9000 system
- Display and search cardholder information and images
- 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.
- Association of access control hardware to cameras for simultaneous display of doors and video.
- Select and categorize the events the user wants to view from the CCure 9000 system
- Trigger system actions based on AC hardware events. For example: start recording, go to PTZ preset, display access request…etc., triggered by door forced, access granted, access denied…etc.
- Personalized login to support segmented database systems.
- AC hardware status display and command interaction on VMS client map user interface.
- Create customized access reports based on search queries in XProtect Smart Client.
- Smart Client pop-up access request notifications.
- AC hardware interaction via XProtect web and mobile clients.

Solution overview

The solution provided is split in 3 components:

1. The “ACM Server” that runs on the CCure 9000 server (Milestone.ACMServer.x64.msi)
2. The ”CCure 9000 ACM Server Plugin” that runs on the CCure 9000 server (Milestone.ACMServer.CCure9k.msi)
3. The “ACM Server MIP Plugin” that runs in the XProtect Event Server (Milestone.ACMServer.MipPlugin.msi)

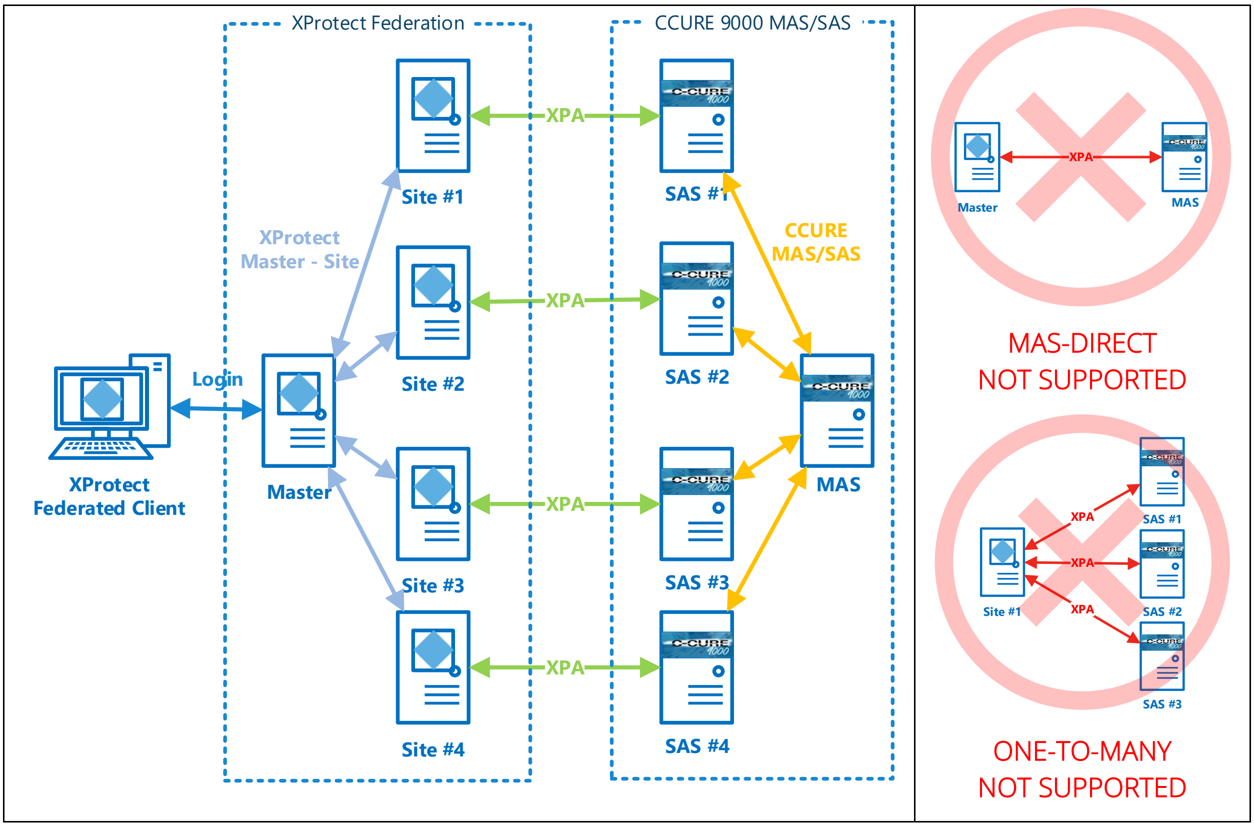


System Design

CCure 9000: Enterprise (MAS/SAS) Configuration

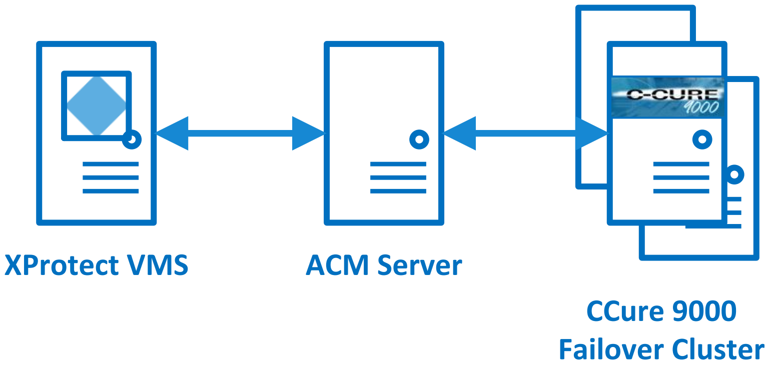
If the CCure 9000 system is part of an Enterprise deployment (MAS/SAS), the Enterprise system must be correctly configured and functioning before setting up the integration. Each CCure 9000 Satellite Application Server (SAS) of an Enterprise deployment must be independently connected through XProtect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

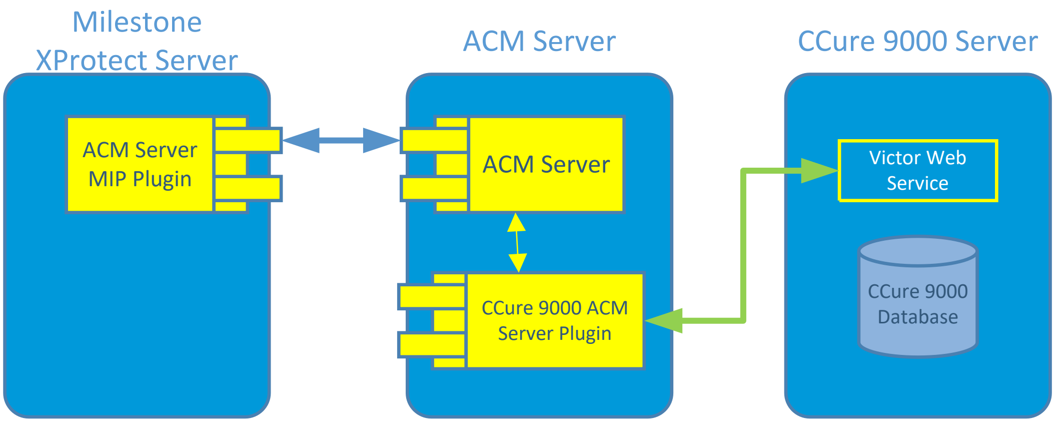


CCure 9000: Alternate Configuration

In some systems the CCure 9000 server cannot host additional software components. If the CCure 9000 software is being supported by a failover cluster, then the ACM server and the CCure 9000 ACM plugin will need to be installed on a different server.



In this scenario it is possible to configure the integrated system with a separate ACM server as the host for the ACM server and the CCure 9000 ACM Server Plugin.



Failover Clustering is not the only scenario that may require installing the ACM Server and CCure 9000 ACM plugin on a separate host machine. No matter the reason - redundancy, isolation of services, separation of maintenance responsibility...etc., this alternate configuration option is fully supported.

Prerequisites

Time Synchronization

All servers (i.e. the CCure 9000 and Milestone server operating systems) 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 https://connectedpartnerprogram.partnerproducts.com/ web site.

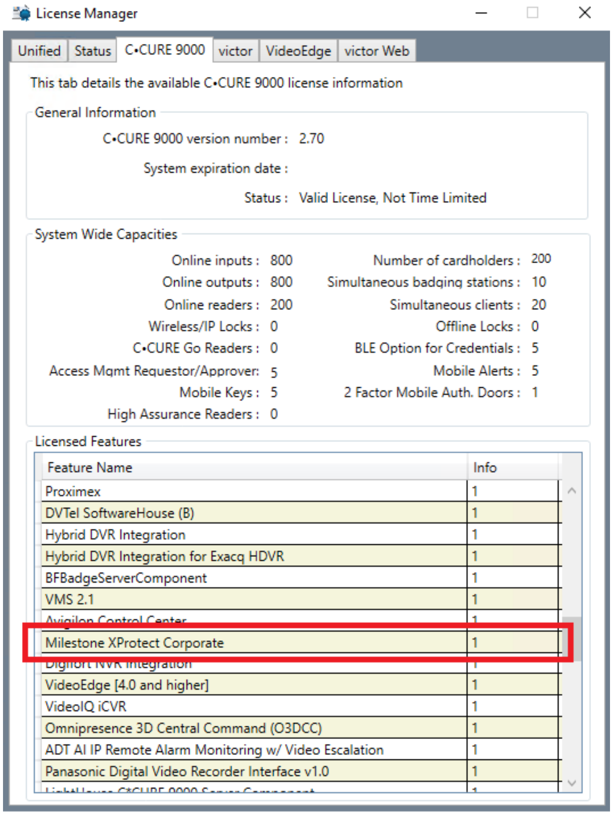
CCure 9000: Victor Web Service SSL Configuration

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 the “victor Web Service User Guide 2.90” for details.

CCure 9000: Licenses

Two features must be licensed in CCure for the integration to work:

1. “Milestone XProtect Corporate” – PLEASE READ THE WARNING NOTE BELOW
2. “victor web service”



This tab details the available C•CURE 9000 license information

General Information

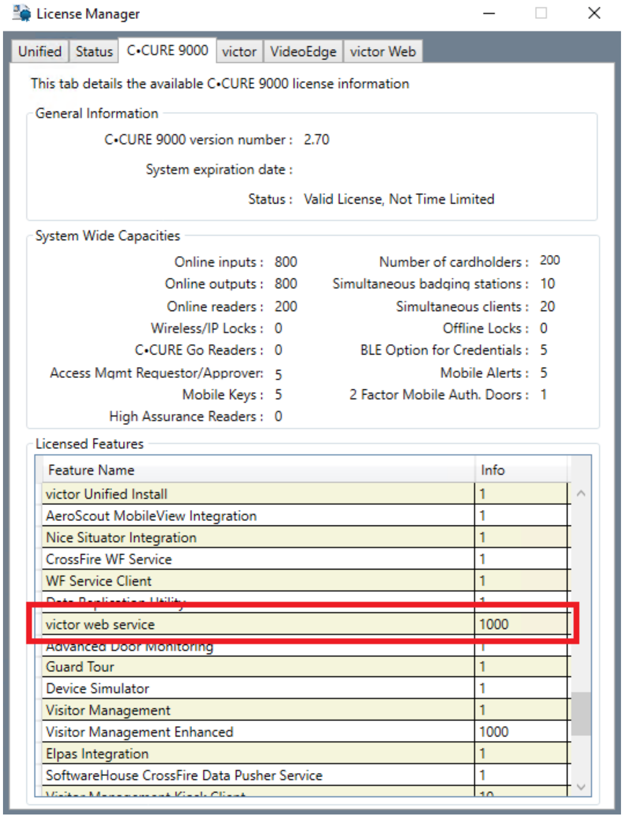
C•CURE 9000 version number : 2.70
System expiration date :
Status : Valid License, Not Time Limited

System Wide Capacities

Online inputs : 800
Online outputs : 800
Online readers : 200
Wireless/IP Locks : 0
C•CURE Go Readers : 0
Access Mgmt Requestor/Approver: 5
Mobile Keys : 5
High Assurance Readers : 0
Number of cardholders : 200
Simultaneous badging stations : 10
Simultaneous clients : 20
Offline Locks : 0
BLE Option for Credentials : 5
Mobile Alerts : 5
2 Factor Mobile Auth. Doors : 1

Licensed Features

Feature Name	Info
Proximex	1
DVTel SoftwareHouse (B)	1
Hybrid DVR Integration	1
Hybrid DVR Integration for Exacq HDVR	1
BFBadgeServerComponent	1
VMS 2.1	1
Avigilon Control Center	1
Milestone XProtect Corporate	1
Digifort NVR Integration	1
VideoEdge [4.0 and higher]	1
VideoIQ iCVR	1
Omnipresence 3D Central Command (O3DCC)	1
ADT AI IP Remote Alarm Monitoring w/ Video Escalation	1
Panasonic Digital Video Recorder Interface v1.0	1
LightHouse C*CURE 9000 Server Component	1



This tab details the available C•CURE 9000 license information

General Information

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

System Wide Capacities

Online inputs : 800
Online outputs : 800
Online readers : 200
Wireless/IP Locks : 0
C•CURE Go Readers : 0
Access Mgmt Requestor/Approver: 5
Mobile Keys : 5
High Assurance Readers : 0
Number of cardholders : 200
Simultaneous badging stations : 10
Simultaneous clients : 20
Offline Locks : 0
BLE Option for Credentials : 5
Mobile Alerts : 5
2 Factor Mobile Auth. Doors : 1

Licensed Features

Feature Name	Info
victor Unified Install	1
AeroScout MobileView Integration	1
Nice Situator Integration	1
CrossFire WF Service	1
WF Service Client	1
Data Replication Utility	1
victor web service	1000
Advanced Door Monitoring	1
Guard Tour	1
Device Simulator	1
Visitor Management	1
Visitor Management Enhanced	1000
Elpas Integration	1
SoftwareHouse CrossFire Data Pusher Service	1
Visitor Management Kiosk Client	10

The CCure 9000 license required to integrate with Milestone XProtect is named “Milestone XProtect Corporate.” This does not mean that the only XProtect product that integrates with CCure 9000 is Corporate. Corporate, Expert, and Professional+ VMS products from Milestone are all tested and supported. Only the name for the license from CCure is limited to “Milestone XProtect Corporate.”

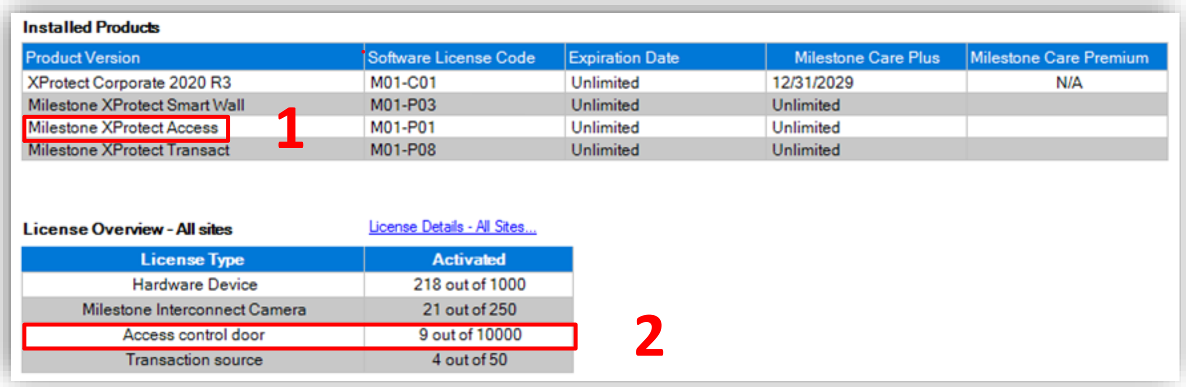
The ACM Server uses a permanent connection to CCure web service (to receive statuses and events) and uses multiple transient connections for specific user operations, such as fetching configuration and executing commands. For optimal operation of Milestone XProtect Access, the feature license activated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

.NET Framework: Installation on CCure 9000 Server machine

.NET Framework 4.7.2 must be installed on the CCure 9000 server machine (NDP472-KB4054530-x86-x64-AllOS-ENU.exe). Any version newer than Windows 10 April 2018 Update and Windows Server version 1803 includes this component. 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 2020 R3	M01-C01	Unlimited	12/31/2029	N/A
Milestone XProtect Smart Wall	M01-P03	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08	Unlimited	Unlimited	

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

License Type	Activated
Hardware Device	218 out of 1000
Milestone Interconnect Camera	21 out of 250
Access control door	9 out of 10000
Transaction source	4 out of 50

Milestone XProtect®: Event Server machine DNS / Name resolution

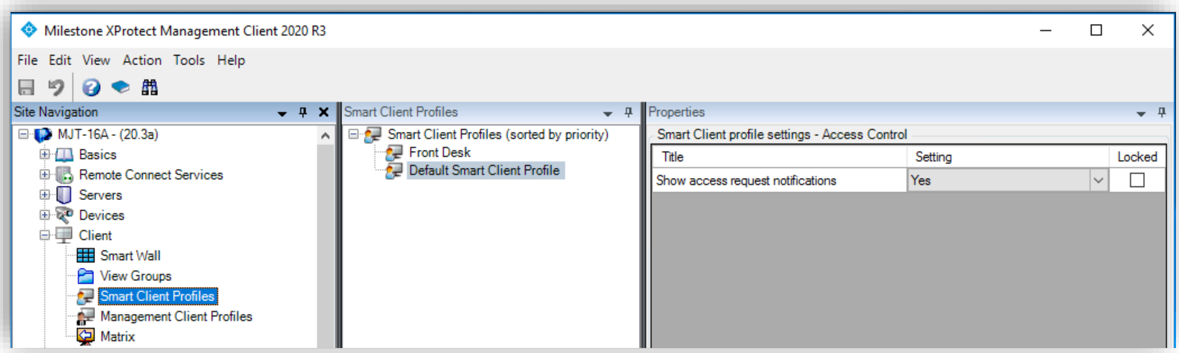
The Milestone XProtect Event Server must have network name resolution with the computer name of the CCure 9000 Server (e.g. DNS, manual host file entry, etc). The CCure 9000 Server machine must also resolve the Milestone server.

Milestone XProtect®: Smart Client Profiles

All Smart Client Profiles used in the system need to include:

- Access Control – Show access request notifications = Yes

“Yes” is the default configuration for all Smart Client Profiles. This configuration controls if users receive Access Control notifications with the Smart Client.



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

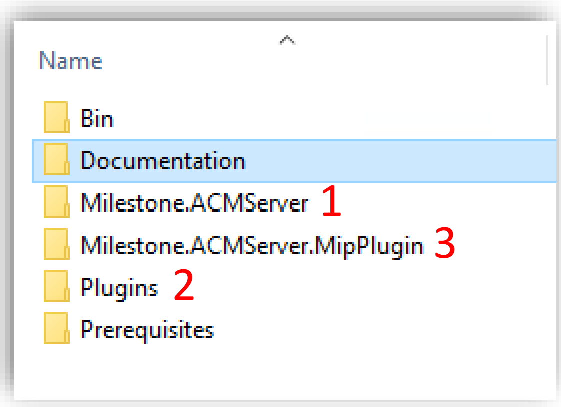
2. **Milestone.ACMServer.CCure9k.msi:** Installer for the CCure 9000 ACM Server plugin
   - Installed on the CCure 9000 server machine, after the ACM Server.
3. **Milestone.ACMServer.MipPlugin.msi:** Installer for the XProtect Event Server ACM MIP plugin
   - Installed on the XProtect Machine that hosts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

Download the most recent version **(v1.2)** of the CCure 9000 ACM integration from the following location:

http://Download.milestonesys.com/ccure9kacm/

Unzip the installation package. Identify the three required software components listed above and ensure that the .msi files for the ACM Server (1) and the CCure 9000 ACM Server plugin (2) are available on the CCure 9000 server host, and the .msi file for the XProtect Event Server ACM MIP plugin (3) is available on the XProtect Event Server host.

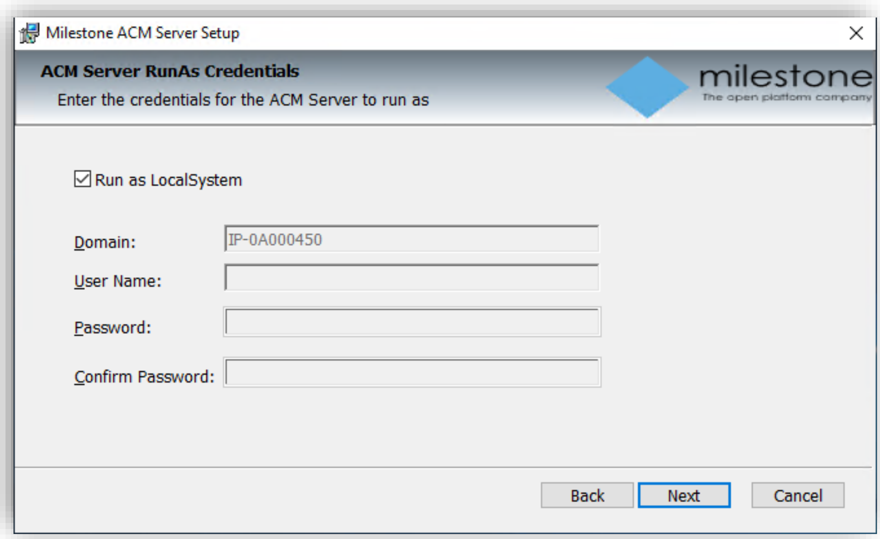


ACM Server Installation

Go to the CCure 9000 host machine, locate the required .msi file to start the installation wizard. The required file is named:

- Milestone.ACMServer.x64.msi

Double-click the installation file. Click "Next" to begin the wizard.



Milestone ACM Server Setup

ACM Server RunAs Credentials

Enter the credentials for the ACM Server to run as

☑ Run as LocalSystem

Domain: IP-0A000450

User Name:

Password:

Confirm Password:

At the ACM Server RunAs Credentials step, the default option of Run as LocalSystem can be used, or remove this option to enter a user name and password for the ACM Server. Click ”Next” to continue. Click ”Install” to install the ACM Server, or click ”Back” if you need to change the default installation directory. The default installation directory is:

- C:\Program Files\Milestone ACM Server\

Finish the ACM Server installation wizard.

ACM Server: CCure 9000 Plugin Installation

Go to the CCure 9000 host machine, locate the required .msi file to start the installation wizard. The required file is named:

- Milestone.ACMServer.CCure9k.msi

Double-click the installation file. Once the wizard detects the CCure 9000 server and the ACM Server it will continue. There are no configurable options in this installer. Click ”Install” to begin.

ACM Server: XProtect ACM MIP Plugin

In most scenarios, the XProtect Management Server host server is where this component is installed. However, it is technically required to install this final component on the server hosts the XProtect Event Server. Go to the XProtect Event Server host, locate the required .msi file. The required file is named:

- Milestone.ACMServer.MipPlugin.msi

Double-click the installation file. Once the wizard detects the XProtect Event Server it will continue. Click "Next" to continue. At the Destination Folder step the default installation directory is provided. This is the default location:

- C:\Program Files\Milestone ACM Server MIP Plugin\

Change the directory location if required, or click "Next" to continue.   Complete the XProtect Event Server MIP Plugin installation 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 on the Event Server. Milestone distributes all component installers with each 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.

XProtect ACM MIP Plugin Configuration

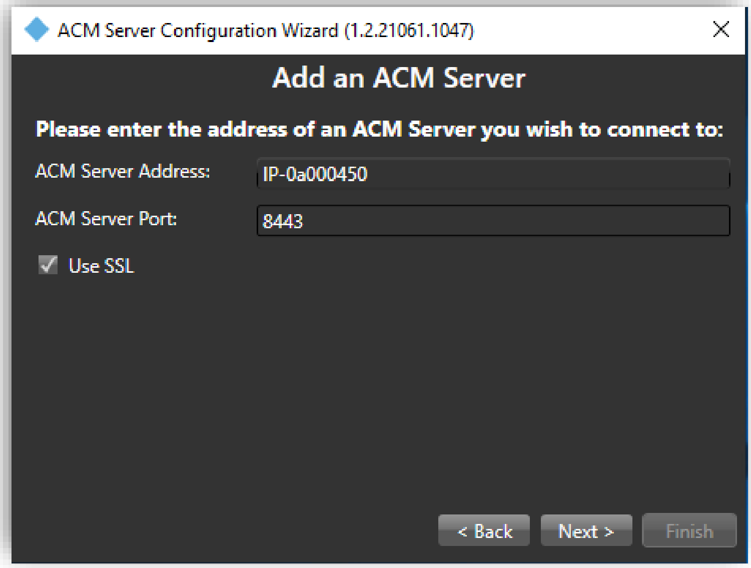
ACM Server Wizard

Once all three software components have been installed:

1. ACM Server
2. CCure 9000 Plugin
3. MIP ACM Plugin

Go to the XProtect Event Server host server and configure the MIP ACM Plugin. The configuration is performed through a wizard application found in the Windows start menu. The wizard can be found by searching for the program by name: "Milestone ACM Server Wizard."

Launch the wizard and click "Next." At the "Add an ACM Server" step, the ACM Server Address field is required and should be entered as the host name of the CCure 9000 host server.


ACM Server Configuration Wizard (1.2.21061.1047)

Add an ACM Server

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

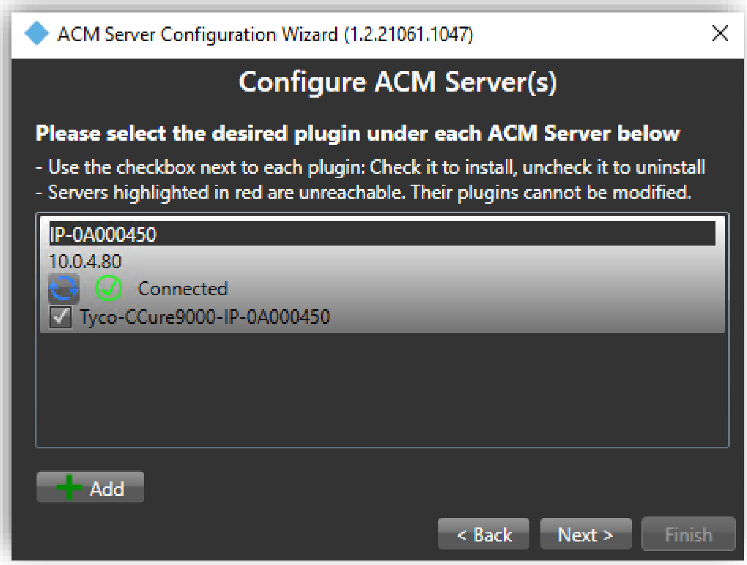
ACM Server Address: IP-0a000450

ACM Server Port: 8443

☑ Use SSL

After the wizard validates the ACM Server address, a green checkmark next to the "Connected" text, indicates a successful connection. Select the checkbox next to the plugin that will be installed. The plugin should be named:

- Tyco-CCure9000-Hostname



ACM Server Configuration Wizard (1.2.21061.1047)

Configure ACM Server(s)

Please select the desired plugin under each ACM Server below

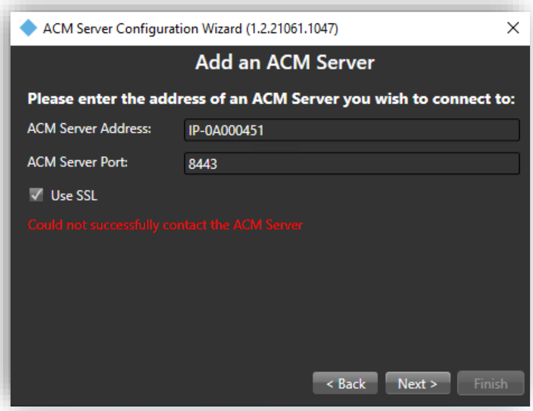
- Use the checkbox next to each plugin: Check it to install, uncheck it to uninstall
- Servers highlighted in red are unreachable. Their plugins cannot be modified.

IP-0A000450
10.0.4.80
Connected
☑ Tyco-CCure9000-IP-0A000450

Complete the Milestone ACM Server Wizard to complete the configuration of the MIP ACM Plugin.

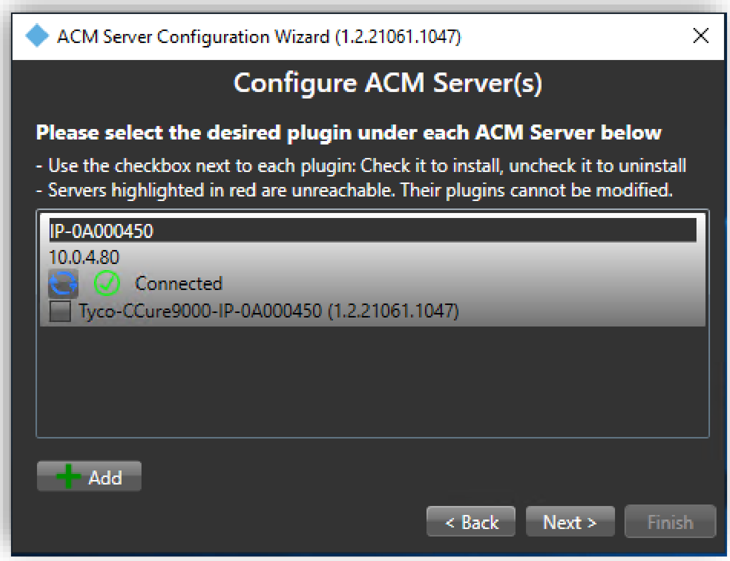
Reasons for failure:

If the Milestone ACM Server Wizard fails to connect to the ACM Server on the CCure 9000 host, a red error message will appear. The wizard will not continue without a valid connection.

Reasons for failed connection	Error message text
Incorrect IP address or hostname for the CCure 9000 host server.	Could not successfully contact the ACM Server  ACM Server Configuration Wizard (1.2.21061.1047) Add an ACM Server **Please enter the address of an ACM Server you wish to connect to:** ACM Server Address: IP-0A000451 ACM Server Port: 8443 ☑ Use SSL Could not successfully contact the ACM Server < Back · Next > · Finish
ACM Server on CCure 9000 host is not running.	
ACM Server on CCure 9000 host is running with insufficient privileges.	

Removing an ACM Server

To remove an ACM Server from the MIP Plugin configuration, start the Milestone ACM Server Wizard and uncheck the checkbox next to the plugin that was previously installed,


ACM Server Configuration Wizard (1.2.21061.1047)

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.

IP-0A000450
10.0.4.80
Connected
□ Tyco-CCure9000-IP-0A000450 (1.2.21061.1047)

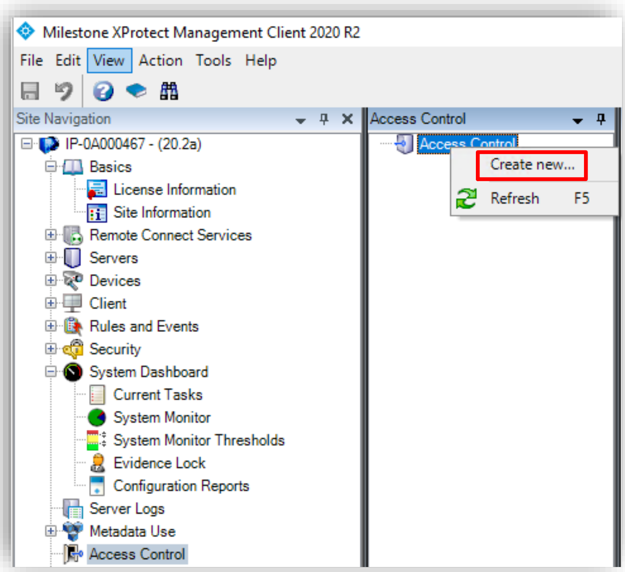
Complete the installation wizard to uninstall the plugin.

XProtect Management Client Configuration

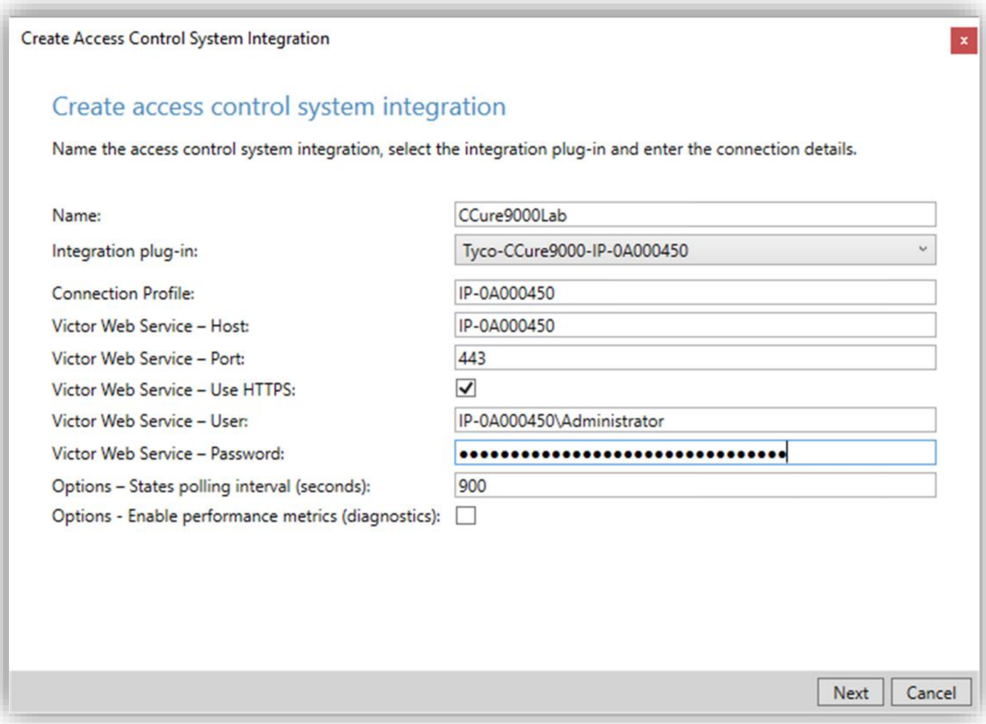
Create XPA Instance Wizard & Establish Connection

Once the MIP ACM Plugin is installed and configured the XProtect Access (XPA) instance can be created in the Management Client.

Go to the Access Control menu in the XProtect Management Client. Right click on the Access Control root node in the Access Control pane and choose “Create new...” from the shortcut menu.



The XPA instance creation wizard begins. Enter a name for the plugin and select the CCure 9000 plugin from the list. The plugin is named Tyco-CCure9000-{Hostname} where {Hostname} is the hostname of the machine where the ACM Server is installed. After selecting the plugin, you will have to provide credentials and parameters to configure the connection to the CCure 9000 victor web service.

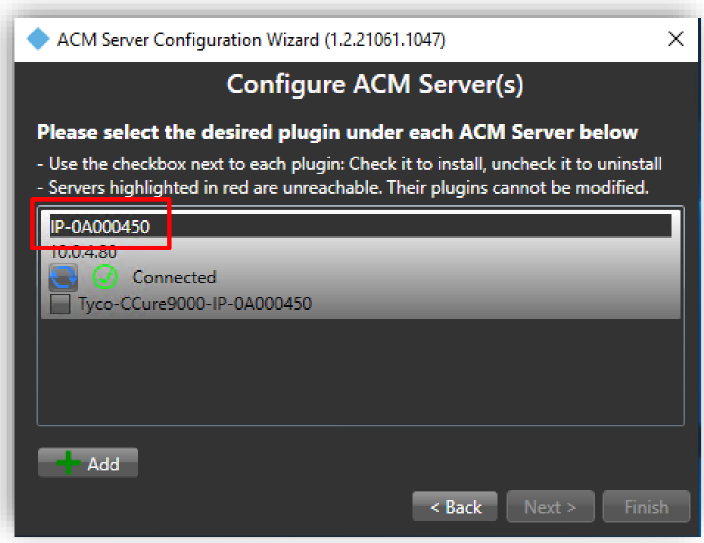

Create Access Control System Integration

Create access control system integration

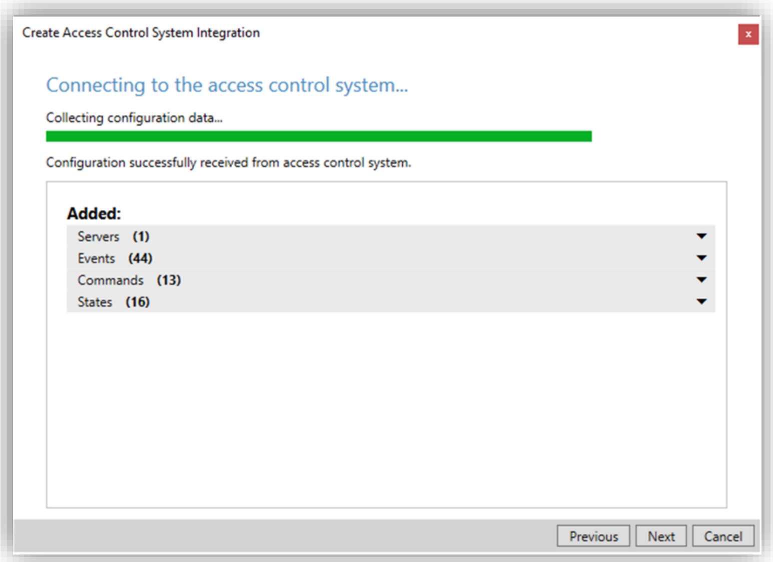
Name the access control system integration, select the integration plug-in and enter the connection details.

Name:	CCure9000Lab
Integration plug-in:	Tyco-CCure9000-IP-0A000450
Connection Profile:	IP-0A000450
Victor Web Service – Host:	IP-0A000450
Victor Web Service – Port:	443
Victor Web Service – Use HTTPS:	☑
Victor Web Service – User:	IP-0A000450\Administrator
Victor Web Service – Password:	••••••••••••••••••••••••••••••••••
Options – States polling interval (seconds):	900
Options - Enable performance metrics (diagnostics):	☐

The credentials and parameters required are detailed below:

Property Name	Required Entry Details
Name	Custom name field
Integration Plugin	Displays the current version of the ACM MIP Plugin
Connection Profile	[Hostname.Domain] address which was displayed in the Milestone ACM Server Wizard.  ACM Server Configuration Wizard (1.2.21061.1047) 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. IP-0A000450 10.0.4.80 Connected □ Tyco-CCure9000-IP-0A000450
Victor Web Service - Host	Host name of the CCure 9000 server
Victor Web Service - Port	443 is the default
Victor Web Service - Use HTTPS	HTTPS is required for secure connection to CCure 9000 by default
Victor Web Service - User	[Domain\Username] for a user account with administrative privileges on the CCure 9000 server.
Victor Web Service - Password	Password for the user account selected for the “Username” field.
Options – States polling interval (seconds)	Default value is 900 seconds. Frequency of status updates retrieved for access control hardware devices. This value can be used to control event processing throughput.
Options – Enable performance metrics (diagnostics)	Not selected by default. Select this option to include performance statistic logging on event metadata.

The wizard will connect to the CCure 9000 system and fetch the configuration into Milestone. This includes servers, controllers, doors, card holders, events, commands, states…etc.


Create Access Control System Integration

Connecting to the access control system...

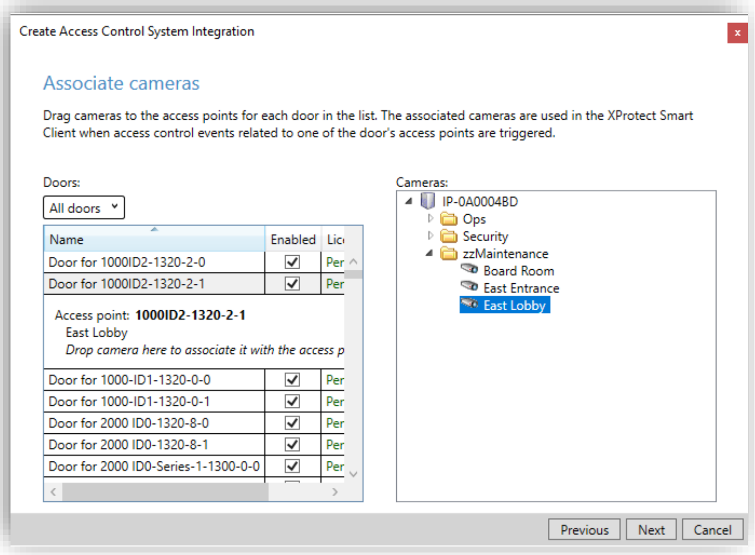
Collecting configuration data...

Configuration successfully received from access control system.

Added:

- Servers (1)
- Events (44)
- Commands (13)
- States (16)

Once the configuration has been fetched, continue the setup wizard. The wizard provides the option to link doors and cameras. This link configures which cameras are displayed when viewing real-time door alarms and events, and when viewing live or recorded video associated to doors. For each link, drag a camera from the camera tree on the right, and place it under a door on the left to create the association.


Create Access Control System Integration

Associate 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: All doors

Name	Enabled	Lic
Door for 1000ID2-1320-2-0	☑	Per
Door for 1000ID2-1320-2-1	☑	Per
Access point: **1000ID2-1320-2-1** East Lobby *Drop camera here to associate it with the access p*		
Door for 1000-ID1-1320-0-0	☑	Per
Door for 1000-ID1-1320-0-1	☑	Per
Door for 2000 ID0-1320-8-0	☑	Per
Door for 2000 ID0-1320-8-1	☑	Per
Door for 2000 ID0-Series-1-1300-0-0	☑	Per

Cameras:

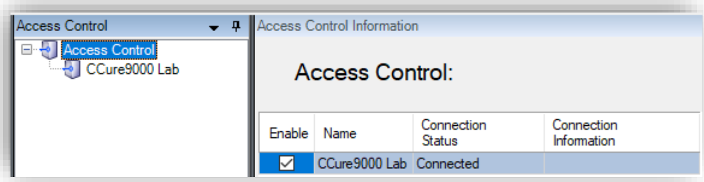
- IP-0A0004BD
  - Ops
  - Security
  - zzMaintenance
    - Board Room
    - East Entrance
    - East Lobby

Complete the wizard to finish creating the XPA instance..

Administrative Configuration:

General Settings:

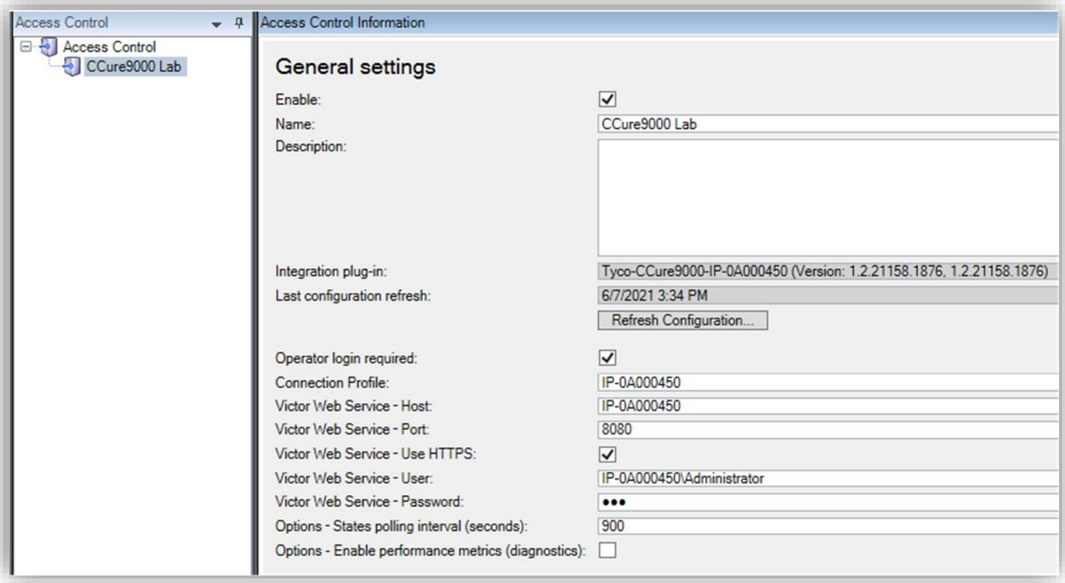
Go to the access control menu in the directory tree of the XProtect Management Client. You can check the status of all instances by selecting the root of the Access Control directory.



Access Control:

Enable	Name	Connection Status	Connection Information
☑	CCure9000 Lab	Connected	

Click on your CCure 9000 XPA Instance to view or modify the properties of the connection.



General settings

Enable:	☑
Name:	CCure9000 Lab
Description:	
Integration plug-in:	Tyco-CCure9000-IP-0A000450 (Version: 1.2.21158.1876, 1.2.21158.1876)
Last configuration refresh:	6/7/2021 3:34 PM
Operator login required:	☑
Connection Profile:	IP-0A000450
Victor Web Service - Host:	IP-0A000450
Victor Web Service - Port:	8080
Victor Web Service - Use HTTPS:	☑
Victor Web Service - User:	IP-0A000450\Administrator
Victor Web Service - Password:	●●●
Options - States polling interval (seconds):	900
Options - Enable performance metrics (diagnostics):	☐

The properties are listed here:

Property Name	Description – Purpose
Enable	Selected by default. Remain selected to keep connection properties active
Name	Custom name field.
Description	Reference information field.
Integration plugin-in	Displays the current version of the ACM MIP Plugin.
Last configuration refresh	Displays the date and time the last system configuration refresh was performed.
Operator login required	Not selected by default. This option should be selected to enable the personalized login feature.

Connection Profile	Internal identification of the ACM MIP Plugin instance used to establish this connection. By default, this field contains the hostname of the CCure 9000 server that hosts the ACM Server.
Victor Web Service - Host	IP address or hostname of the CCure 9000 server that hosts the victor web service.
Victor Web Service - Port	Port used to authenticate to the victor web service. Default is 443.
Victor Web Service - Use HTTPS	Selected by default. Choose this option to enable encrypted credential exchange.
Victor Web Service - User	Username for the account used to authenticate with the victor web service.
Victor Web Service - Password	Password for the account used to authenticate with the victor web service.
Options – States polling interval (seconds)	Default value is 900 seconds. Frequency of status updates retrieved for access control hardware devices. This value can be used to control event processing throughput.
Options – Enable performance metrics (diagnostics)	Not selected by default. Select this option to include performance statistic logging on event metadata.

Personalized Login

Personalized login is an optional feature of XProtect Access. When a user logs into XProtect Smart Client, personalized login adds a second login into CCure 9000. The user presents valid CCure 9000 credentials, and the Smart Client features will only work with access control hardware, events and alarms available to that user's privileges.

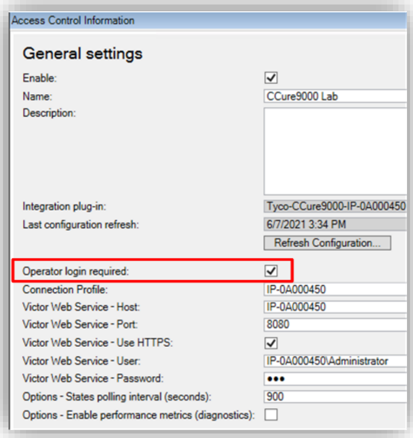
Personalized login manages two configurations. First, is the global configuration used by the Management Client. Second, is the personalized configuration used in the Smart Client. Personalized configurations are subsets of the global configuration. This helps ensure accurate event handling, command execution…etc.

Requirements for Personalized Login

- XPA CCure 9000 integration version 1.1 or higher.
- CCure 9000 version 2.70 SP3 CU1 or higher.

Enable/Disable Personalized Login

Enabling/disabling personalized login for a specific access control plugin is done in the Management Client. The option is in the General settings menu titled "Operator login required:"



Access Control Information

General settings

Enable: ☑

Name: CCure9000 Lab

Description:

Integration plug-in: Tyco-CCure9000-IP-0A000450

Last configuration refresh: 6/7/2021 3:34 PM

Operator login required: ☑

Connection Profile: IP-0A000450

Victor Web Service - Host: IP-0A000450

Victor Web Service - Port: 8080

Victor Web Service - Use HTTPS: ☑

Victor Web Service - User: IP-0A000450\Administrator

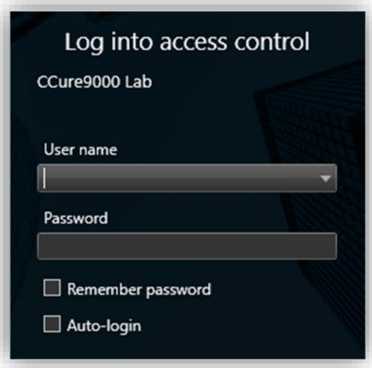
Victor Web Service - Password: •••

Options - States polling interval (seconds): 900

Options - Enable performance metrics (diagnostics): □

Smart Client Personalized Login

A second login into access control dialog is required. It occurs immediately after the standard Smart Client login dialog.



Log into access control

CCure9000 Lab

User name

Password

□ Remember password

□ Auto-login

After entering the username and password, XProtect will attempt to validate the credentials against the CCure 9000 system. If “Skip this step” is selected, the Smart Client is opened without using personalized login, and no XPA features are available in the Smart Client. After authentication with CCure 9000, Smart Client loads a personalized configuration. The Smart Client will only display access control information from the user account that logged in during the personalized configuration login dialog. This includes:

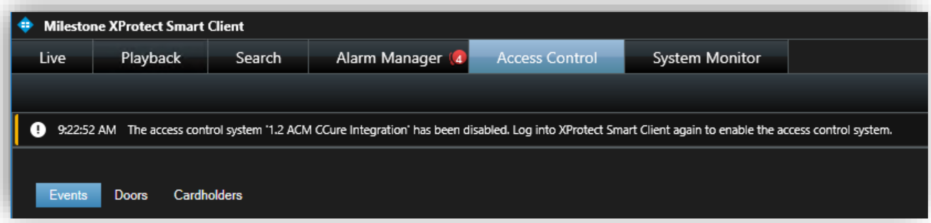
- Alarms related to hardware the user can view in CCure.
- Events related to hardware the user can view in CCure.
- Devices in the map element selector that the user can view in CCure.

XProtect Personalized Login does not specifically include personalized alarm acknowledgment. Rather, as with standard “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.

Refreshing the Personalized Configurations

The XProtect Event Server stores personalized configurations for XProtect Smart Client users. Stored personalized configurations are cleared when the Event Server restarts. When the global configuration of the XPA instance is refreshed, the Event Server updates all stored personalized configurations. Log out of the Smart Client and log back in using the personalized configuration to load the updated configuration.

If the global configuration is changed for a user who is currently logged into the Smart Client using the personalized login feature, and their CCure access rights are included in the change, the Smart Client application will have the following info message displayed.



9:22:52 AM The access control system '1.2 ACM CCure Integration' has been disabled. Log into XProtect Smart Client again to enable the access control system.

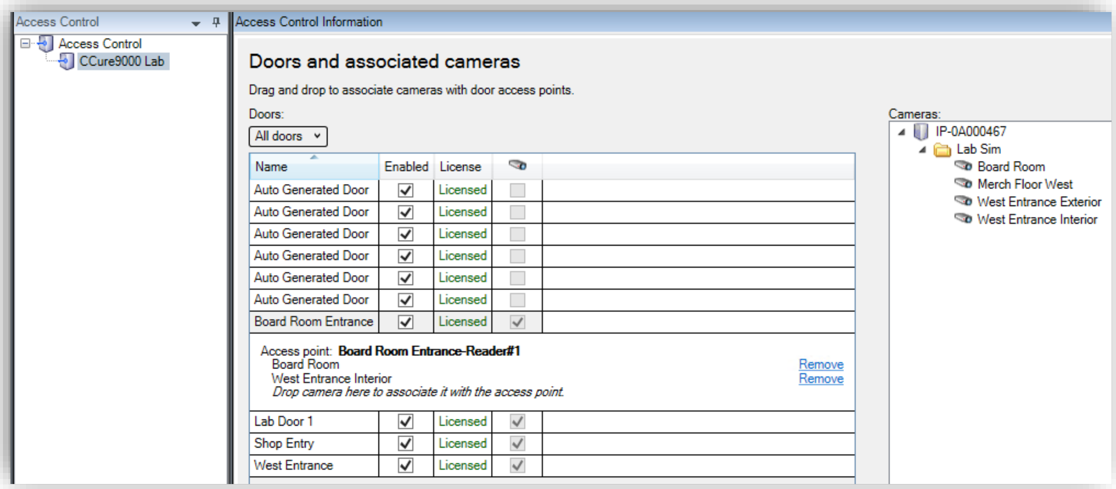
If this message appears, simply follow the instructions in the message. Logging out of the Smart Client application and re-authenticating using the personalized login process will fetch an updated configuration.

Door & Camera Association

In the Doors and Associated Cameras menu of the XPA Instance it is possible to verify the status of all connected doors, and create, reassign, and remove the association between cameras and doors.

Doors require associated cameras to view live and recorded video - and listen to or play audio through any XProtect client application that supports visualization of doors.

Open the doors list and select a panel or the “All doors” group to view all doors connected to that panel.



Doors and associated cameras

Drag and drop to associate cameras with door access points.

Doors: All doors

Name	Enabled	License	
Auto Generated Door	☑	Licensed	□
Auto Generated Door	☑	Licensed	□
Auto Generated Door	☑	Licensed	□
Auto Generated Door	☑	Licensed	□
Auto Generated Door	☑	Licensed	□
Auto Generated Door	☑	Licensed	□
Board Room Entrance	☑	Licensed	☑
Access point: **Board Room Entrance-Reader#1** Board Room — Remove West Entrance Interior — Remove *Drop camera here to associate it with the access point*			
Lab Door 1	☑	Licensed	☑
Shop Entry	☑	Licensed	☑
West Entrance	☑	Licensed	☑

Cameras:
- IP-0A000467
  - Lab Sim
    - Board Room
    - Merch Floor West
    - West Entrance Exterior
    - West Entrance Interior

Click on a door. Under it all associated cameras are listed. Select a camera from the Cameras list on the right and drag the selected camera into the list of cameras associated to the chosen door. Click the Remove link to end the association between the camera and the door.

Categorize Events

Large scale access control systems, such as those managed by CCure 9000, need to functionally integrate with XProtect without programming large numbers of individual alarms and rules. Categorizing access control events greatly minimizes the number of individual alarms and rules that need to be programmed.

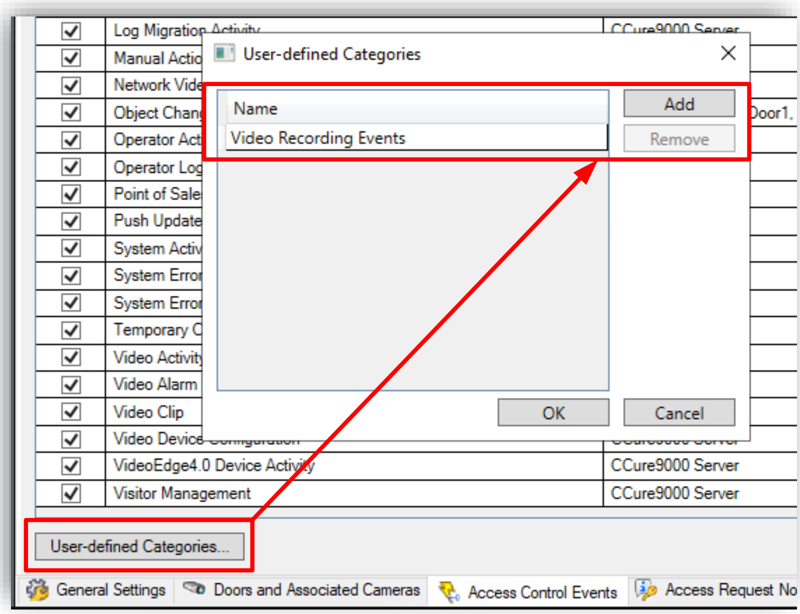
To generate XProtect alarms or rule-based actions triggered by any one of a group of individual CCure events, the events must be categorized. For example, the integration can be configured to start recording video from associated cameras based on any number of unique hardware events: “Door Forced,” “Denied, Badge Not in Panel,” and “Access Denied Unauthorized Entry Level.” Chosen events are placed in the same category, and then a rule is created to start recording based on the receipt within XPA of any event in that category.

The categories are:

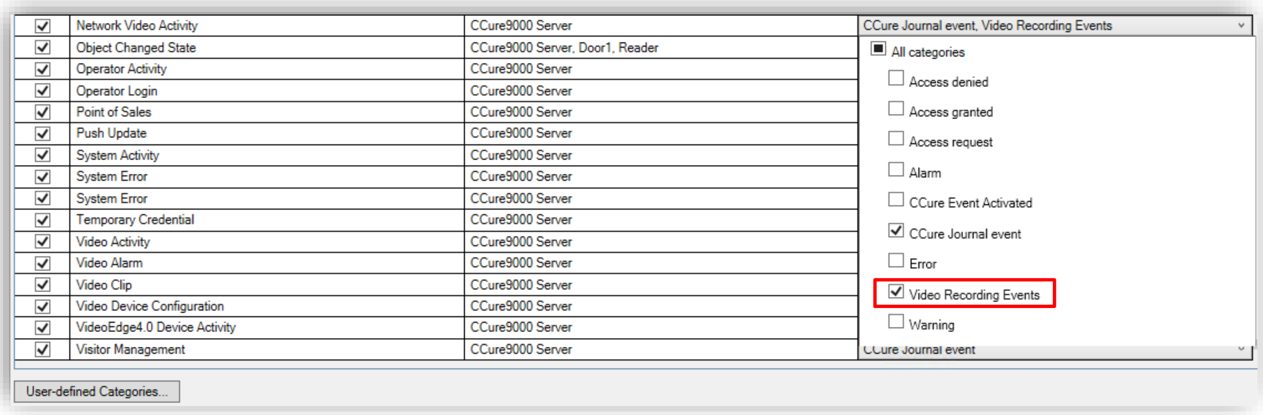
Default XPA Events	CCure Events	Custom Events
• Access Granted • Access Request • Access Denied • Alarm	• CCure Event Activated • CCure Journal event	• User Defined Category…

• Error • Warning		

To create a User-defined Category, there is a User-defined Categories button on the bottom left corner of the Access control events menu. Click the User-defined Categories button to create your own custom event category.



Click Add, name the category, and press OK. The User-defined Category appears as an option in the Event Category list.

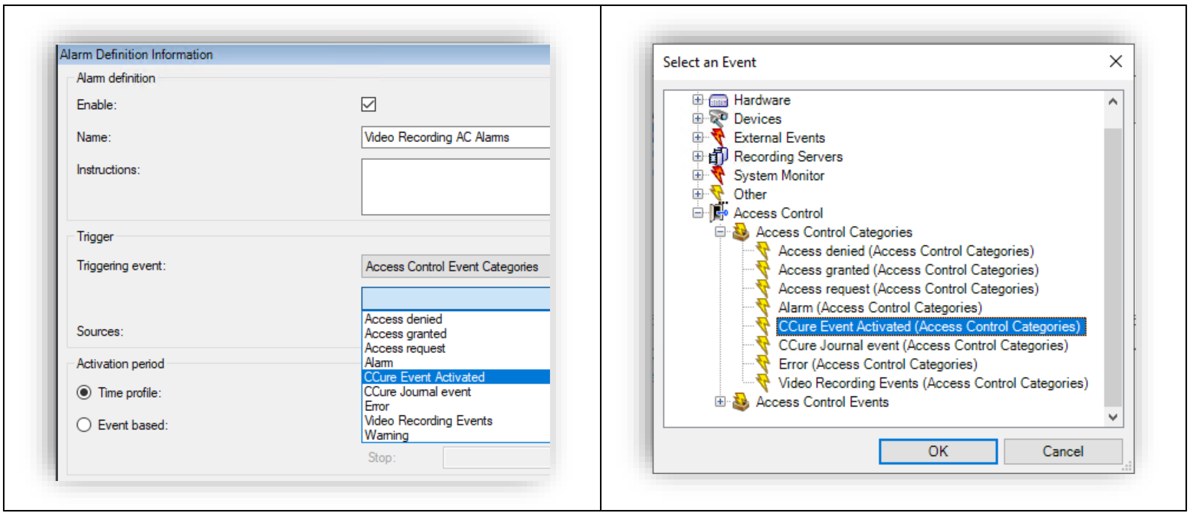


☑	Network Video Activity	CCure9000 Server	CCure Journal event, Video Recording Events
☑	Object Changed State	CCure9000 Server, Door1, Reader	
☑	Operator Activity	CCure9000 Server	
☑	Operator Login	CCure9000 Server	
☑	Point of Sales	CCure9000 Server	
☑	Push Update	CCure9000 Server	
☑	System Activity	CCure9000 Server	
☑	System Error	CCure9000 Server	
☑	System Error	CCure9000 Server	
☑	Temporary Credential	CCure9000 Server	
☑	Video Activity	CCure9000 Server	
☑	Video Alarm	CCure9000 Server	
☑	Video Clip	CCure9000 Server	
☑	Video Device Configuration	CCure9000 Server	
☑	VideoEdge4.0 Device Activity	CCure9000 Server	
☑	Visitor Management	CCure9000 Server	CCure Journal event

■ All categories
□ Access denied
□ Access granted
□ Access request
□ Alarm
□ CCure Event Activated
☑ CCure Journal event
□ Error
☑ Video Recording Events
□ Warning

Alarms and Rules in XProtect are triggered using any category of event.

Alarm Access Control Categories Event list	Rule Access Control Categories Event list



Alarm Definition Information

Alarm definition

Enable: ☑

Name: Video Recording AC Alarms

Instructions:

Trigger

Triggering event: Access Control Event Categories

Sources:

Activation period

● Time profile:

○ Event based:

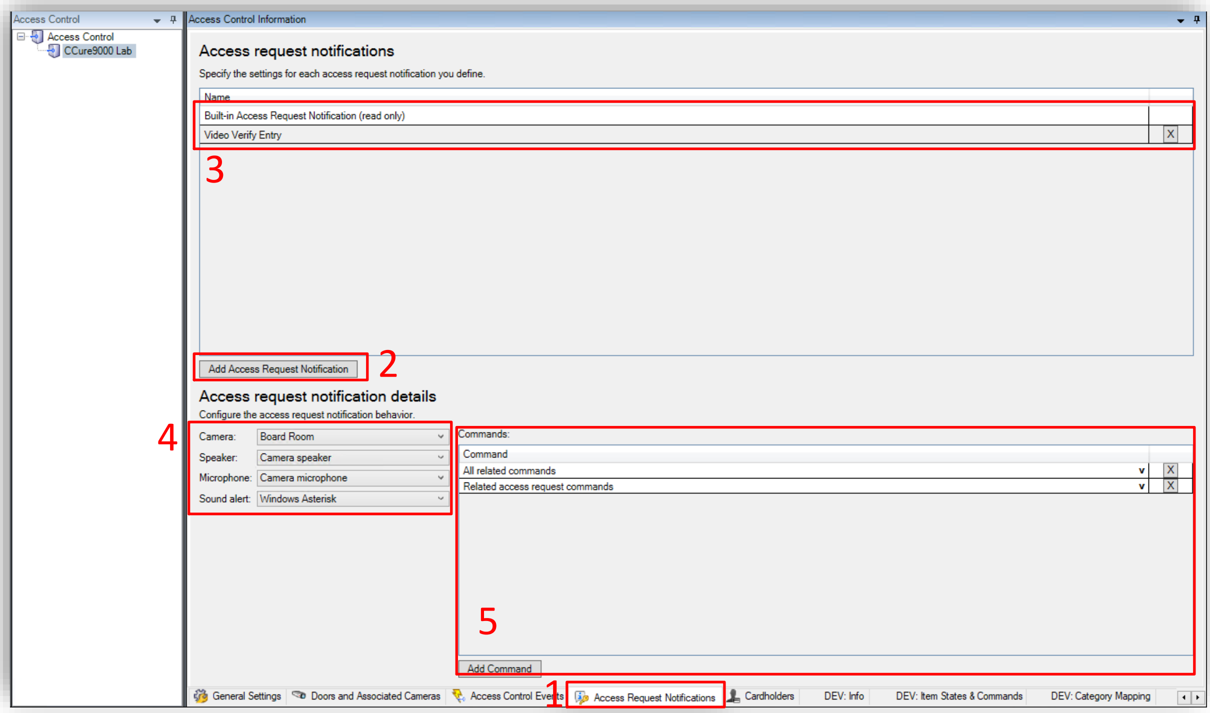
Stop:

Access denied
Access granted
Access request
Alarm
CCure Event Activated
CCure Journal event
Error
Video Recording Events
Warning
Select an Event
Hardware
Devices
External Events
Recording Servers
System Monitor
Other
Access Control
Access Control Categories
Access denied (Access Control Categories)
Access granted (Access Control Categories)
Access request (Access Control Categories)
Alarm (Access Control Categories)
CCure Event Activated (Access Control Categories)
CCure Journal event (Access Control Categories)
Error (Access Control Categories)
Video Recording Events (Access Control Categories)
Access Control Events
OK
Cancel

Access Request Notifications

Access Request Notifications are pop-up notifications which appear in front of all other desktop applications for all users logged into the Smart Client with access to view XPA features and devices. These notifications can be customized in the Access Request Notifications menu. The XPA integration includes a Built-in Access Request Notification.

1. Go to the Access Request Notification menu.
2. Click the Add Access Request Notification button.
3. Name the new notification.
4. Associate cameras, speakers, microphones, and sounds.
5. Click the Add Command button and open the Command list to select which Commands appear on the Notification.



Access request notifications

Specify the settings for each access request notification you define.

Name	
Built-in Access Request Notification (read only)	
Video Verify Entry	X

Access request notification details

Configure the access request notification behavior.

Camera: Board Room

Speaker: Camera speaker

Microphone: Camera microphone

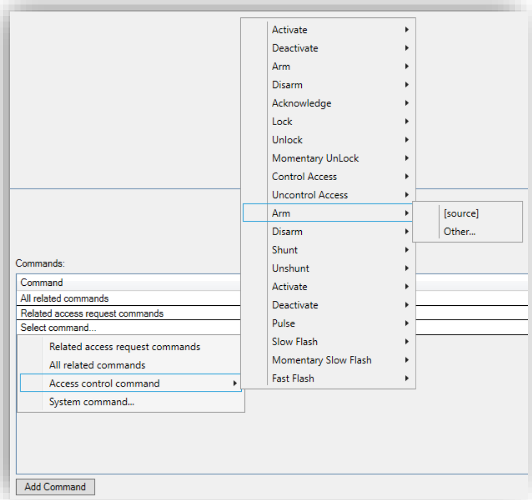
Sound alert: Windows Asterisk

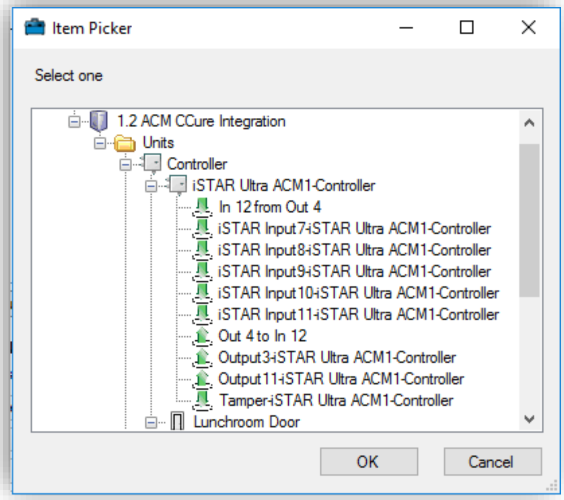
Commands:

Command	
All related commands	X
Related access request commands	X

Access Control
Access Control
CCure9000 Lab
Access Control Information
3
Add Access Request Notification
2
4
5
Add Command
1
General Settings
Doors and Associated Cameras
Access Control Events
Access Request Notifications
Cardholders
DEV: Info
DEV: Item States & Commands
DEV: Category Mapping

Open the Commands list and choose a type of Command, the action the Command will perform, and the hardware device to Command. If the Command should interact with a hardware device that is not related to the device which triggered the Access Request Notification, choose “Other” and select from the list of all devices.

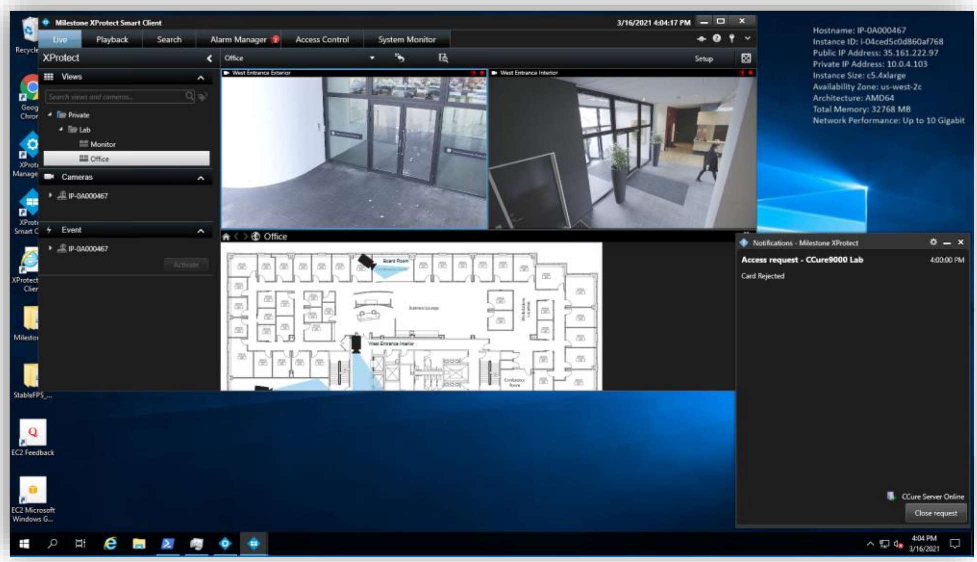




Item Picker
Select one
1.2 ACM CCure Integration
Units
Controller
iSTAR Ultra ACM1-Controller
In 12 from Out 4
iSTAR Input7-iSTAR Ultra ACM1-Controller
iSTAR Input8-iSTAR Ultra ACM1-Controller
iSTAR Input9-iSTAR Ultra ACM1-Controller
iSTAR Input10-iSTAR Ultra ACM1-Controller
iSTAR Input11-iSTAR Ultra ACM1-Controller
Out 4 to In 12
Output3-iSTAR Ultra ACM1-Controller
Output11-iSTAR Ultra ACM1-Controller
Tamper-iSTAR Ultra ACM1-Controller
Lunchroom Door
OK
Cancel

When the notification pops up on the desktop a sound will play if you choose to include a Sound alert. The Built-in Access Request Notification does not include a Sound alert.

Access Request Notifications can be used to trigger pop up notifications from within the XProtect rules system, and the notifications do not need to be connected to access control hardware devices.

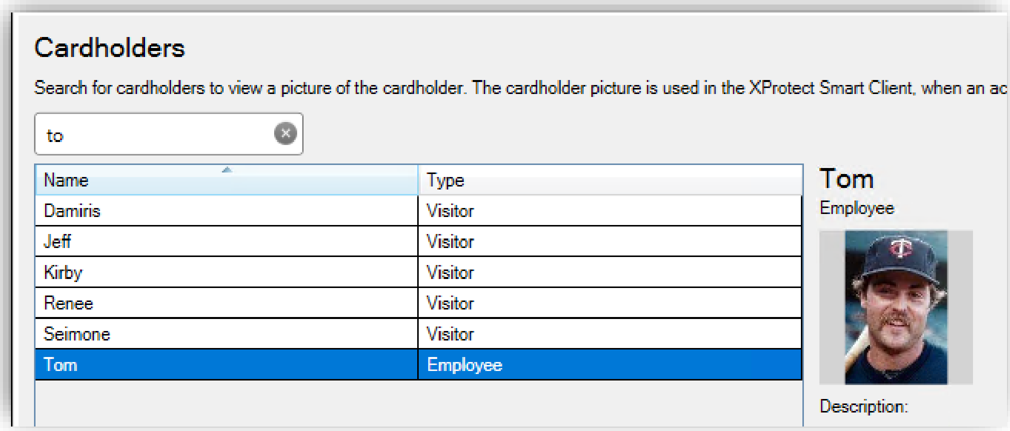


Hostname: IP-0A000467
Instance ID: i-04ced5c0d860af768
Public IP Address: 35.161.222.97
Private IP Address: 10.0.4.103
Instance Size: c5.4xlarge
Availability Zone: us-west-2c
Architecture: AMD64
Total Memory: 32768 MB
Network Performance: Up to 10 Gigabit

Access request - CCure9000 Lab 4:00:00 PM
Card Rejected

Searching Cardholders

All cardholders in the CCure system are imported from the connected server. Search for cardholders in the Cardholders menu of the XPA instance. First Name, Last Name, Badge Numbers, and Cardholder ID are all included in the search. As characters are typed in the box, searching begins across all fields:



Cardholders

Search for cardholders to view a picture of the cardholder. The cardholder picture is used in the XProtect Smart Client, when an ac

to

Name	Type
Damiris	Visitor
Jeff	Visitor
Kirby	Visitor
Renee	Visitor
Seimone	Visitor
Tom	Employee

Tom
Employee

Description:

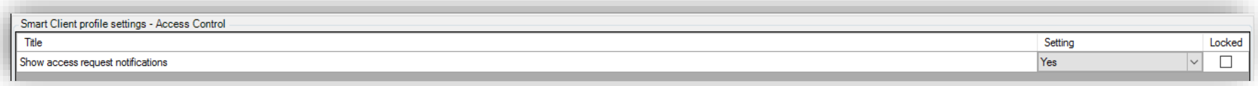
Visibility of Cardholder information, such as name, Badge numbers…etc., are controlled within the CCure database.

Client Profiles & Roles

Smart Client Profiles and User Roles in XProtect allow administrators to control the features available in the XProtect Smart Client.

Smart Client Profiles allow control over the visibility of access request notifications. Roles allow control over access control globally, visibility of the cardholder list, and access request notifications. For example, if a user cannot receive access request notifications it could be disabled in both the Smart Client Profile that user is assigned, or in their Role.

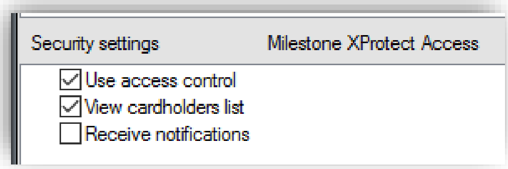
To manage Smart Client Profiles – open the Management Client, expand Client and select Smart Client Profiles. The Access Control menu contains the setting for notifications.



Smart Client profile settings - Access Control

Title	Setting	Locked
Show access request notifications	Yes	□

To manage Roles – open the Management Client, expand Security and select Roles. Select the role to manage and click on the Access Control menu to adjust the available settings.



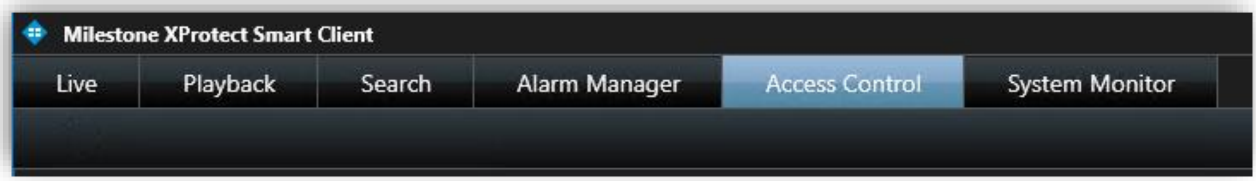
Security settings | Milestone XProtect Access

☑ Use access control
☑ View cardholders list
□ Receive notifications

Smart Client Features

Access Control Workspace

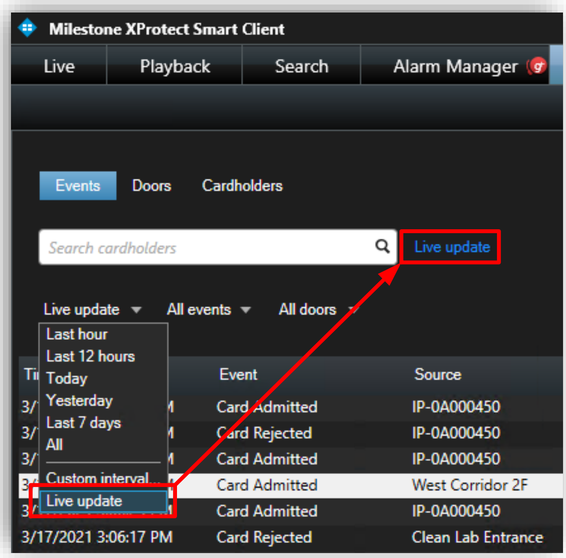
The XPA CCure integration adds a new workspace, or tab, into the XProtect Smart Client. The Access Control workspace should appear in the Smart Client.



This workspace is used to search and filter Events, Doors and Cardholders.

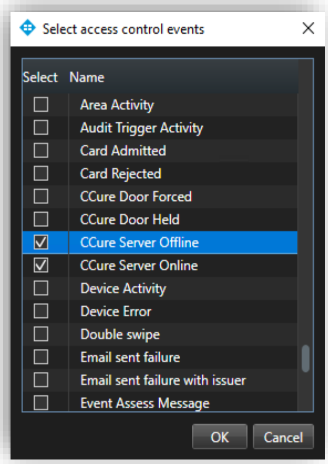
Events:

Choose a time range, including a custom time range, or live update. Choose the Live update time range to view a real-time display of access control events.



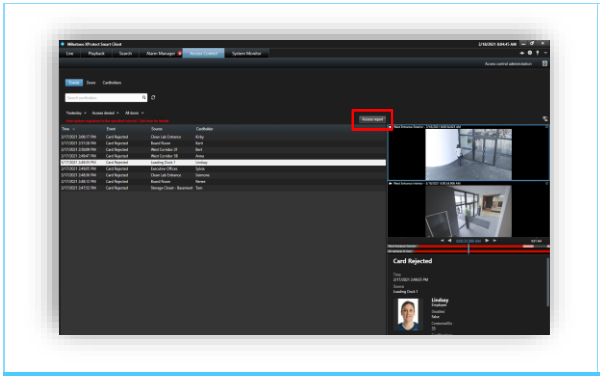
Ti	Event	Source
3/	Card Admitted	IP-0A000450
3/	Card Rejected	IP-0A000450
3/	Card Admitted	IP-0A000450
3/	Card Admitted	West Corridor 2F
3/	Card Admitted	IP-0A000450
3/17/2021 3:06:17 PM	Card Rejected	Clean Lab Entrance

Filter for specific events including custom events and all integrated CCure events. Open the All events list and select the “Access control event...” option to open the Select access control events window. Choose a specific CCure event from this list.



Select	Name
☐	Area Activity
☐	Audit Trigger Activity
☐	Card Admitted
☐	Card Rejected
☐	CCure Door Forced
☐	CCure Door Held
☑	CCure Server Offline
☑	CCure Server Online
☐	Device Activity
☐	Device Error
☐	Double swipe
☐	Email sent failure
☐	Email sent failure with issuer
☐	Event Assess Message

Filter for specific hardware devices. Click the Access report button to create a PDF file of the events in the current list. In the Access report window: name the report, choose a destination to save the report, include comments, and select the option to include snapshots.



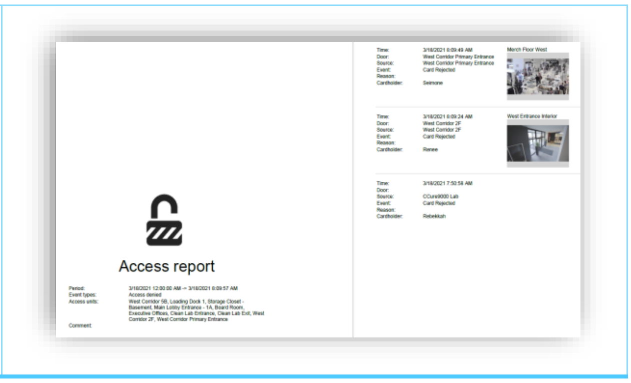
Time	Event	Source	Cardholder
3/17/2021 3:06:17 PM	Card Rejected	Clean Lab Entrance	Kirby
3/17/2021 2:57:38 PM	Card Rejected	Board Room	Kent
3/17/2021 2:50:09 PM	Card Rejected	West Corridor 2F	Bert
3/17/2021 2:49:47 PM	Card Rejected	West Corridor 5B	Anna
3/17/2021 2:49:31 PM	Card Rejected	Loading Dock 1	Lindsay
3/17/2021 2:49:05 PM	Card Rejected	Executive Offices	Sylvia
3/17/2021 2:48:36 PM	Card Rejected	Clean Lab Entrance	Seimone
3/17/2021 2:48:12 PM	Card Rejected	Board Room	Renee
3/17/2021 2:47:52 PM	Card Rejected	Storage Closet - Basement	Tom

Card Rejected

Time
3/17/2021 2:49:05 PM

Source
Loading Dock 1

Lindsay
Employee
Disabled
False
CredentialIDs
35


Access report

Period: 3/18/2021 12:00:00 AM -> 3/18/2021 8:09:57 AM
Event types: Access denied
Access units: West Corridor 5B, Loading Dock 1, Storage Closet - Basement, Main Lobby Entrance - 1A, Board Room, Executive Offices, Clean Lab Entrance, Clean Lab Exit, West Corridor 2F, West Corridor Primary Entrance
Comment:

Time: 3/18/2021 8:09:49 AM
Door: West Corridor Primary Entrance
Source: West Corridor Primary Entrance
Event: Card Rejected
Reason:
Cardholder: Seimone

Merch Floor West

Time: 3/18/2021 8:09:24 AM
Door: West Corridor 2F
Source: West Corridor 2F
Event: Card Rejected
Reason:
Cardholder: Renee

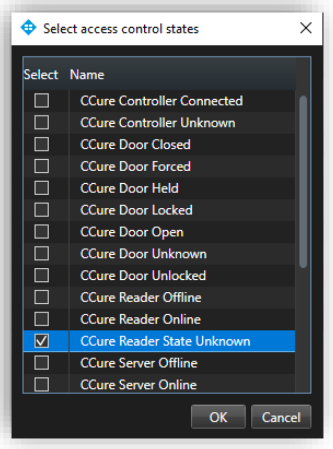
West Entrance Interior

Time: 3/18/2021 7:50:58 AM
Door:
Source: CCure9000 Lab
Event: Card Rejected
Reason:
Cardholder: Rebekkah

Doors:

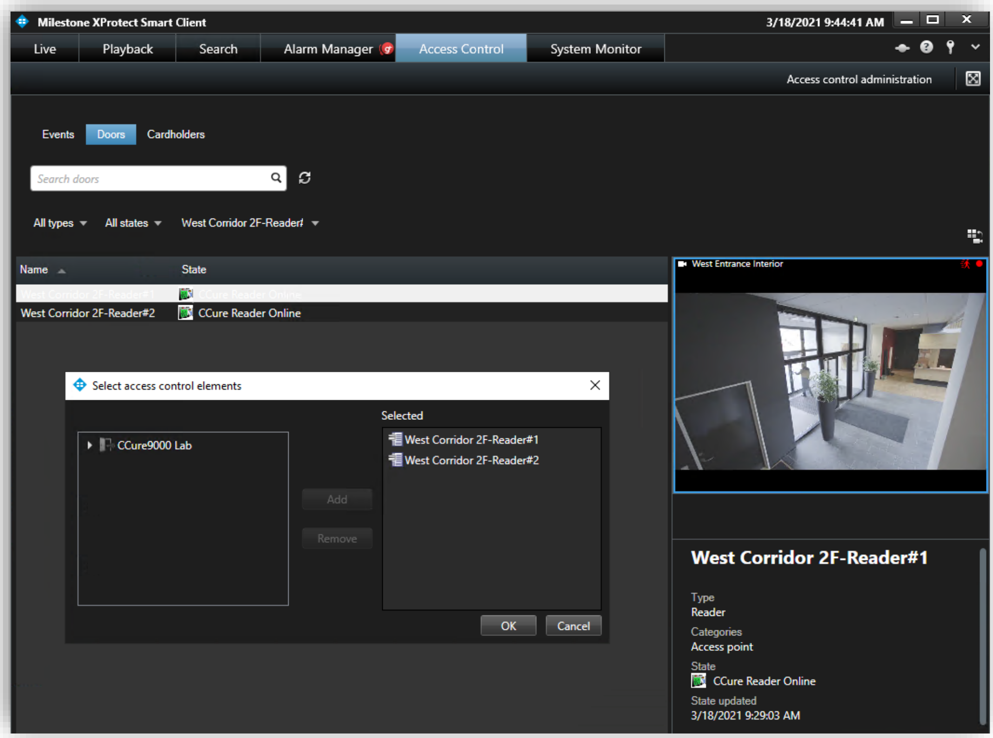
Open the Door list and select the type of access control hardware to display. Choose the “Access control type...,” option to open the “Select access control types” window. “Door” is the default option for this list, however, servers, and readers can also be selected.

Open the “All states” list to filter hardware by status. Choose the “Access control state...,” option to open the Select access control states window and select from the list of all available CCure hardware states.


Select access control states

Select	Name
□	CCure Controller Connected
□	CCure Controller Unknown
□	CCure Door Closed
□	CCure Door Forced
□	CCure Door Held
□	CCure Door Locked
□	CCure Door Open
□	CCure Door Unknown
□	CCure Door Unlocked
□	CCure Reader Offline
□	CCure Reader Online
☑	CCure Reader State Unknown
□	CCure Server Offline
□	CCure Server Online

Open the “All doors” list and expand the list or select the “Other...,” option to open the Select access control elements window. This window provides a directory of all the CCure hardware in the system. Expand the directory, find the hardware device(s), and add them to the selected list. When choosing a specific type of hardware, verify that the hardware type filter does not conflict with the chosen device(s).



Name	State
West Corridor 2F-Reader#1	CCure Reader Online
West Corridor 2F-Reader#2	CCure Reader Online

Selected
- West Corridor 2F-Reader#1
- West Corridor 2F-Reader#2

West Corridor 2F-Reader#1

Type
Reader

Categories
Access point

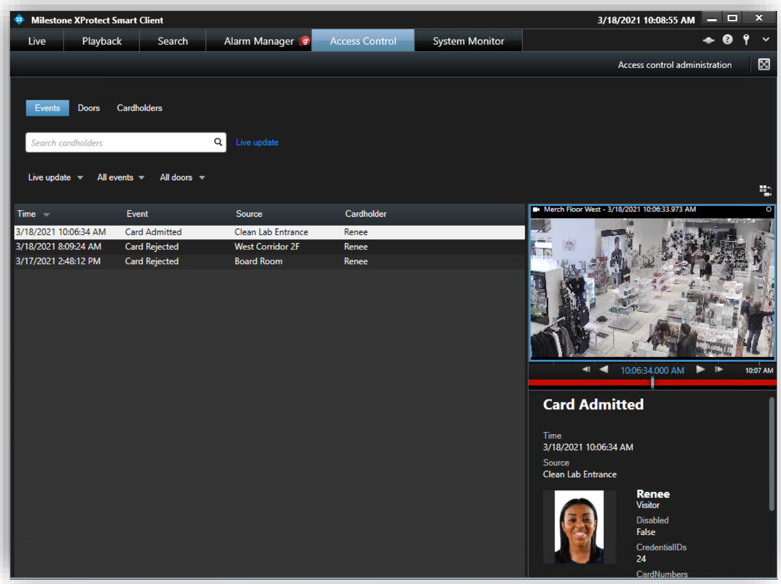
State
CCure Reader Online

State updated
3/18/2021 9:29:03 AM

Select a Door or other type of hardware device in the list to see video from associated cameras, view status information, and Command buttons available for that device.

Cardholders:

By default, all cardholders in the system are displayed in the list. Filter for specific cardholders by typing into the search field. Select a cardholder to view their data. Click the View cardholder events button to switch to the Events list automatically filtered to display events only from the chosen cardholder.



Time	Event	Source	Cardholder
3/18/2021 10:06:34 AM	Card Admitted	Clean Lab Entrance	Renee
3/18/2021 8:09:24 AM	Card Rejected	West Corridor 2F	Renee
3/17/2021 2:48:12 PM	Card Rejected	Board Room	Renee

Card Admitted

Time
3/18/2021 10:06:34 AM

Source
Clean Lab Entrance

Renee
Visitor

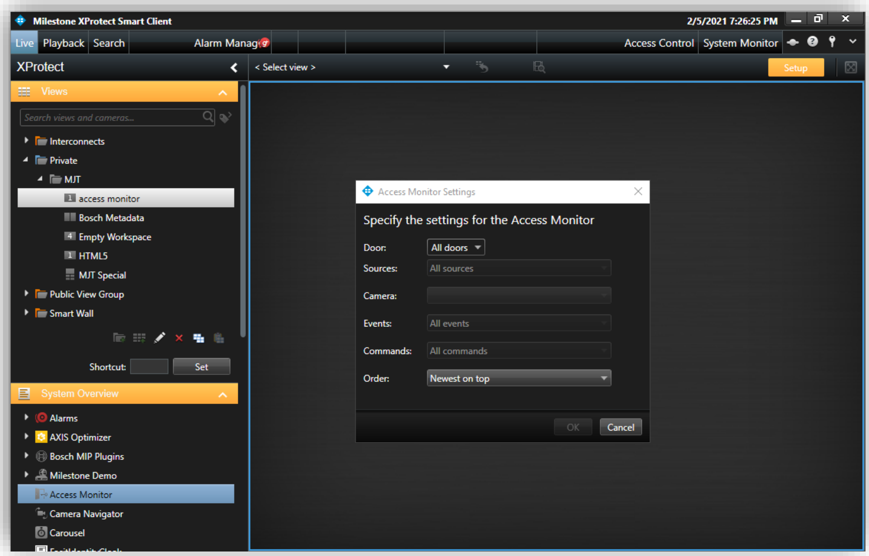
Disabled
False

CredentialIDs
24

CardNumbers

Access Monitor

The Access Monitor view item displays live status from doors and video from associated cameras in a single view pane in the Smart Client. Click Setup in the Smart Client and expand the System Overview panel menu. Select the Access Monitor view item and drag it into any available view pane:



Access Monitor Settings

Specify the settings for the Access Monitor

Door: All doors

Sources: All sources

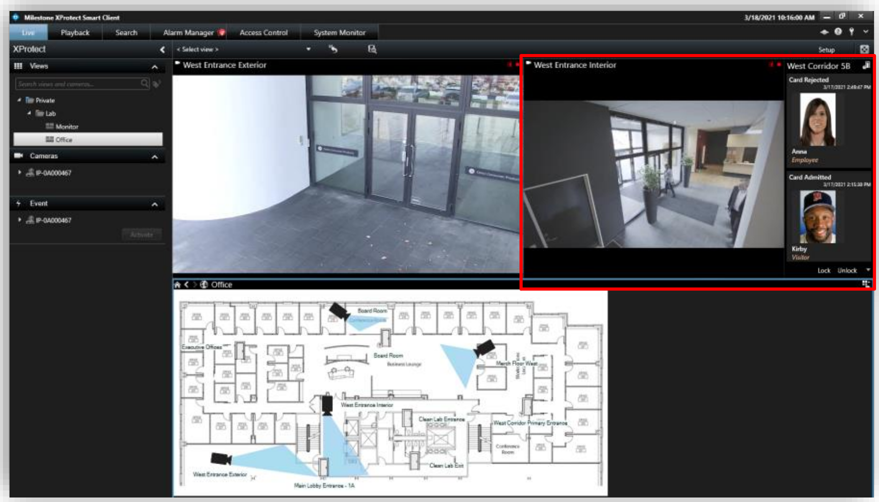
Camera:

Events: All events

Commands: All commands

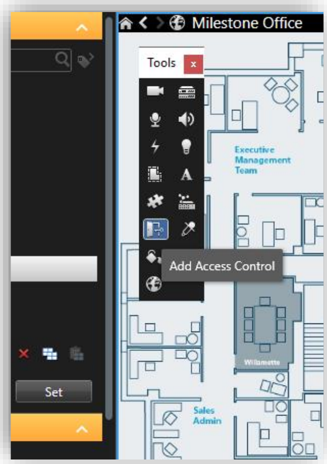
Order: Newest on top

In the access monitor settings window open the lists to select the door, sources, cameras, events, commands, and the order in which new events appear in the access monitor. Once the door is selected, many of the other options will change, based upon the available cameras, events, and commands. The access monitor view item can be added to any available view pane and works in a view alongside all available view items.

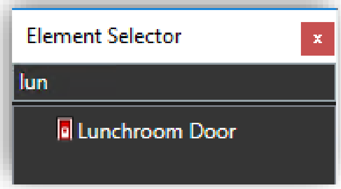


Maps

It is possible to place doors, readers, inputs, outputs, panels and CCure server(s) on an existing Smart Client Map. The map icons display hardware status as well as execute commands. With the Smart Client in setup mode a Tools window will appear in the view pane. From this window, select the Add access control icon:

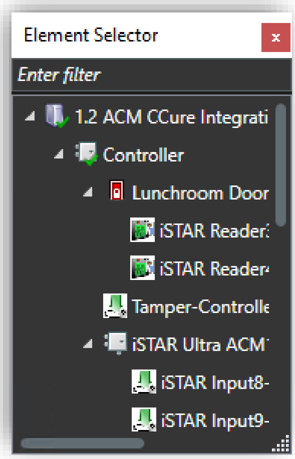


The Element selector window will appear. Type the name of a hardware device into the filter to quickly find a device or expand the servers and panels to find all available hardware icons in the system.


Element Selector

lun

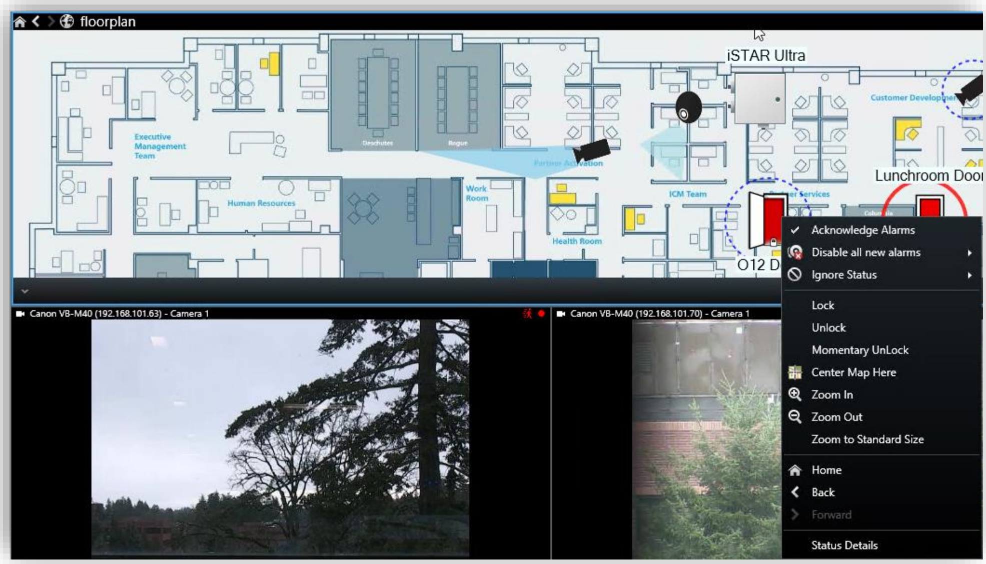
Lunchroom Door


Element Selector

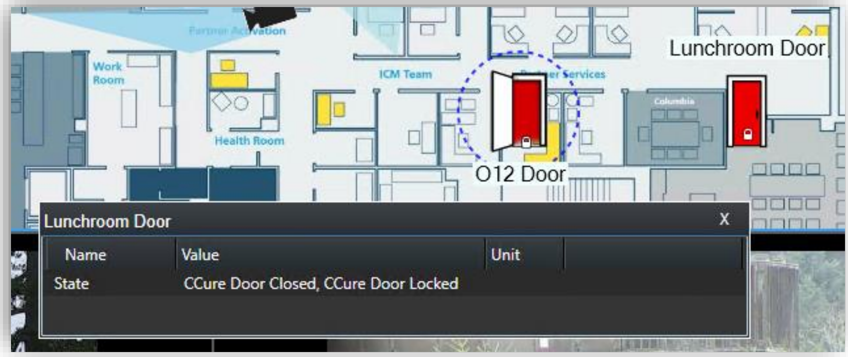
Enter filter

- 1.2 ACM CCure Integrati
  - Controller
    - Lunchroom Door
      - iSTAR Reader:
      - iSTAR Reader‹
    - Tamper-Controlle
    - iSTAR Ultra ACM
      - iSTAR Input8-
      - iSTAR Input9-

Drag the chosen icon onto the map. During normal operations, it is possible to right-click on any of these icons to execute the commands from the shortcut menu.



Right click the device icon and select Status Details from the shortcut menu to view more information.

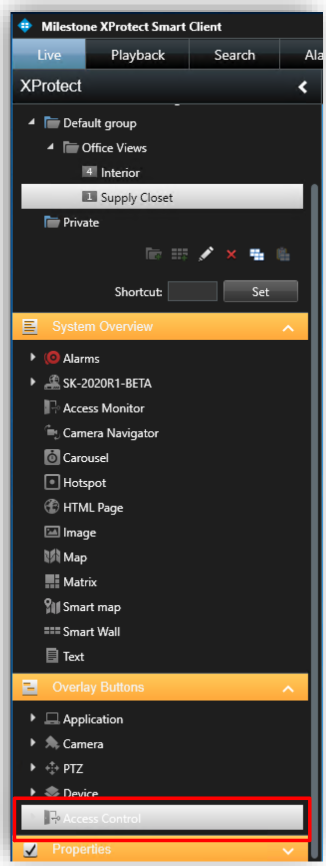


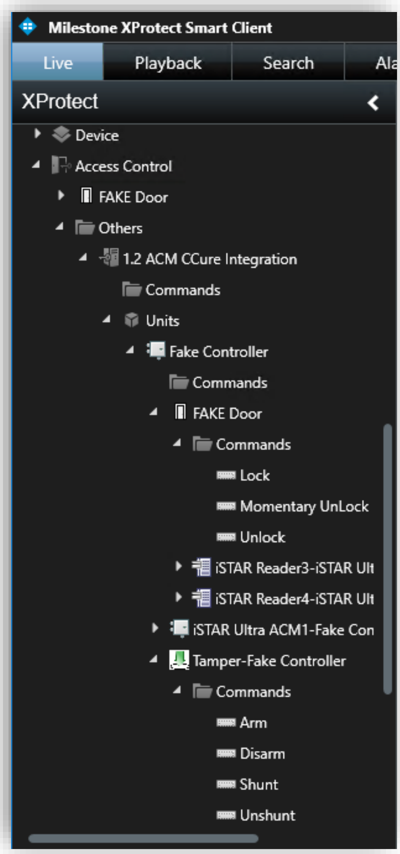
Lunchroom Door

Name	Value	Unit
State	CCure Door Closed, CCure Door Locked	

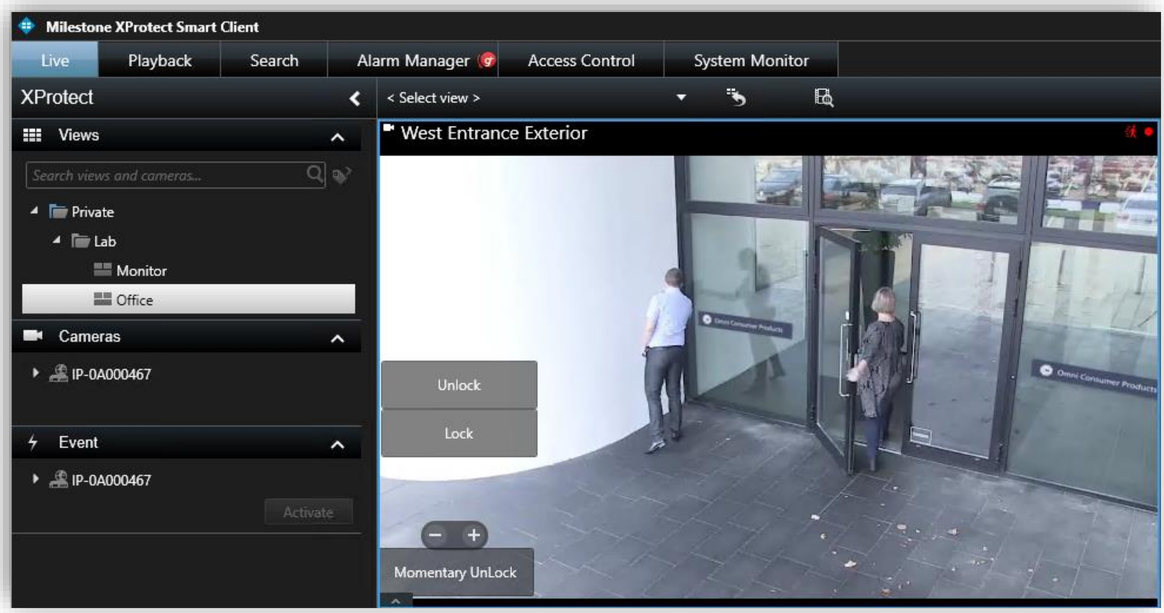
Overlay Buttons & Commands

Overlay buttons are used to add manual buttons to video panes. Anything that can be triggered by a command can be added with an overlay button in the Smart Client. When the Smart Client is in setup mode, there is an Overlay Buttons panel on the left side of the client, select the Access Control icon. Expand the Access Control icon to find all the doors and readers, panels, and the connected inputs and outputs in the system.





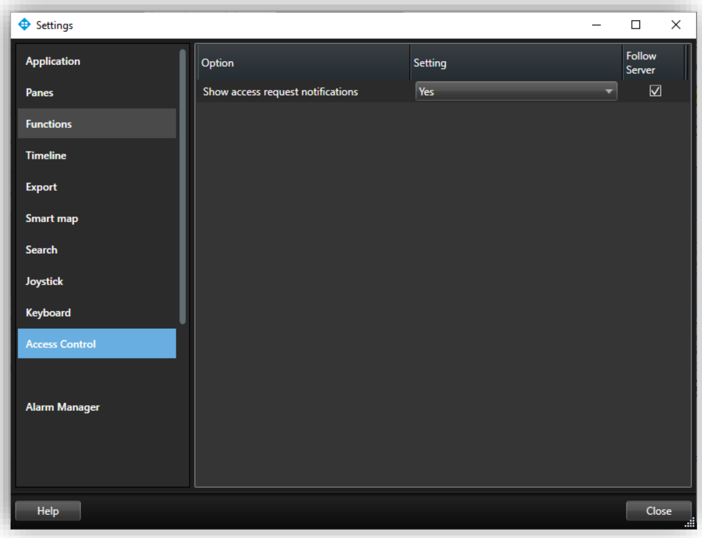
Select a Command from the list and drag it onto the view pane. Once the commands are visible on a camera view pane they can be resized, moved around, and - with a right click - the name of the command can be edited.



Access Control Options

In the upper right corner of the Smart Client application is a down arrow icon.

Click on this icon and choose the settings option to enter the Smart Client settings window. Select the Access control menu in the Settings window. Choose to show or block access request notifications in the Smart Client.



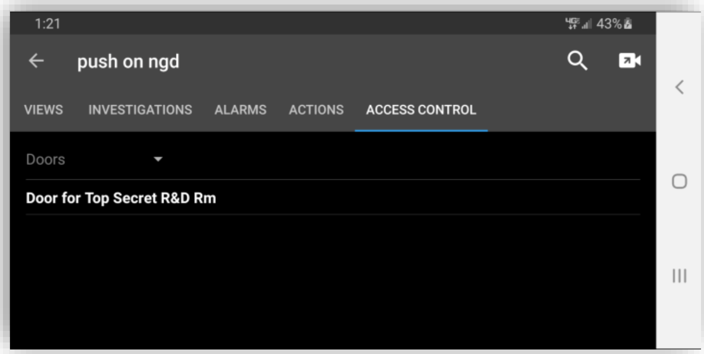
Option	Setting	Follow Server
Show access request notifications	Yes	☑

Mobile Client

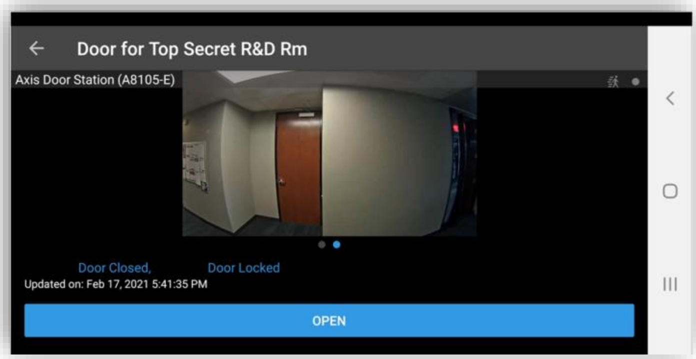
Milestone Mobile is a smartphone app that connects to your VMS system. The XProtect Access CCure 9000 Integration adds functionality to Milestone Mobile. Using Milestone Mobile it is possible to receive a push notification from the access control system, view live video related to the notification, and open the door – all remotely from a smartphone.

Access Control Tab in Milestone Mobile

After logging into the VMS with Milestone Mobile the Views tab is presented by default. From this tab it is possible to select the Access Control tab. The Access Control tab shows the list of doors available.

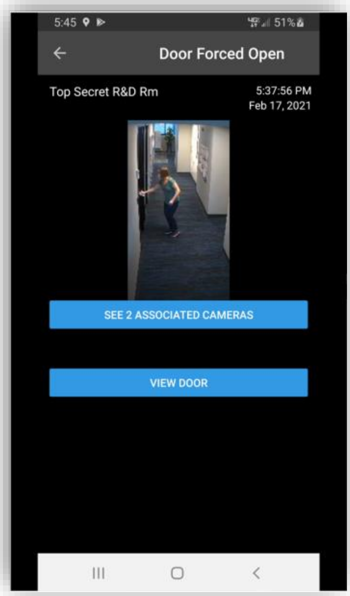


Filter for specific doors or select a door to view cameras associated to that door or interact with commands available for the selected door. Swipe to switch between cameras when multiple cameras are associated to a door.



Door Closed, Door Locked
Updated on: Feb 17, 2021 5:41:35 PM

Switch between Doors, Events, and Access Requests. Select an event from the event list to view still images associated to the event and playback video related to the event. Filter the event list.



Top Secret R&D Rm
5:37:56 PM
Feb 17, 2021

Access requests are only visible if the Smart Client profile assigned to the role of the current user includes the ability to view access requests.

Alarm Acknowledgement

Bi-directional alarm/event acknowledgment is supported between XProtect and CCure 9000.

⚠ In systems using the XProtect Access integration with CCure and the Video Push CCure integration – XProtect analytics alarms generated by the Video Push CCure integration only support automatic acknowledgement if they are acknowledged in the CCure Monitoring Station application, and the "Auto-acknowledge alarms" option was selected in the CCure event definition. Acknowledging analytics alarms in the XProtect Smart Client will not automatically acknowledge the alarms in the CCure system.

CCure 9000 to XProtect

- When a CCure 9000 event is acknowledged, if an alarm was triggered in XProtect for that event, the XProtect alarm will be acknowledged.

XProtect to CCure 9000

- When an alarm is acknowledged in XProtect, the associated event in CCure 9000 that triggered the alarm will be acknowledged.

For automatic Bi-directional alarm acknowledgement to function, there are specific conditions which must be met:

- The CCure 9000 event must have triggered the alarm in XProtect.
  - Check the Access Control tab, and the Events list, in the Smart Client to view the event.
  - Verify the Access Control Event Category used in the Alarm Definition in XProtect Management Client matches the category assigned to the event in the Access Control Events list.
- The source of the alarm must correspond to the source exposed by the integration. For some CCure 9000 events, a door will be used as the source. For other events, such as user-created events, the CCure 9000 server is exposed as the source. It is required to specify the source in the Alarm Definition in XProtect.
  - The source of each event is listed in the Access Control tab's Event list in the Smart Client.

- The CCure event must be configured to require acknowledgment and must not be in a state that prevents acknowledgement, such as “Latched.”
  - Verify individual Event details in the Configuration menu of the Administration Workstation application for the CCure 9000 system.

When using the XProtect Smart Client’s Alarm Manager tab, right-click an alarm, and select either Acknowledge. The associated CCure 9000 event will be acknowledged.

⚠ Acknowledging an alarm in XProtect will acknowledge the alarm in CCure. Closing an alarm in XProtect will not acknowledge the alarm in CCure 9000. Only “acknowledgement” of the alarm in XProtect will impact the alarms status in CCure 9000.

Logging

Logs are enabled for the Milestone Event Server plugin and the CCure 9000 ACM Server, but they are set at the “Info” level by default when installed. The detail level of the logs can be increased for diagnostics purposes, but be aware that this change causes more information to be logged, thus consuming extra disk space and possibly slowing down operations on busy servers.

⚠ Do not leave logs configured at increased detail levels. This level of detail should only be used for diagnostic purposes and returned to default afterwards.

Gathering logs

Milestone

1. Go to the Milestone Event Server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Log files are in these locations:
   a. C:\ProgramData\VideoOS\ACMServerPlugin
   b. C:\ProgramData\Milestone\XProtect Event Server\logs

CCure 9000

1. Go to the CCure 9000 server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Log files are in these locations:
   a. C:\ProgramData\VideoOS\ServiceHost\logs
   b. C:\ProgramData\VideoOS\ServiceHost\Services\VIdeoOSACMServerService\logs
   c. C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService\Plugins\CCure9kAcmServerPlugin\logs

Changing logging level

The log file's level of detail can be changed by setting the logging level. The logging level can be set at any of the following values:

- Off
- Fatal
- Error
- Warn
- Info
- Debug
- Trace

"Off" writes no information to the file and "Trace" writes as much information as possible to the file. The default setting is "Info." New log files are created each day. After 10 days the files are automatically deleted. Here is the procedure to change the log levels:

Milestone

1. Go to the Milestone Event Server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Open the following folder:
   a. C:\ProgramData\VideoOS\ACMServerPlugin
4. In each subfolder named with a globally unique identifier (GUID) – something like "4c53f6e5-e951-1616-83f0-e44fb813e451") do the following:
   a. Find the file named "ACMServerPluginNLog.xml" and open it with notepad.
   b. Near the end of the file is a line like this <logger name="*" minlevel="Info" writeTo="mainlog"/>
   c. Change the "Info" to "Debug" or "Trace," or any of the other log levels and save the file.
   d. Depending on the OS it may be necessary to save the file to the desktop and copy it back to that folder because Windows account permissions don't allow saving a file at that location directly.

CCure 9000

1. Go to the CCure 9000 Server.
2. Open File Explorer. Select the View menu and enable Hidden items.
3. Open the following folder:
   a. C:\ProgramData\VideoOS\ServiceHost
   b. Find the file named "ServiceHostNLog.xml" and open it with notepad.
   c. Near the end of the file are several lines starting with "<logger name="*"
   d. Locate the following lines:
      i. <logger name="CCure9kAcmServerPlugin.*" minlevel="Info" writeTo="ccurelog" final="true" />
      ii. <logger name="Milestone.CCure9k.Client.*" minlevel="Info" writeTo="ccurelog" final="true" />
   e. Change the "Info" to "Debug" or "Trace," or any of the other log levels and save the file.
   f. Depending on the OS it may be necessary to save the file to the desktop and copy it back to that folder because Windows account permissions don't allow saving a file at that location directly.
4. Go to the CCure 9000 Server.

5. Open the following folder:
   a. C:\ProgramData\VideoOS\ServiceHost\Services\VideoOSACMServerService
   b. Find the file named VideoOSACMServerAsmScannerNLog.xml and open it with notepad.
   c. Near the end of the file is a line like this <logger name="*" minlevel="Info" writeTo="mainlog" />
   d. Change the "Info" to "Debug" or "Trace," or any of the other log levels and save the file.
   e. Depending on the OS it may be necessary to save the file to the desktop and copy it back to the that folder because Windows account permissions don't allow saving a file at that location directly.

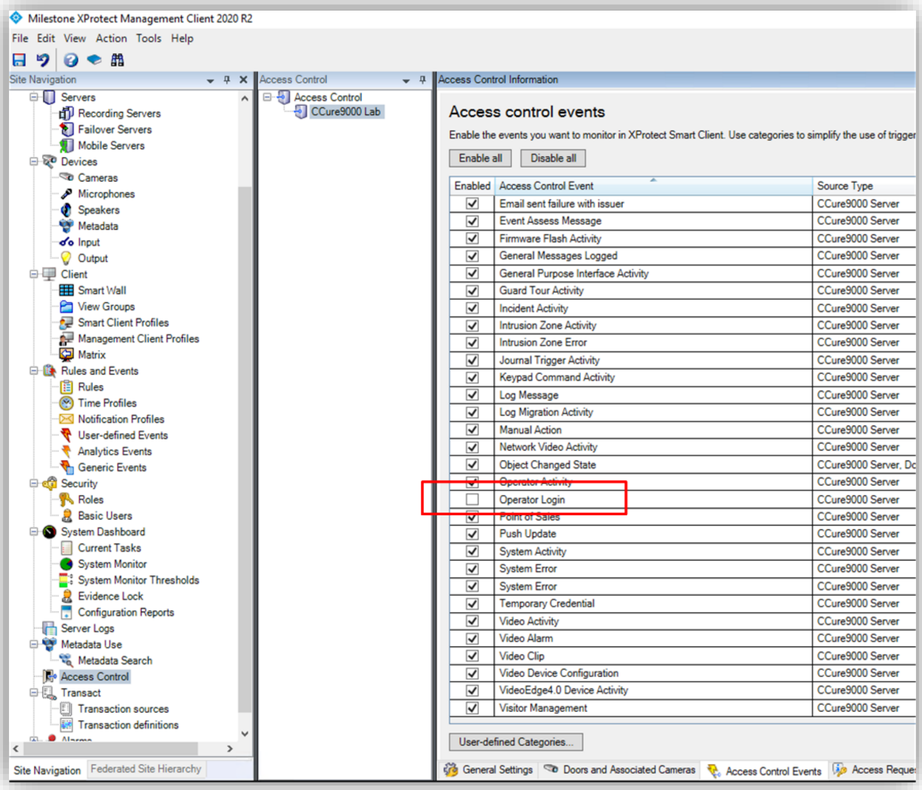
Troubleshooting Guide

Upgrading from 1.1 to 1.2 with Operator Login events.

For integrated systems upgrading from version 1.1 of the XPA plugin to the 1.2 version, the default behavior of the CCure 9000 Operator Login event has been changed. This event was monitored by default in the 1.1 version but is not monitored by default in 1.2.

To check status of this event:

1. Open the XProtect Management Client and select the Access Control Events tab of the XPA instance.
2. Scroll down to find the event titled: Operator Login



Access control events

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

Enabled	Access Control Event	Source Type
☑	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
☑	Guard Tour Activity	CCure9000 Server
☑	Incident Activity	CCure9000 Server
☑	Intrusion Zone Activity	CCure9000 Server
☑	Intrusion Zone Error	CCure9000 Server
☑	Journal Trigger Activity	CCure9000 Server
☑	Keypad Command Activity	CCure9000 Server
☑	Log Message	CCure9000 Server
☑	Log Migration Activity	CCure9000 Server
☑	Manual Action	CCure9000 Server
☑	Network Video Activity	CCure9000 Server
☑	Object Changed State	CCure9000 Server, Dc
☑	Operator Activity	CCure9000 Server
☐	Operator Login	CCure9000 Server
☑	Point of Sales	CCure9000 Server
☑	Push Update	CCure9000 Server
☑	System Activity	CCure9000 Server
☑	System Error	CCure9000 Server
☑	System Error	CCure9000 Server
☑	Temporary Credential	CCure9000 Server
☑	Video Activity	CCure9000 Server
☑	Video Alarm	CCure9000 Server
☑	Video Clip	CCure9000 Server
☑	Video Device Configuration	CCure9000 Server
☑	VideoEdge4.0 Device Activity	CCure9000 Server
☑	Visitor Management	CCure9000 Server

It has been observed, on some systems, that many events are generated. To avoid this behavior, the decision was made to leave this event out of the default list of events which the XPA integration monitors.

However, this default behavior only changes on newly created XPA instances. Therefore, if an upgraded system is receiving many Operator Login events and the behavior must stop being monitored, it is required to disable Operator Login events and save the configuration. Otherwise, this change in the default behavior will not impact an upgraded system.

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

If XProtect is unable to communicate with the CCure 9000 ACM instance, the instance will not appear in the Access Control section of the Management Client. Do the following steps in the following order:

1. Close the Management Client and Smart Client
2. Stop the Milestone Event Server
3. Stop the Milestone ACM Service
4. Ensure CCure 9000 is running successfully. This may require restarting services.
5. Start the Milestone ACM Service
6. Start the Milestone Event Server and wait for it to fully start.
7. Start the Management Client

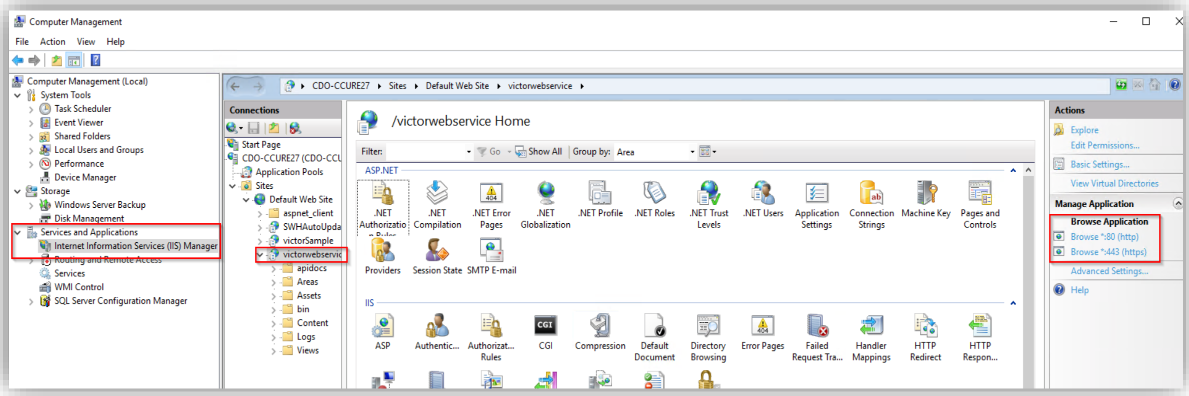
If the instance still does not appear in the Management Client, investigate the logs (see Logging) to discover the specific cause.

CCure 9000 ACM Integration looking for secure connection with victor web service

- This symptom should only occur with XPA integrations using CCure 9000 systems which are version 2.80 or lower. Versions 2.90 and higher have fixed this issue.

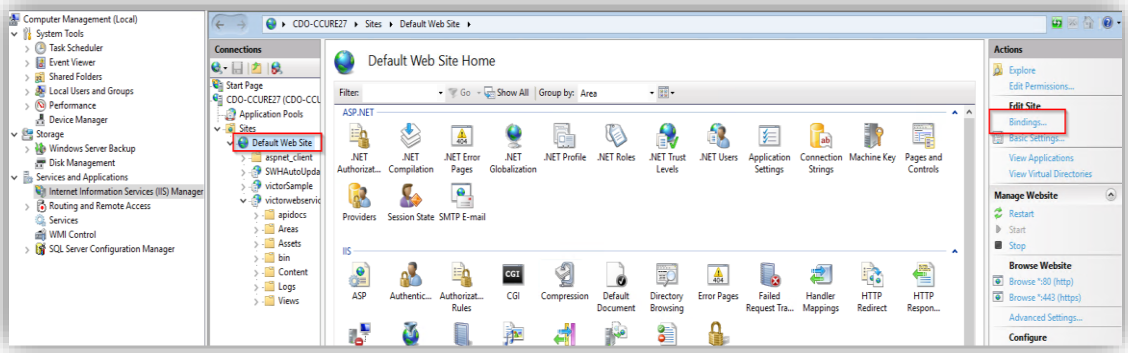
A certificate must be provided and configured in IIS for the CCure 9000 victor web service to accept secure HTTPS connections on port 443. Contact CCure 9000 engineering and support resources to verify the CCure 9000 system is configured to enable secure communications.

Check if the port number (443) is configured to work with HTTPS on the CCure 9000 server. Go to the CCure 9000 server. From the Start menu open the Windows Administrative Tools application and open the Computer Management menu.

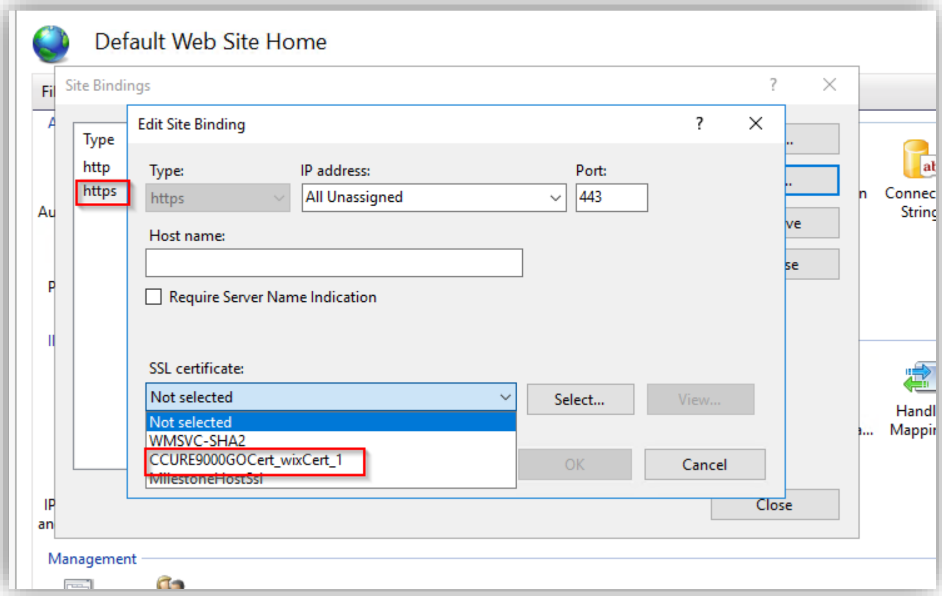


Select the Services and Applications directory and the Internal Information Services (IIS) Manager menu. Expand the IIS Manager directory on the local server to find the “victorwebservice” website. Click on the “browse *.443” link to validate if HTTPS is working. This opens a browser and authenticates using TLS at the specified URL. If it’s blocked, the port is not setup.

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



Then right click on Type https (port 443) and select Edit. Open the SSL certificate list and select the appropriate certificate. The certificate allows authentication using secure ports (443).



Type: https

IP address: All Unassigned

Port: 443

Host name:

☐ Require Server Name Indication

SSL certificate: Not selected

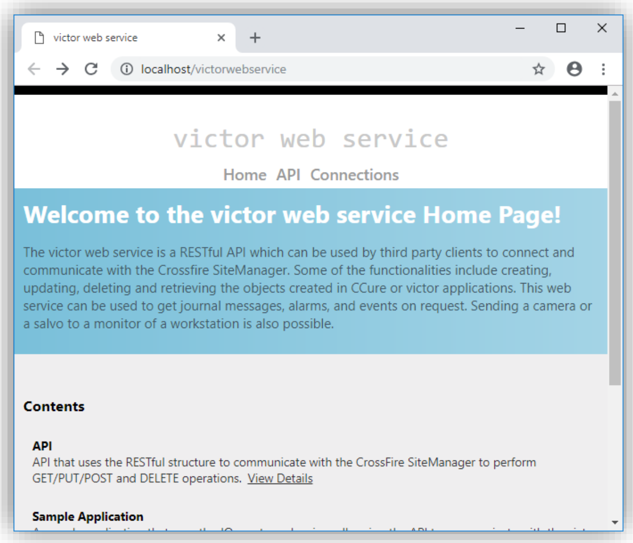
- Not selected
- WMSVC-SHA2
- CCURE9000GOCert_wixCert_1
- MilestoneHostSsl

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. Follow these steps to make sure the CCure 9000 victor web service is correctly started and accepts requests:

- Go to the CCure 9000 server.
- Open a web browser and go the address below:
  - http://localhost/victorwebservice/

- If the browser opens a page similar to the one below. Everything is okay with the victor web-service.



Welcome to the victor web service Home Page!

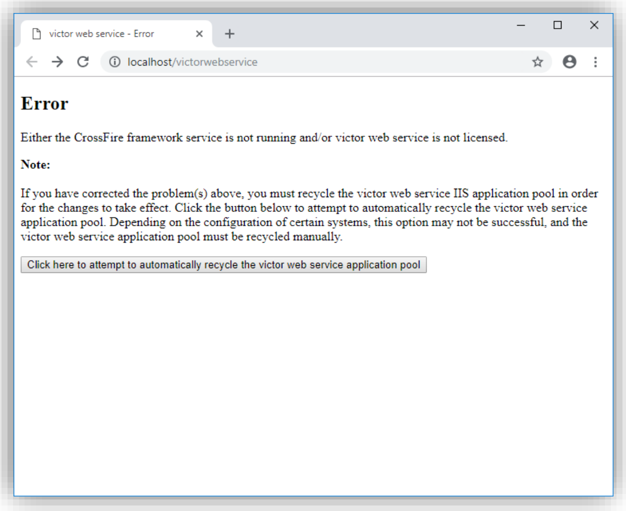
The victor web service is a RESTful API which can be used by third party clients to connect and communicate with the Crossfire SiteManager. Some of the functionalities include creating, updating, deleting and retrieving the objects created in CCure or victor applications. This web service can be used 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 the browser leads to an error message similar to the one seen below, click the button shown on the page 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:

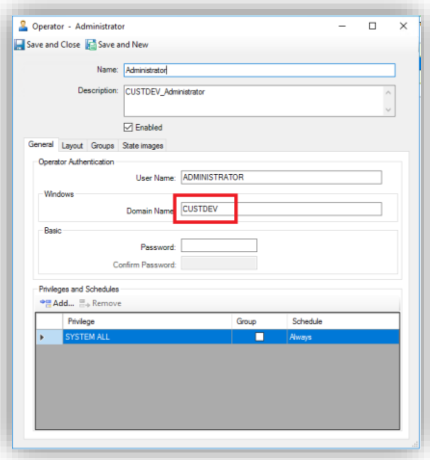
If you have corrected the problem(s) above, you must recycle the victor web service IIS application pool in order for the changes to take effect. Click the button below to attempt to automatically recycle the victor web service application pool. Depending on the configuration of certain systems, this 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

Login fails with CCure 9000 when using a multipart domain user

The default Operator created during CCure 9000 installation will only retain the first part of a multipart domain name.

For example, if CCure 9000 is installed using the Administrator user on the *CUSTDEV.US* domain, only the *CUSTDEV* part of the domain will be kept in the Operator definition - the *.US* part will be lost. Trying to login using the full domain name (*CUSTDEV.US*) won't work. The same exact domain name protocol must be used in both places for login to succeed.



Name: Administrator

Description: CUSTDEV_Administrator

☑ Enabled

Operator Authentication

User Name: ADMINISTRATOR

Windows

Domain Name: CUSTDEV

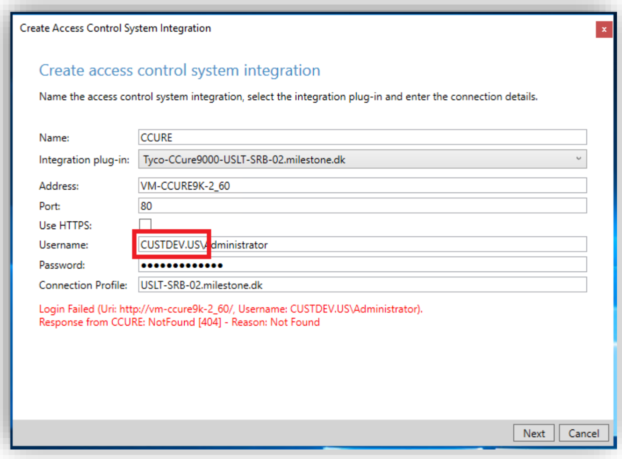
Basic

Password:

Confirm Password:

Privileges and Schedules

Privilege	Group	Schedule
SYSTEM ALL	□	Always



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

Smart Client System Error with StateCode: LicensedQuantityReached

A system error can occur in CCure with the following error code:

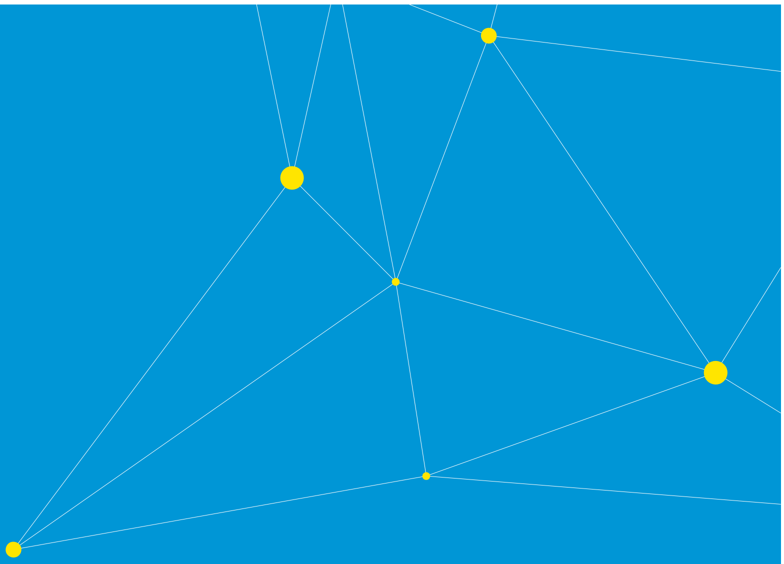
LicenseQuantityReached

“The option Milestone XProtect Corporate is licensed for 1 connections and that limit has been exceeded.”

This error is caused by a known bug in versions of CCure equal or prior to 2.70 SP5 and 2.80 SP1 that prevents the integration from connecting more than once to the CCure Victor Web Service. The integration has been modified to recover from this error automatically when it occurs, but the recommended solution is to update CCure to a service pack higher than the two above-mentioned versions.

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.