MAKE THE
WORLD SEE

Milestone Systems

XProtect Access for CCure 9000

Manual

milestone

Contents

Copyright, trademarks, and disclaimer

Trademarks

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

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

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

Disclaimer

This text 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 reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text 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 system installation folder.

Introduction

Feature list

This document describes specifics to the XProtect Access integration between Milestone XProtect and the CCure 9000 access control (AC) system. This integration supports the following 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 link user privileges from CCure to the access control hardware, events, and alarms available in the Smart Client
- Detailed 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
- Support for third-party SSL certificates to secure XProtect Access service communications
- View and interact with access control devices on the Smart Map.

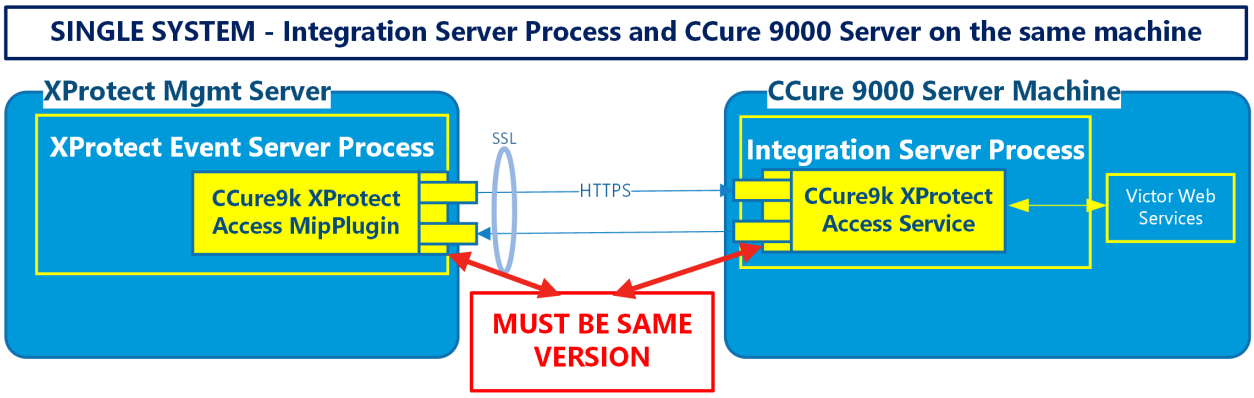
Solution overview

The integration software download is a single context sensitive installation program. This program name is:

XProtectAccess.CCure9k.msi

When this program runs it identifies the software installed on the local server, CCure 9000 or XProtect, and it helps install the required software. One of these two options are presented:

1. The CCure XProtect Access Service that runs on the CCure 9000 server.
2. The CCure XProtect Access MipPlugin that runs on the XProtect server.



Whats new in version 1.5?

The most prominent changes to version 1.5 of the CCure 9000XProtect Access integration are listed below.

Support & Requirements:

- Support for CCure version 3.10
- CCure 9000 and XProtect version support statement: CCure 9000 & XProtect Compatibility.

Features & User Experience:

- Durable subscription support added to improve the resiliency of the data connection stream between CCure and XProtect.

Software version compatibility

The latest version of CCure 9000 - version 3.10 - is only supported by the most recent version of the XProtect Access integration - version 1.5.

Version 3.0 of the CCure 9000 software is not supported by any version of the XProtect Access integration. Older versions of the integration (1.3 and below) do not support CCure 9000 versions 3.00.1 or higher.

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 XProtect Access suite of functionality.

The most up to date compatibility information is located here: https://download.milestonesys.com/ccure9kxpa/

Please confirm you have met the license requirements, and verify the version of CCure 9000 you are running is compatible. Milestone always recommends that you run the latest compatible versions of both CCure 9000 and XProtect.

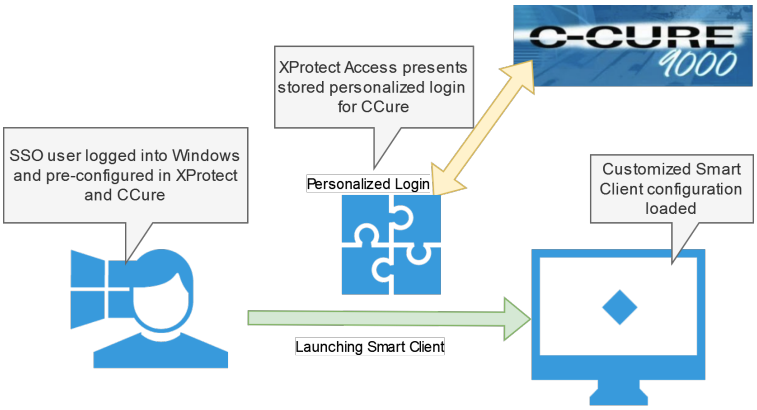
Cardholders

The CCure 9000 XProtect Access 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.

XProtect Access and SSO authentication (explained)

XProtect single sign-on (SSO) does not delegate SSO to the CCure system. XProtect SSO uses the logged in Windows user, and it cannot automatically present that same user to CCure for authentication. The personalized login feature of XProtect Access is how XProtect presents unique credentials for authentication with CCure.

These personalized login credentials can match a user with SSO in CCure. They can even be the same user logged into Windows who is launching the Smart Client. However, the credentials must be entered at the first login of the Smart Client, and re-entered if the credentials are changed in CCure. Then a user can log into Windows, launch the Smart Client, which automatically authenticates with XProtect via SSO. At this point the stored credentials for the personalized login user that matches the XProtect user are presented to CCure and the CCure user's configuration is loaded into the Smart Client. This can all be done without manually presenting any credentials to XProtect or CCure.

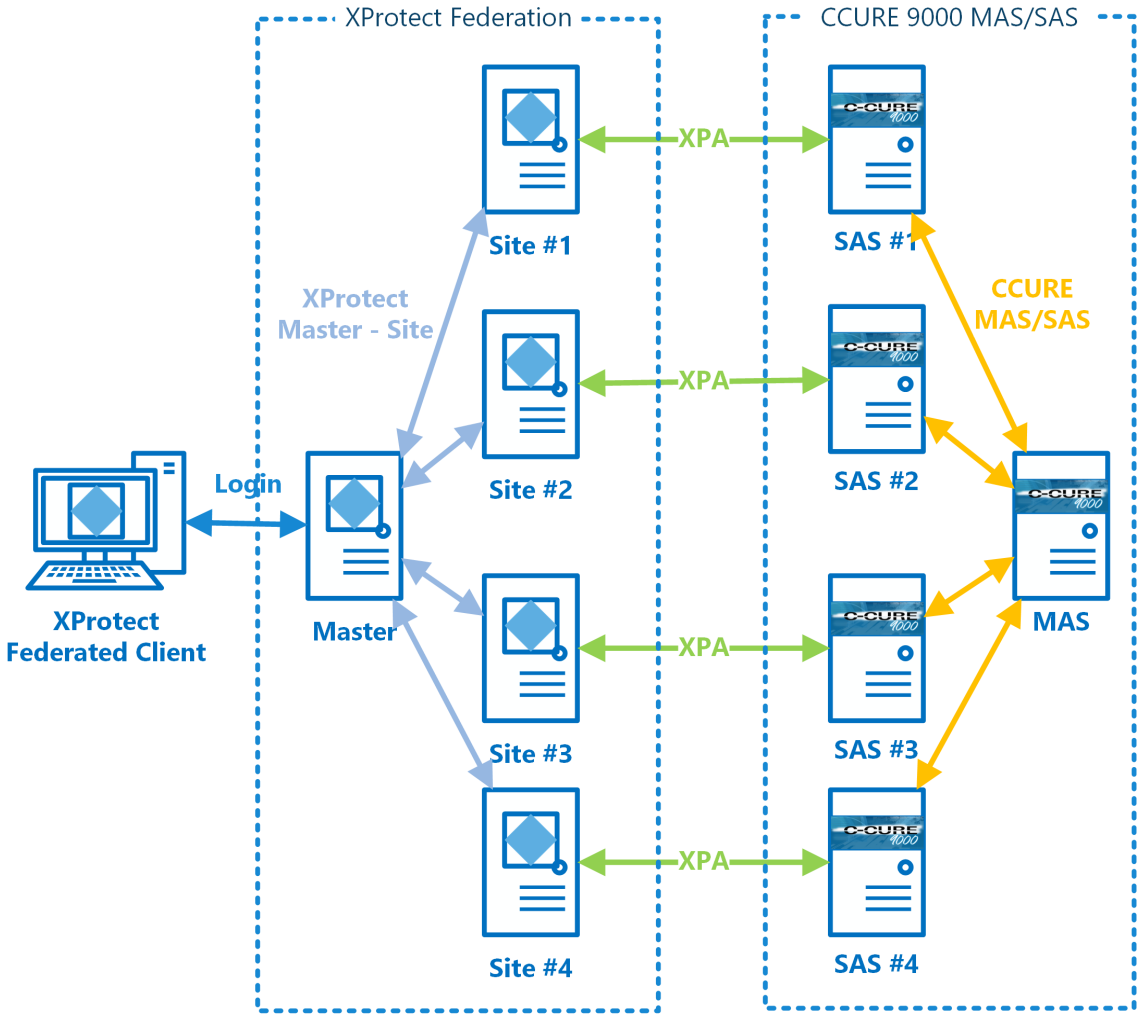


This is the closest to a true SSO user experience that the XProtect Access integration offers. It requires using the personalized login feature. If this feature isn't used, all authentication to CCure from XProtect Access uses the same user credentials that the CCure XProtect Access Service uses to refresh and fetch the configuration from CCure. To utilize this partial SSO user experience with customized privileges, it's important to link XProtect users and roles directly to the appropriate SSO users within CCure.

System Design

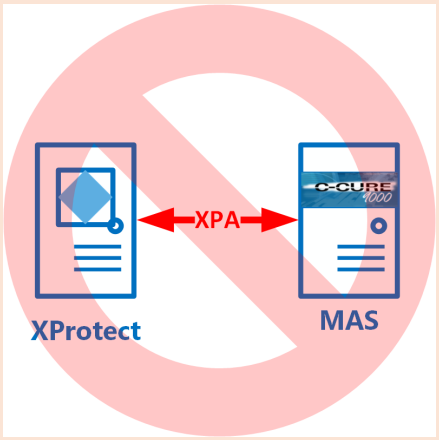
CCure 9000: Enterprise (MAS/SAS) configuration

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.

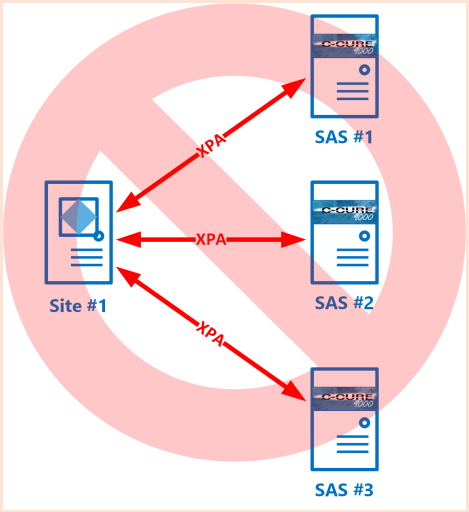


CCure 9000 Enterprise scenarios require that each CCure 9000 Satellite Application Server (SAS) installation has a maximum of one corresponding Federated XProtect site that connects to it. Each XProtect site, for performance reasons, should never have more than one CCure 9000 Satellite Application Server (SAS) connected. CCure 9000 Enterprise scenarios also require that no connection is directly made to a Master Application Server (MAS).

MAS-DIRECT NOT SUPPORTED



ONE-TO-MANY NOT SUPPORTED



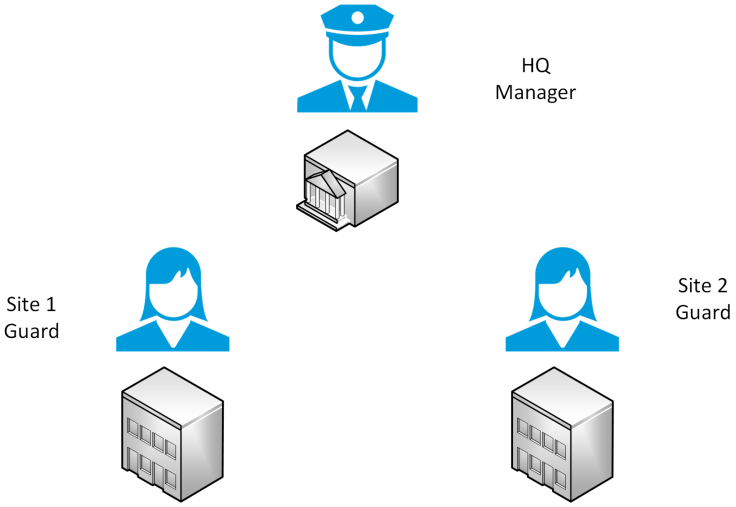
CCure 9000 partitions (explained)

Personalized login can control which devices, events, and alarms users can view in the Smart Client when integrated with partitioned CCure 9000 systems. A partitioned CCure system uses logical groupings, known as partitions, to define which access panels, readers, cardholders, and users work together.

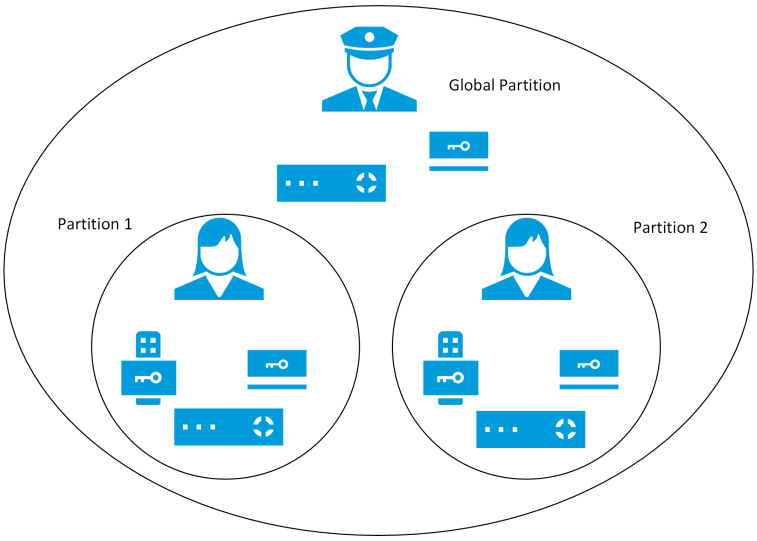
> CCure 9000 requires an Enterprise CCure system to use partitions. Creating a partitioned system within CCure 9000 shouldn't be a part of installing the XProtect Access CCure integration. It's recommended to consult with an authorized CCure representative before configuring partitions or moving to an Enterprise system.

Each application server can manage a subset (one or more partitions) of the devices and personnel contained in the database.

Illustrated below is an organization with three sites, a head quarters, site 1, and site 2.



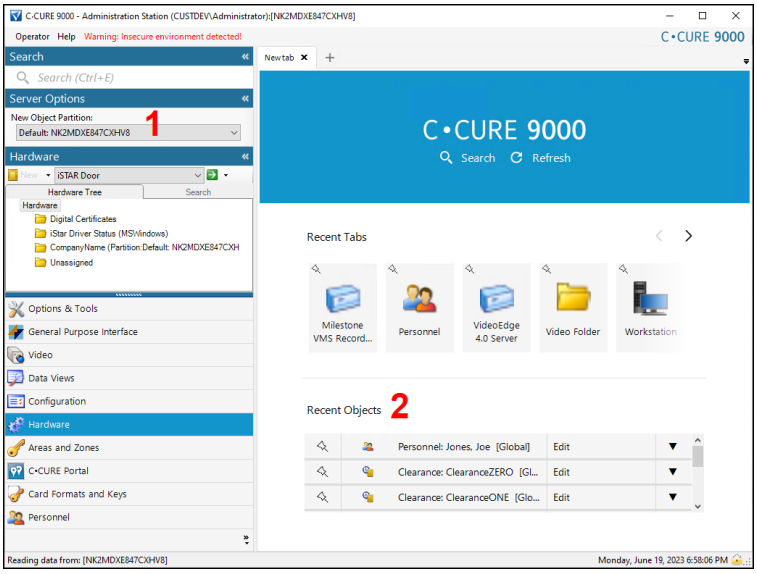
Using partitions, the guard user at site 1 can see readers, panels, and cardholders from partition 1, and the guard user from site 2 can see the devices and information from partition 2. The manager can see all devices and information, since they're in the default "Global" partition.



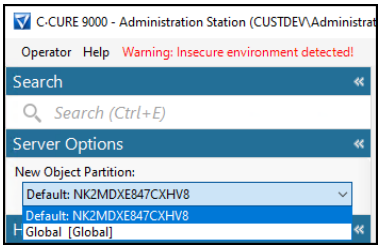
Configuring partitions in CCure

> The following process shows where the information about existing partitions exists within a CCure 9000 system. Please consult with your CCure representative before configuring partitions in an operational CCure system.

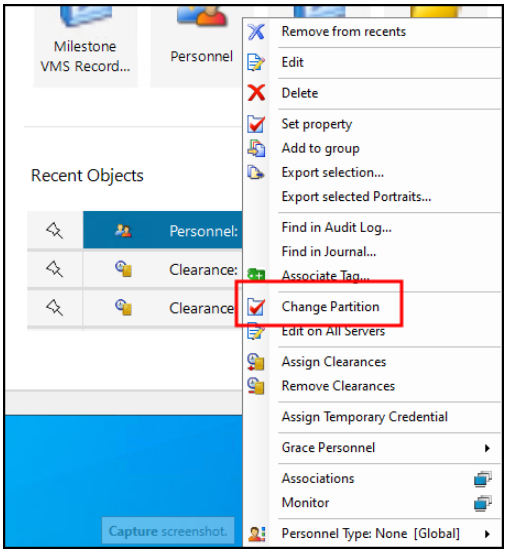
The default interface has several menu options that show information about current partitions.



1. The **New Object Partition** menu allows filtering the client's menus, options, and user privileges based on the selected partition.

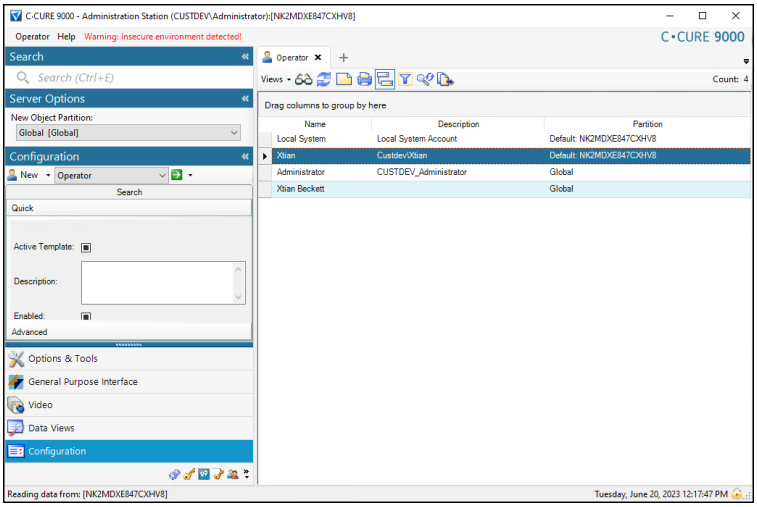


2. Any menu option that provides the operator the ability to interact with individual objects, devices, or personnel can have options for that object's partition.



Mapping users to partitions in CCure

1. Go to the Configuration tab in the Administration Station and search for operators in the chosen partition.

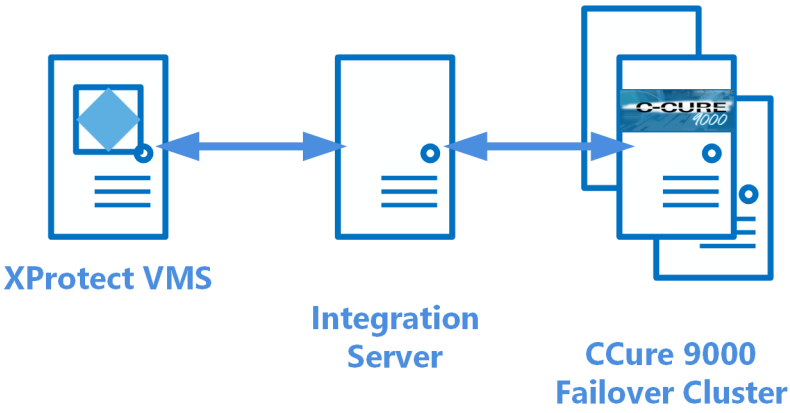


2. Add new users, Domain users, and assign partitions.

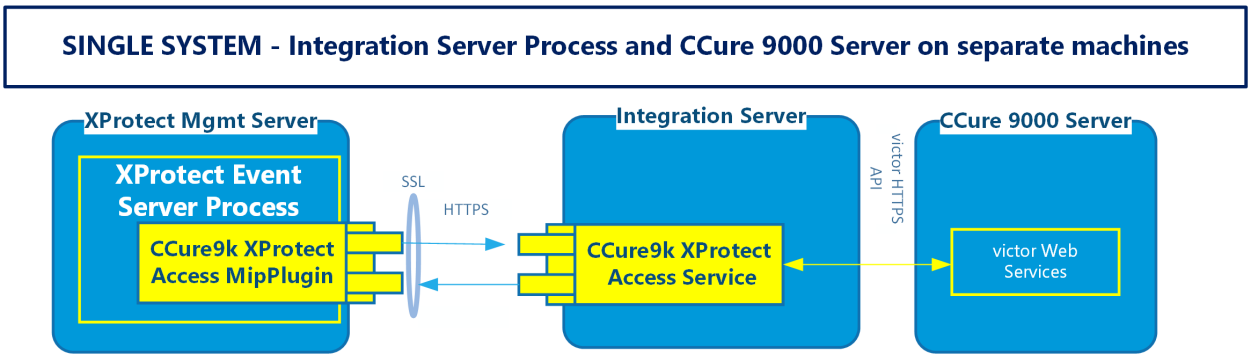
It's recommended to map users logically from your domain, to XProtect, to CCure and to their partition. This lets SSO in XProtect work with the personalized log-in feature, and with partitions within CCure, to simplify the log-in experience, while also customizing and controlling the integrated Smart Client.

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 Milestone CCure XProtect Access Service will need to be installed on a different server in the same network, a server that we will refer to as an integration server.



In this scenario it is possible to configure the integrated system with a separate server as the host for the XProtect Access service.



Failover clustering is not the only scenario that may require installing the integration components 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

Required system configurations

Below is a list of required configurations to support the integration between CCure 9000 and XProtect.

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.

.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.

CCure 9000: victor web service installation

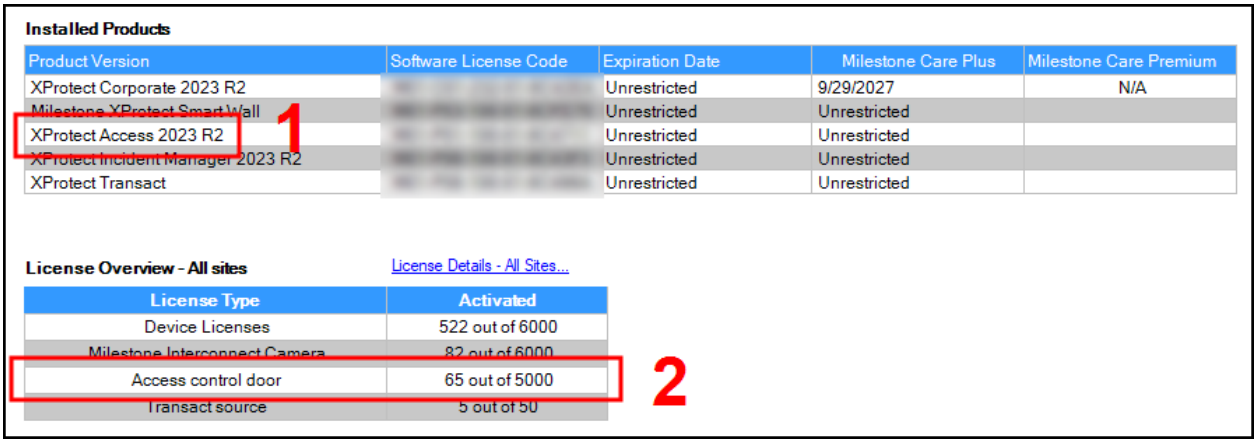
The CCurevictor web service must be installed and configured on the CCure 9000 server. Please follow the Victor Web Service User Guide provided by CCure. The CCure 9000victor web service installer can be obtained by downloading the “CCURE 9000 v2.XX Web Service Package” from the CCure download site, or installing it from the CCure 9000.ISO installation package used to install the access control system.

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 9000victor web service to accept secure HTTPS connections on port 443). See the CCure 9000 XProtect Access integration looking for secure connection with victor web service on page 90 troubleshooting topic for more details.

Milestone XProtect®: license options

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

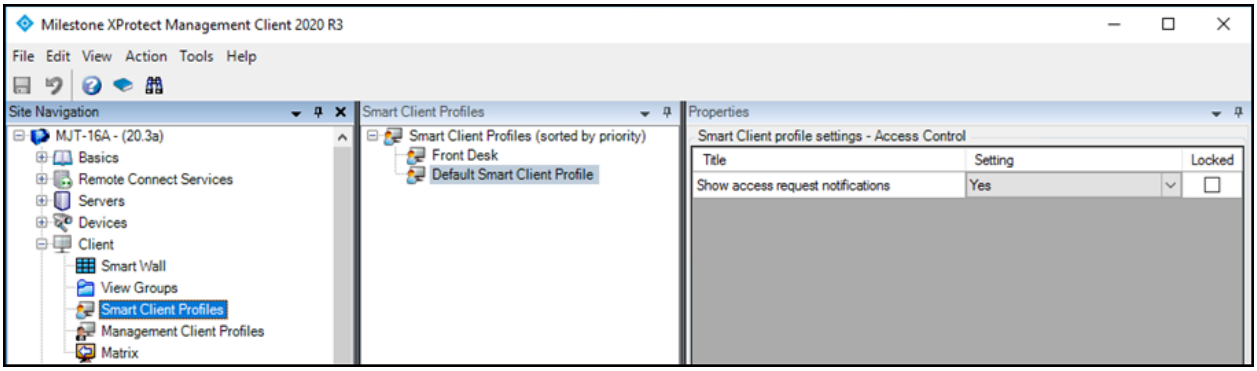


XProtect Smart Client profiles

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 request notifications with the Smart Client.



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.

CCure 9000: licenses explained

The CCure 9000 license required to integrate with Milestone XProtect is “Milestone XProtect Corporate” or "Milestone - XProtect Corporate XProtect Access - Integration." This doesn't mean that the only XProtect product that integrates with CCure 9000 is XProtect Corporate. XProtect Corporate, XProtect Expert, and XProtect Professional+ VMS products from Milestone are all tested and supported.

Licenses required for CCure 9000 are subject to change based on the version of software installed. There are two different types of integration licenses that could be used to enable the CCure XProtect Access integration.

1. Milestone XProtect Corporate - SDK license
2. Milestone - XProtect Corporate XProtect Access - Integration - web service API license

Both of these licenses will work. However, current versions of the XProtect Access integration (1.4 or higher) are only compatible with the web service API license. Also, only recent versions of the CCure 9000 software require the web service API license - versions 3.00.1 and higher. Older versions of the integration (1.3 and below) are not compatible with any version of CCure that is 3.00.1 or higher.

There are three different product SKUs used to order the integration license based on the size of the CCure system (the number of readers). These license options apply to all versions of CCure 9000. This applies to both the SDK license and the web service API license.

License SKU	Description
CC9-MSTVD-SM	CCure 9000 Milestone XProtect Corporate Web Service Integration Small, Series L to N (0-64 readers)
CC9-MSTVD-MD	CCure 9000 Milestone XProtect Coporate Web Service Integration Medium, Series P to R (65-999 readers)
CC9-MSTVD-LG	CCure 9000 Milestone XProtect Corporate Web Service Integration Large, Series RP to T (1000+ readers)

XProtect Access uses a permanent connection to the CCure 9000 victor web service (to receive statuses and events) and uses extra connections for specific user operations, such as fetching configuration and executing commands. For optimal operation of XProtect Access, the feature license activated in CCure must support enough concurrent connections to the victor web service to handle the number of XProtect Access permanent and transient connections.

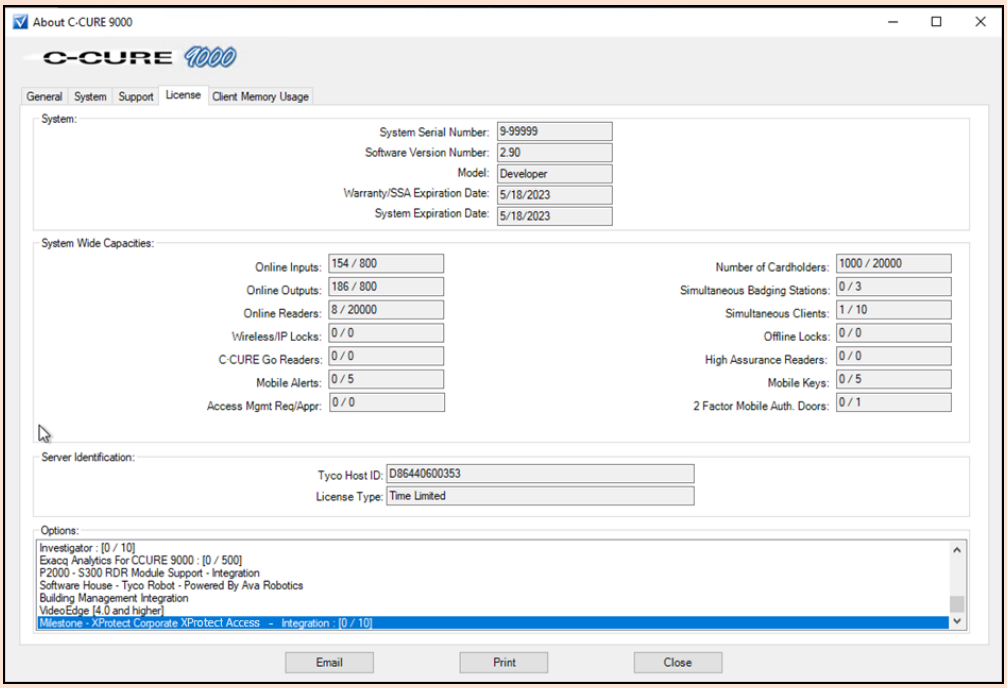
The victor web service is a requirement for the XProtect Access integration with CCure 9000. However, this licensed option is typically included.

CCure 9000 web service API license

In CCure 9000 version 3.00.1 or higher the license requirements change. The only required license is:

- **Milestone - XProtect Corporate XProtect Access - Integration**

This is a web service API license, therefore it includes the victor web service component.

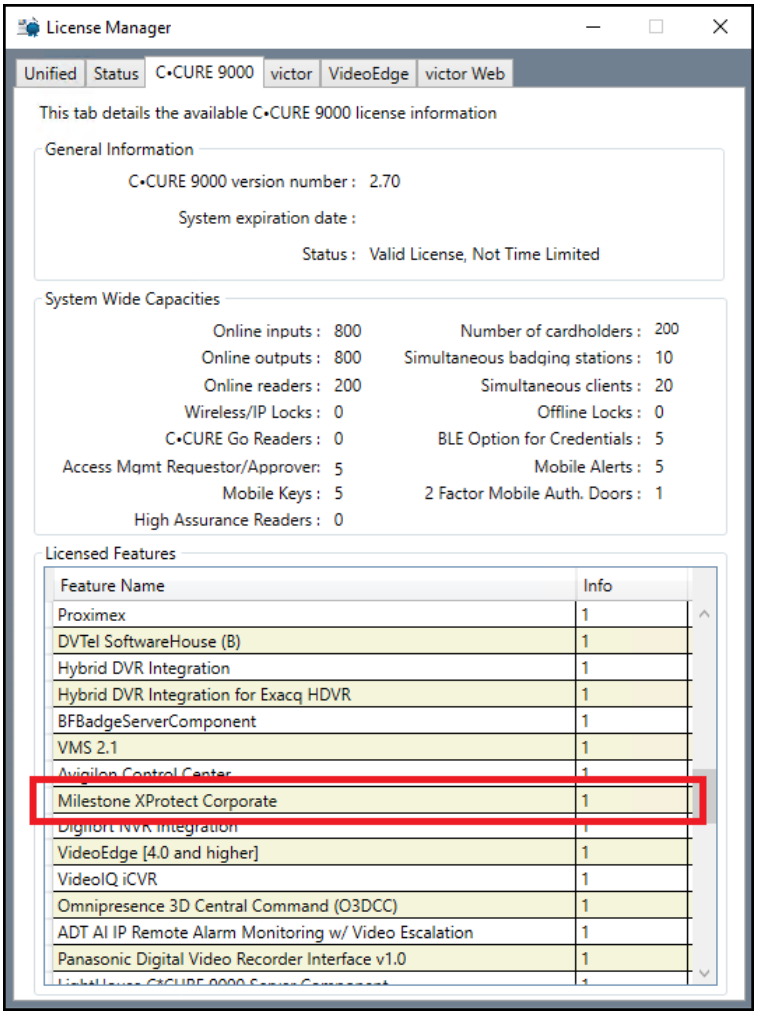


The license must display the available concurrent connections for the web service. [0/10]

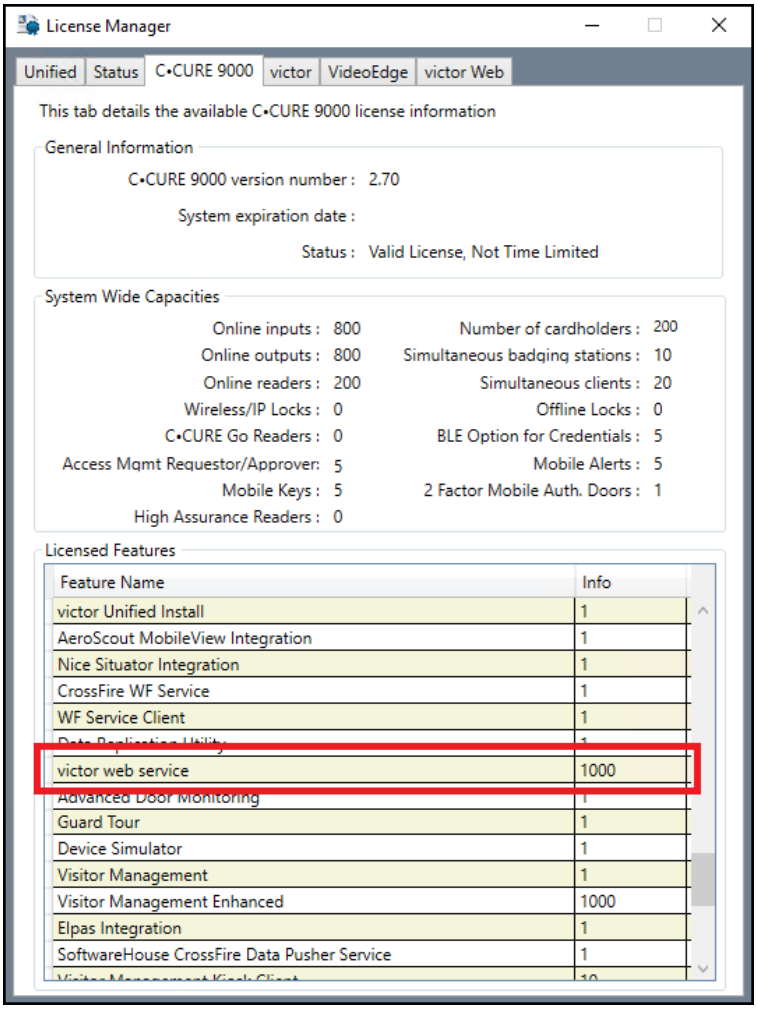
CCure 9000 SDK licenses

There are two feature licenses required in CCure when the SDK license is being used.

1. “Milestone XProtect Corporate” - this is the SDK license.



2. “victor web service” - this license enables the web server functionality to communicate with XProtect Access.


License Manager
Unified
Status
C•CURE 9000
victor
VideoEdge
victor Web
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
victor web service 1000
Guard Tour 1
Device Simulator 1
Visitor Management 1
Visitor Management Enhanced 1000
Elpas Integration 1
SoftwareHouse CrossFire Data Pusher Service 1

Installation

Installation package

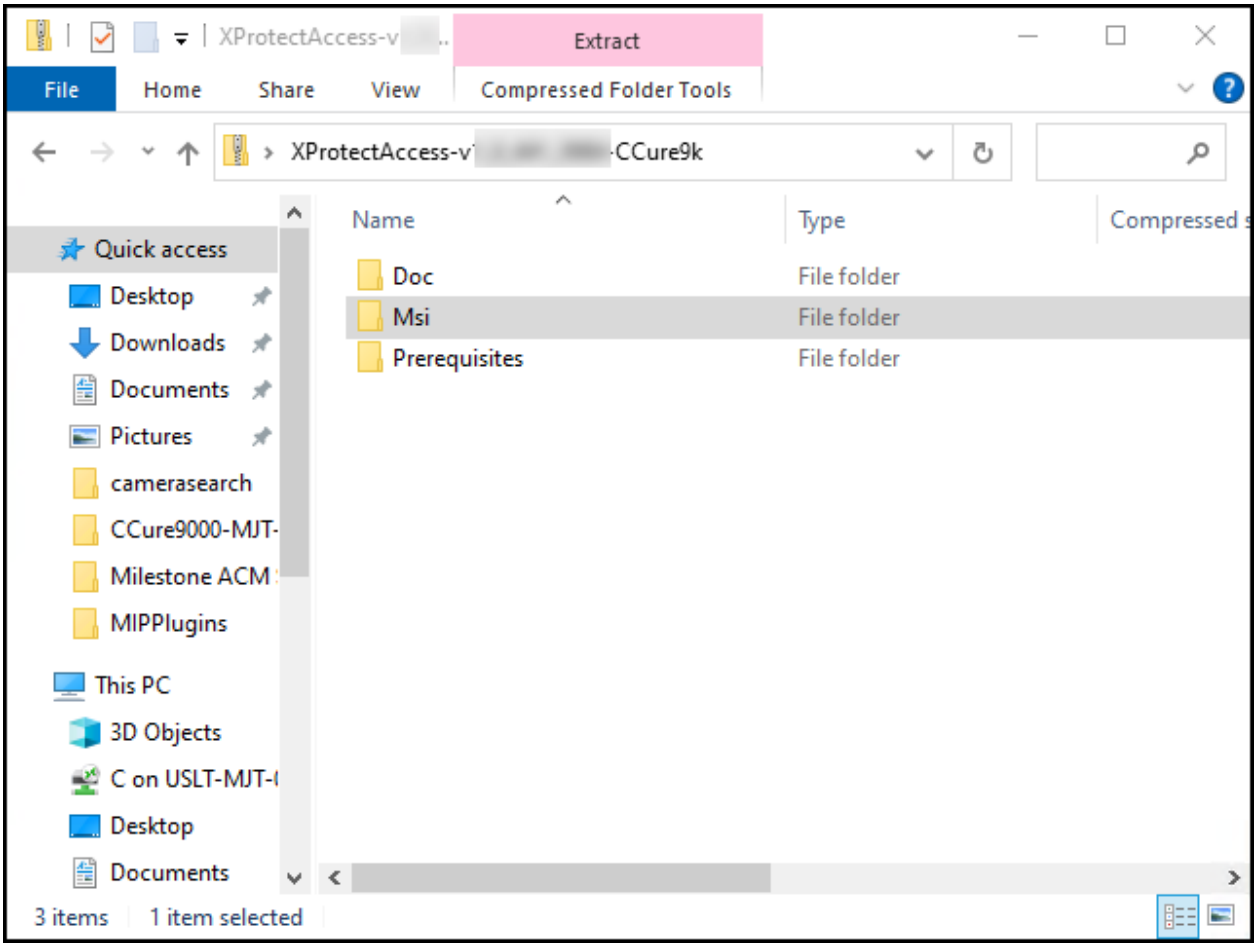
1. Download the most recent version of the CCure 9000 XProtect Access integration from the following location:

   https://download.milestonesys.com/ccure9kxpa/

2. Unzip the installation package.

- The installation package consists of a single installer in the MSI folder, a folder for documentation, and a folder for prerequisites.

:



3. Open the MSI folder to find the XProtectAccess.CCure9k.msi installer program for both the XProtect and CCure 9000 systems.

It is mandatory that the same version of the CCure 9000 XProtect Access integration software components are installed on both the XProtect and CCure 9000 machines.

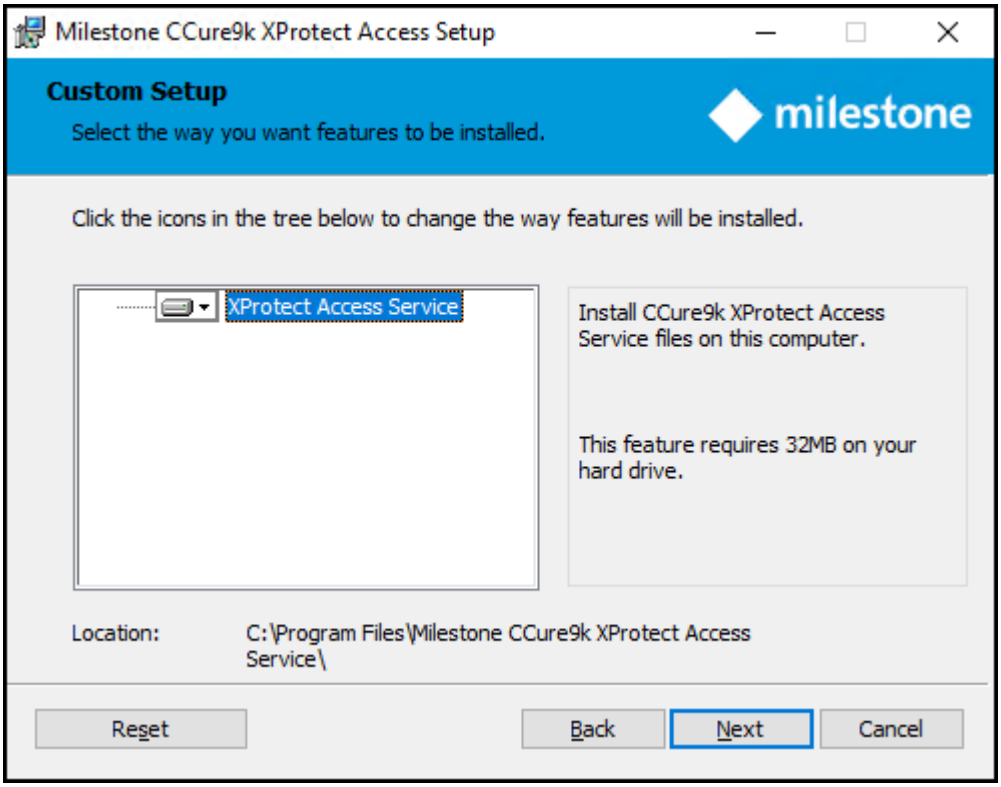
CCure9k XProtect Access Service installation

The process documented here is for when you are installing the XProtect Access Service on the CCure 9000 server. If you are installing the XProtect Access Service on a separate server you will need to consult the CCure9k XProtect Access Service installation on an integration server on page 23 topic.

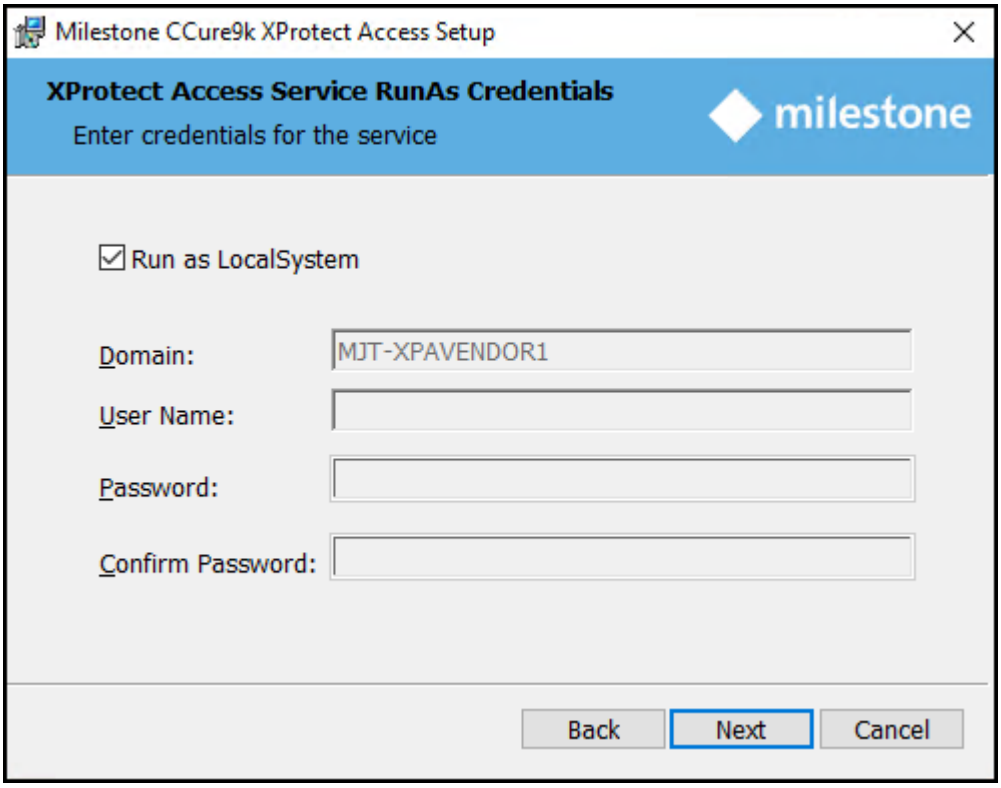
1. Go to the CCure 9000 server, locate the required .msi file to start the installation wizard. The file name is:

- **XProtectAccess.CCure9k.msi**

2. Double-click the installation file. Click **Next** to begin the wizard.
3. At the Custom Setup step of the wizard choose to install the CCure XProtect Access Service.



4. At the **XProtect Access Service RunAs Credentials** step, the default option of **Run as LocalSystem** is used, or remove this option to enter a user name and password for the service. Click **Next** to continue.



5. Click **Install** to install the CCure XProtect Access Service.
6. Finish the installation wizard.

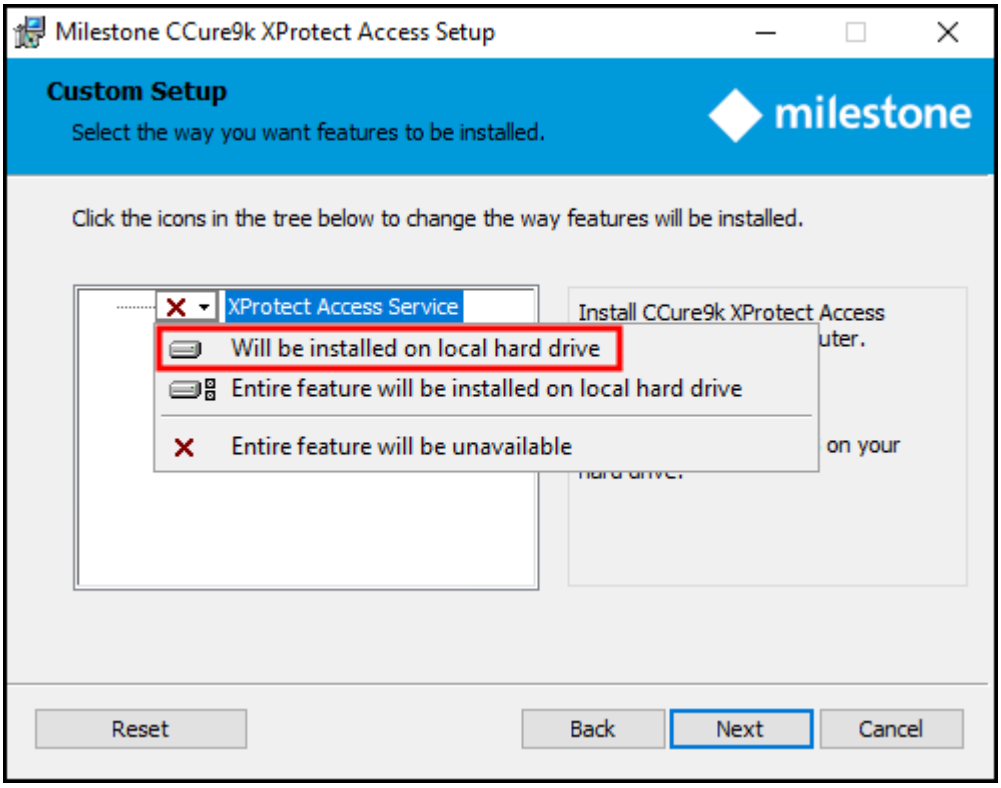
CCure9k XProtect Access Service installation on an integration server

> The process documented here is for installing the XProtect Access Service on an integration server - according to this topic: CCure 9000: Alternate configuration on page 14.

1. Go to the integration server, locate the required .msi file to start the installation wizard. The required file is named:

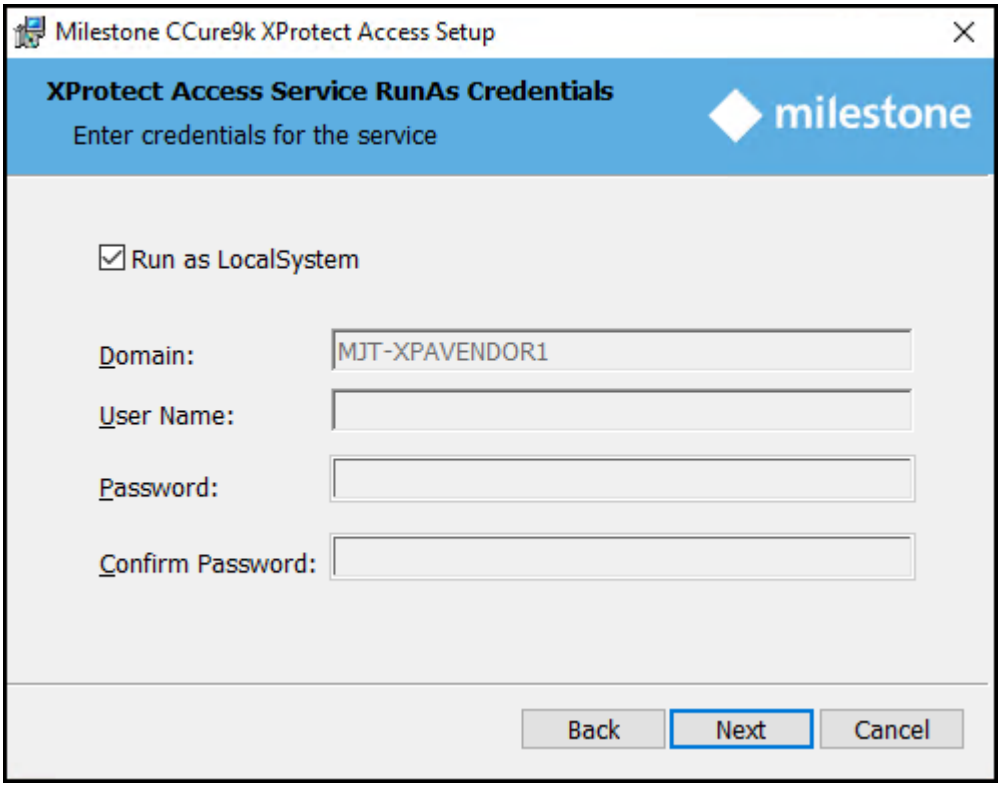
- **XProtectAccess.CCure9k.msi**

2. Double-click the installation file. Click **Next** to begin the wizard.
3. At the Custom Setup step of the wizard expand the XProtect Access Service option and select **Will be installed on local hard drive** to install the CCure XProtect Access Service.



By default, none of the components of the integration will be selected for install. Also, there may be other components listed as available to install at this step. The **XProtect Access Service** component is the only one that should be installed.

4. At the **XProtect Access Service RunAs Credentials** step, the default option is **Run as LocalSystem** is selected. Continue with this option, or enter the credentials of an administrative user with access to both XProtect and CCure. Click **Next** to continue.



5. Click **Install** to install the CCure XProtect Access Service.
6. Finish the installation wizard.

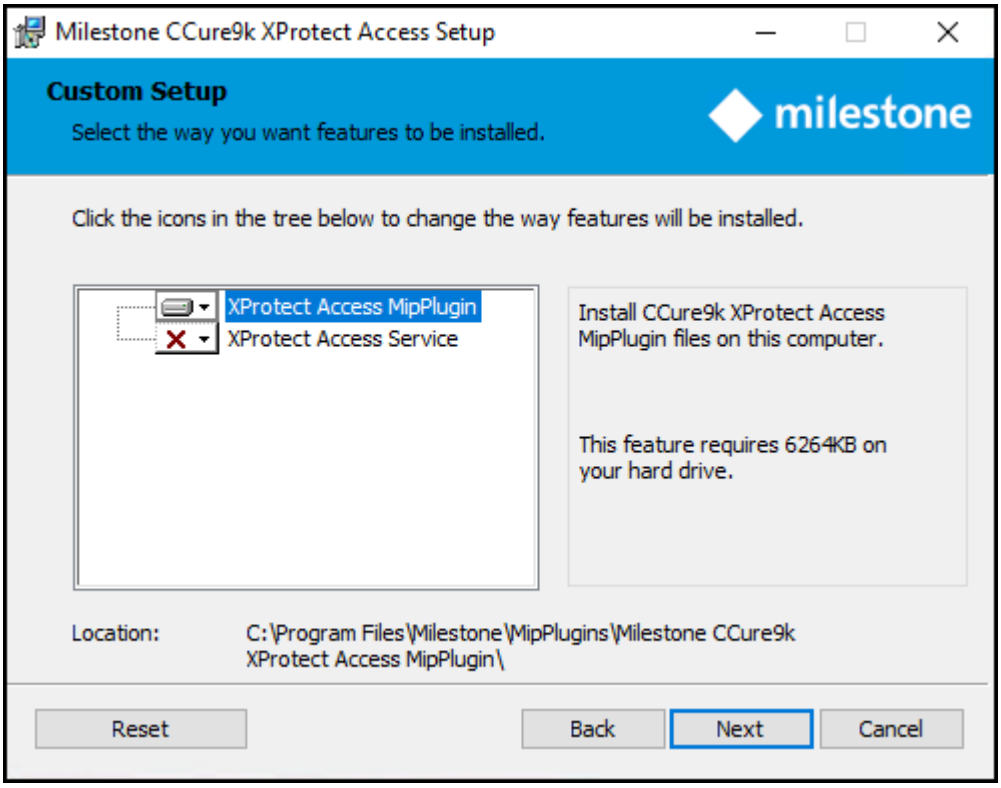
Milestone Server: Installing the CCure9k XProtect Access MipPlugin

In most scenarios, the Milestone XProtect Management Server host server is where this component is installed. However, it is technically required to install this component on the server that hosts the XProtect Event Server.

1. Go to the XProtect Event Server host and locate the required .msi file. The required file is named:

- **XProtectAccess.CCure9k.msi**

2. Double-click the installation file, and click **Next** to begin.
3. At the **Custom Setup** step choose to install the **XProtect Access MipPlugin** and click **Next** to continue.



4. Click **Install** to complete the plugin installation wizard.

MIP Plugin upgrades

Recent CCure 9000 software versions require a different type of license (web service API license) compared to all previous versions (which required an SDK license). These versions are:

- 3.00.1 and all other minor versions 3.00.x
- 3.10

In an existing integrated system, running an older version of the integration (1.3 or below), it is required to first upgrade the integration to the current version, before upgrading the CCure software. Older versions of the integration are not compatible with the new web service license type.

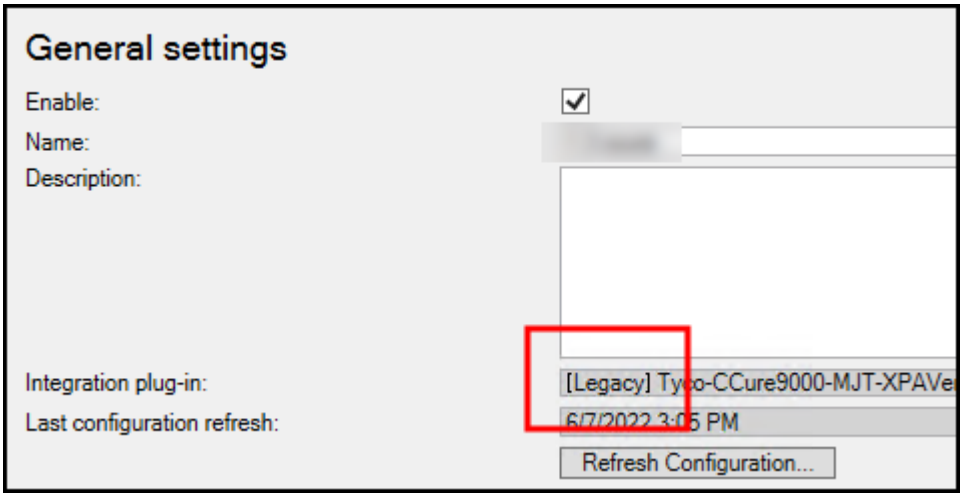
Please read this troubleshooting topic if the CCure system was upgraded and the XPA plugin installation fails.

Always upgrade both the CCure 9000 integration components on the CCure 9000 machine, and the MipPlugin software on the XProtect server. Milestone distributes all component installers with each CCure 9000 XProtect Access integration release. Simply run the installer program on both the CCure 9000 server and the XProtect server; it will upgrade any installed software.

Automatic MipPlugin upgrades of configured and installed instances in the Management Client are also supported for all versions of the CCure 9000 XProtect Access integration.

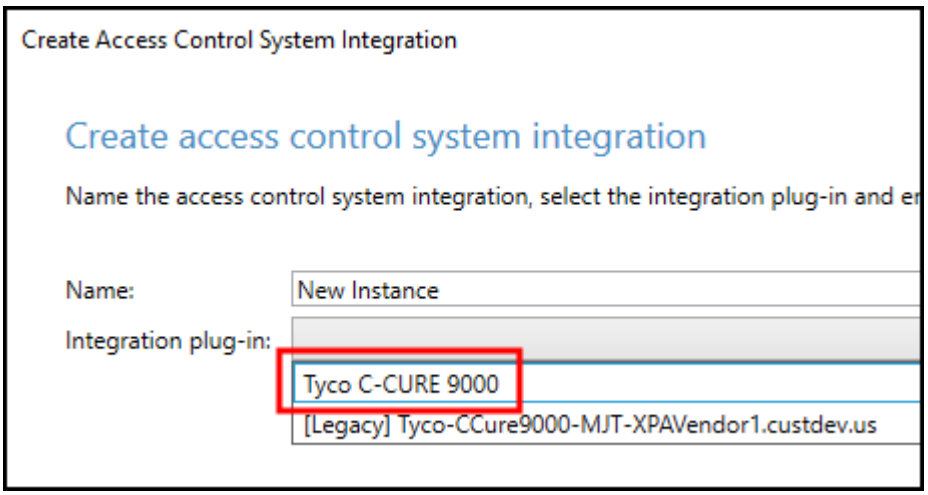
> When upgrading to version 1.3 or higher of the integration, from all versions prior to 1.3, it is required that the file directories where the integration files from the old version where stored are not deleted, before or after the integration is upgraded. Below is the directory for the old integration files:
>
> **C:\ProgramData\VideoOS\ACMServers**

After upgrading the integration, any previous versions of the XProtect Access instance in the XProtect Management Client will have the **[Legacy]** label added to it. This simply identifies an upgraded XProtect Access instance.



Any new XProtect Access instances which are added to the same XProtect system have the option to choose between the new version and the **[Legacy]** version during the instance creation wizard. New instances should always choose the version which is labled:

- **Tyco C-CURE 9000**



Secure communications explained

XProtect Access integrations can be configured to use encrypted communications. The XProtect Access integration with CCure 9000 can encrypt communications between the XProtect Access service and the XProtect Event Server which is running the CCure XProtect Access MipPlugin, and between the XProtect Access service and victor web service.

The fully detailed process included here is for self-signed certificates. If you are using a third party certificate, from a commercial certificate provider, please skip ahead to step number two below.

The following steps will enable secure communications for this solution.

1. Install a root certificate on the same server that will host the CCure XProtect Access Service
2. Install a certificate on the victor web service host and configure the IIS server to use the certificate
3. Configure the CCure XProtect Access Service to use a certificate
4. Configure the XProtect Access instance to use secure communications

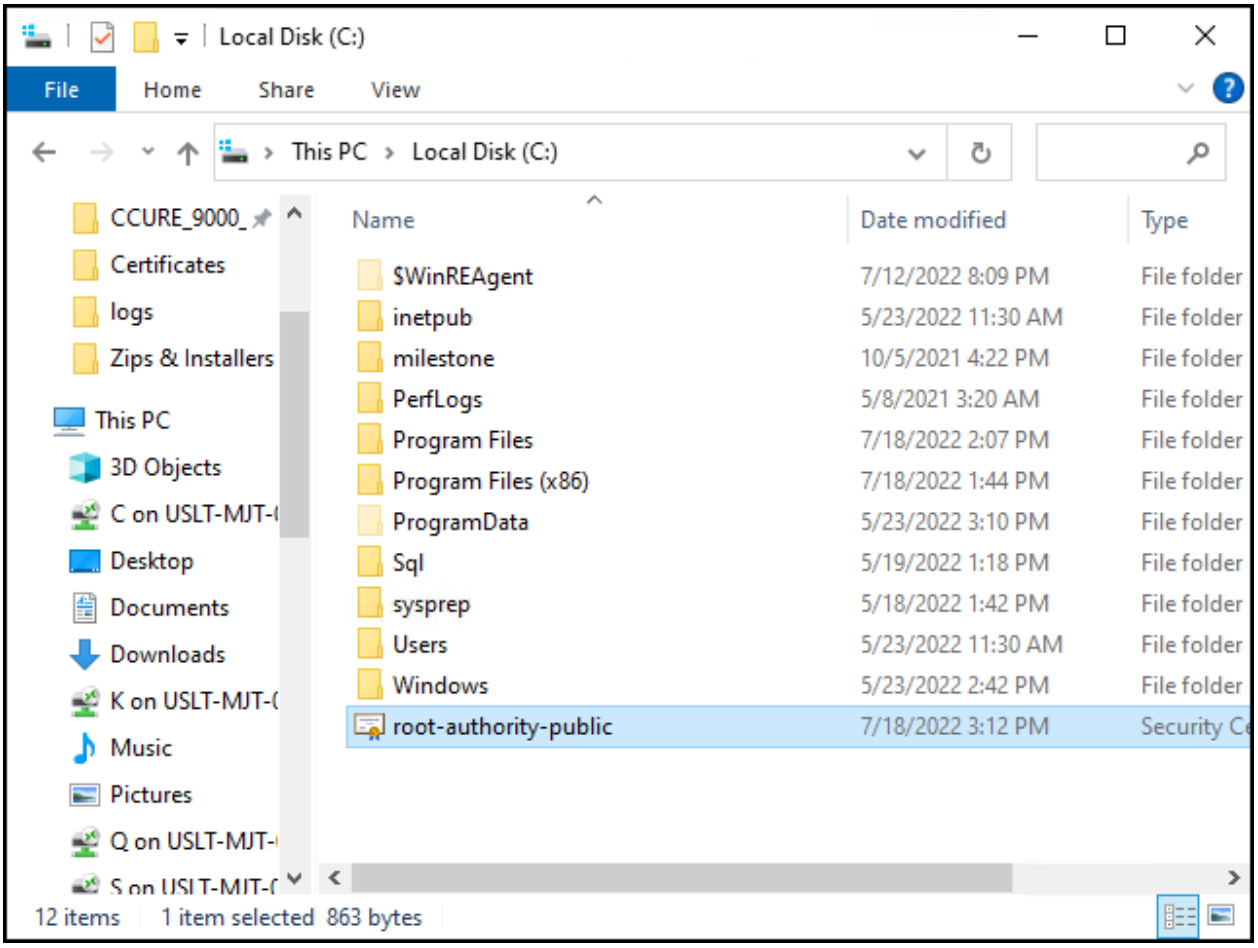
Please note that the instructions contained in this document are for generating your own certificates. It is also possible to obtain certificates from a trusted third-party certificate provider. For more information about certificates please read the XProtect VMS certificates guide

Encrypting communication between the XProtect Access service and the victor web service

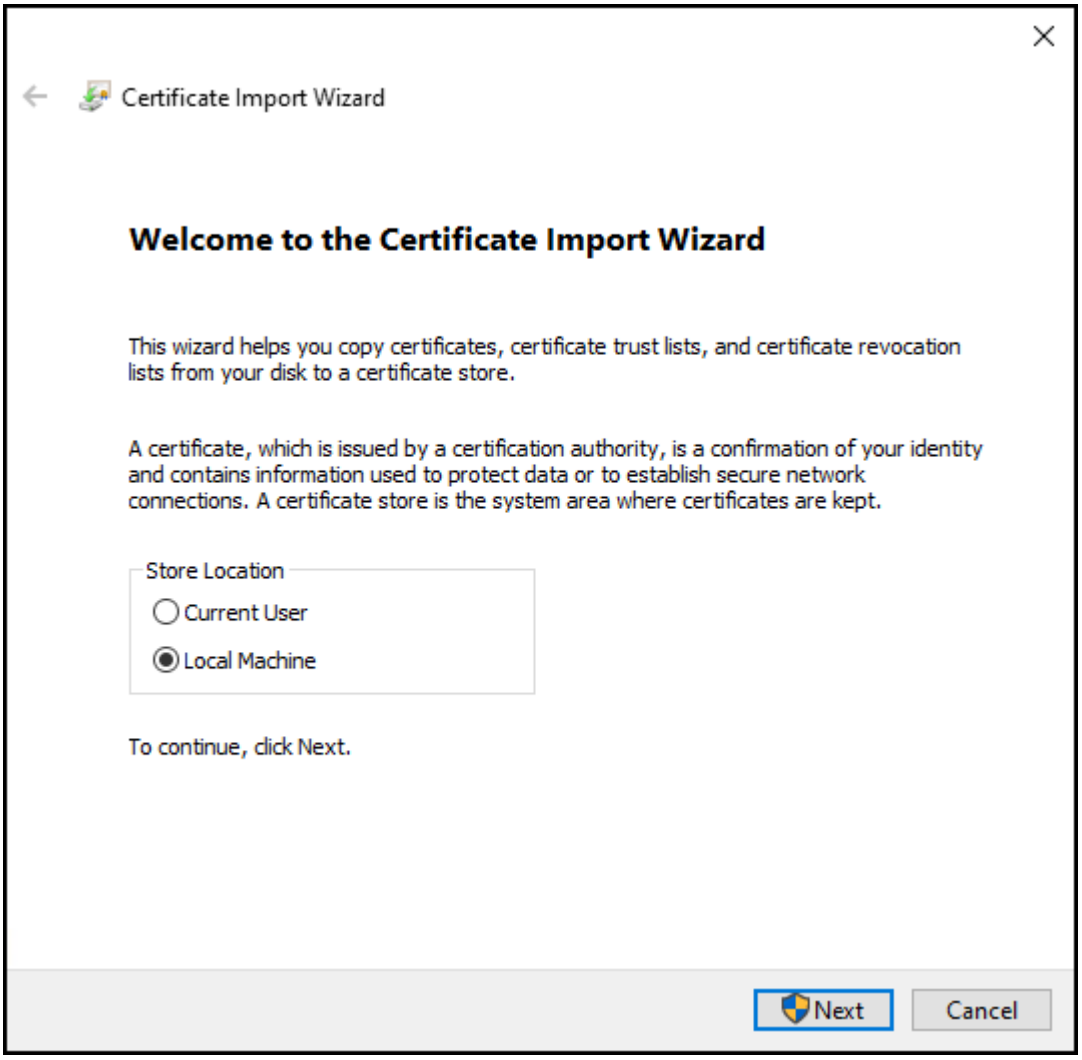
In the current version of the XProtect Access CCure 9000 integration it's possible to encrypt communications between the CCure XProtect Access Service and the victor web service. To do so, install a root certificate on the server that hosts the CCure XProtect Access Service and configure the victor web service to use the certificate. Below are the steps required to install the root certificate and configure the victor web service.

The fully detailed process included here is for self-signed certificates. If you are using a third party certificate, from a commercial certificate provider, please skip ahead to step number ten below. Refer to the XProtect Certificate Guide for any questions on dealing with certificates.

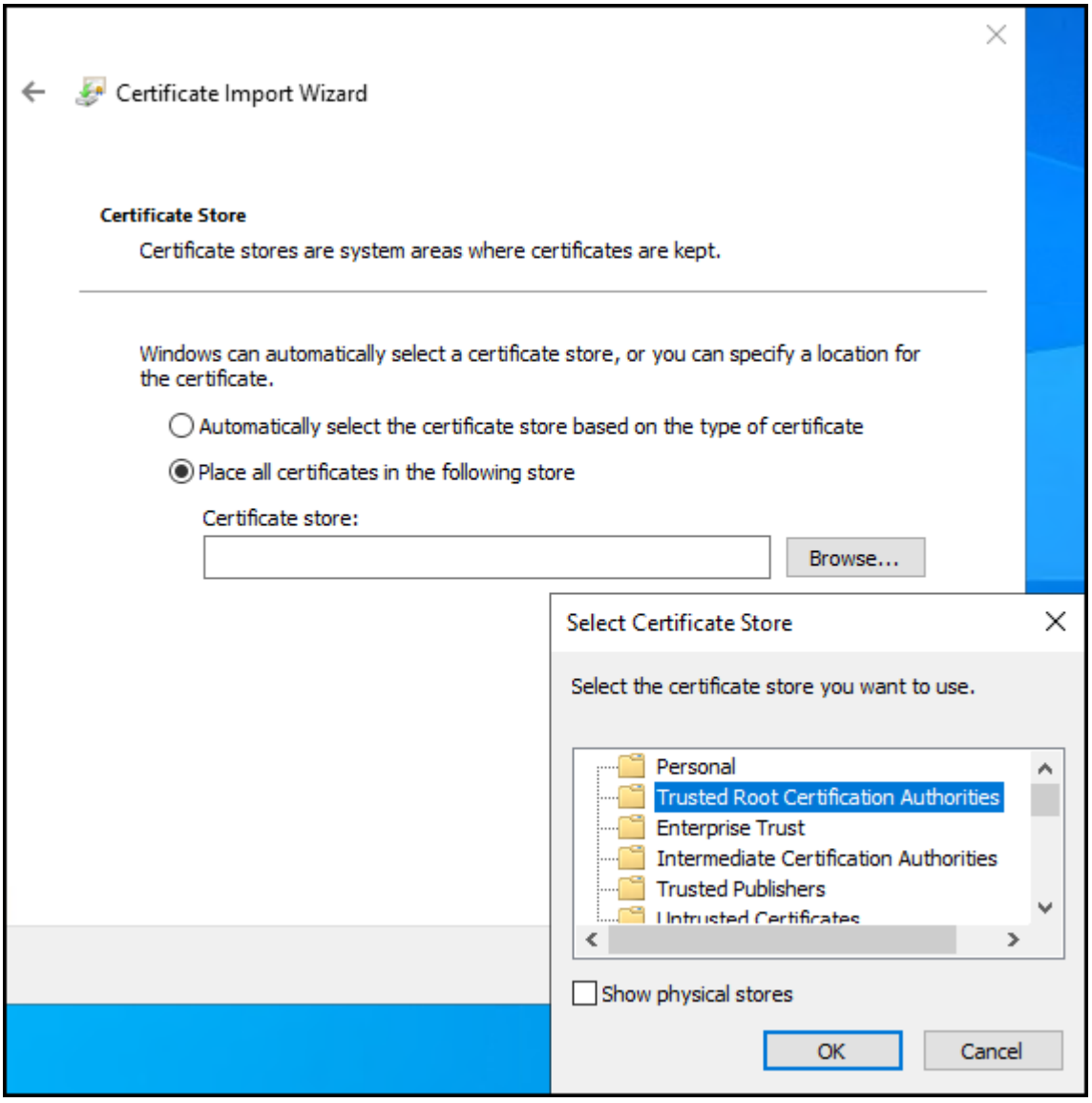
1. On a server with restricted access, open PowerShell and run the script in Appendix A, to create a CA certificate.



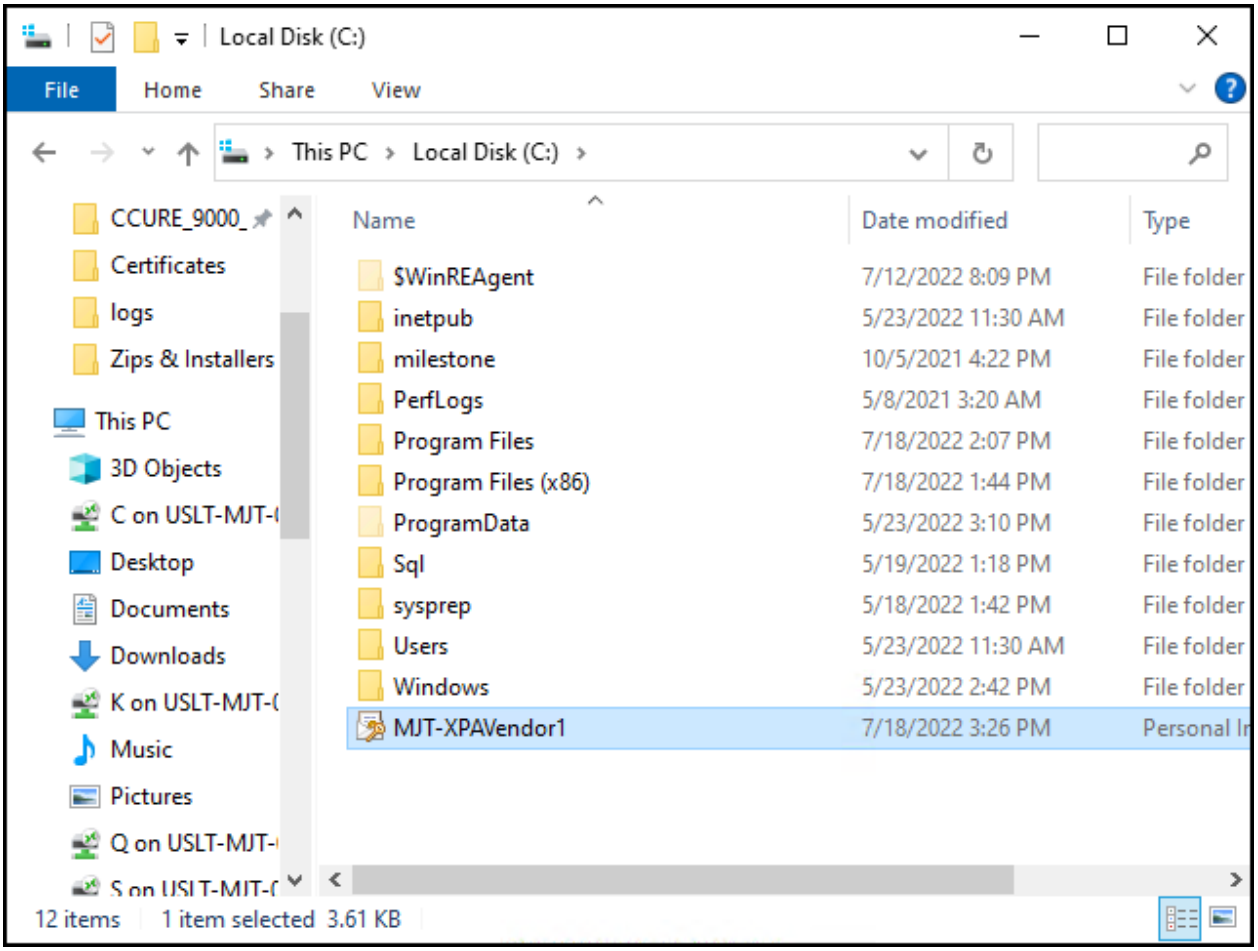
2. By default the script places the new root certificate in the **C:** file location. Move the certificate to the server that hosts the CCure XProtect Access Service.
3. Go to the server that hosts the CCure XProtect Access Service and right-click the certificate and select **Install Certificate** to begin the certificate installation wizard.
4. Choose to place the certificate in the **Store Location** of the **Local Machine**.



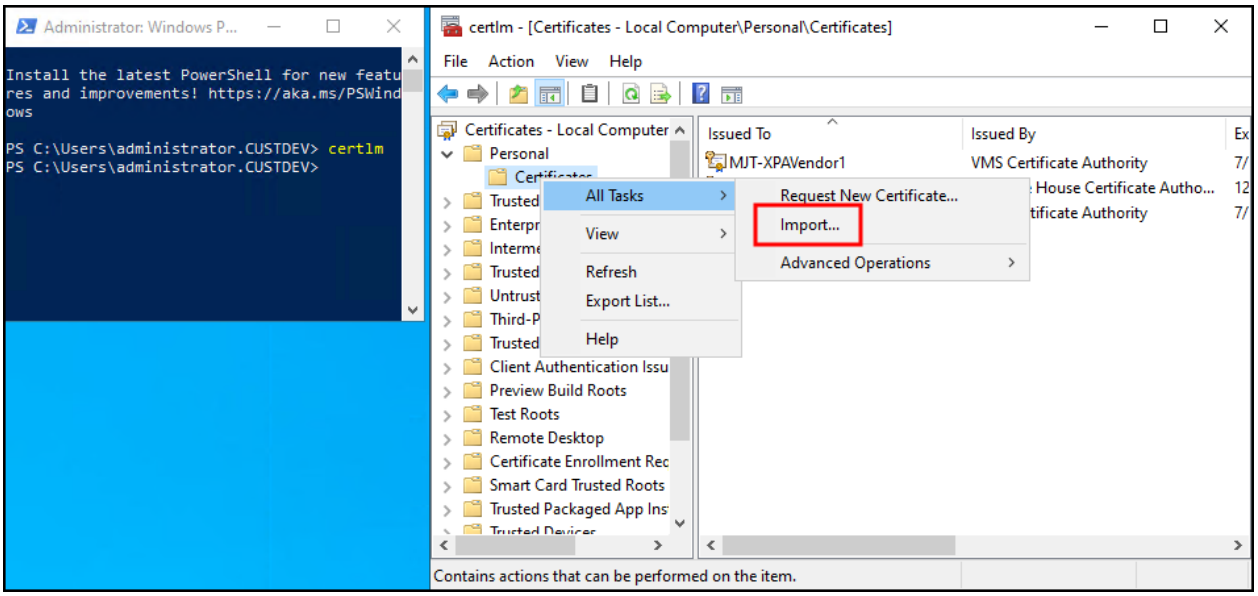
5. Browse and import the certificate in to the **Trusted Root Certification Authorities** folder.



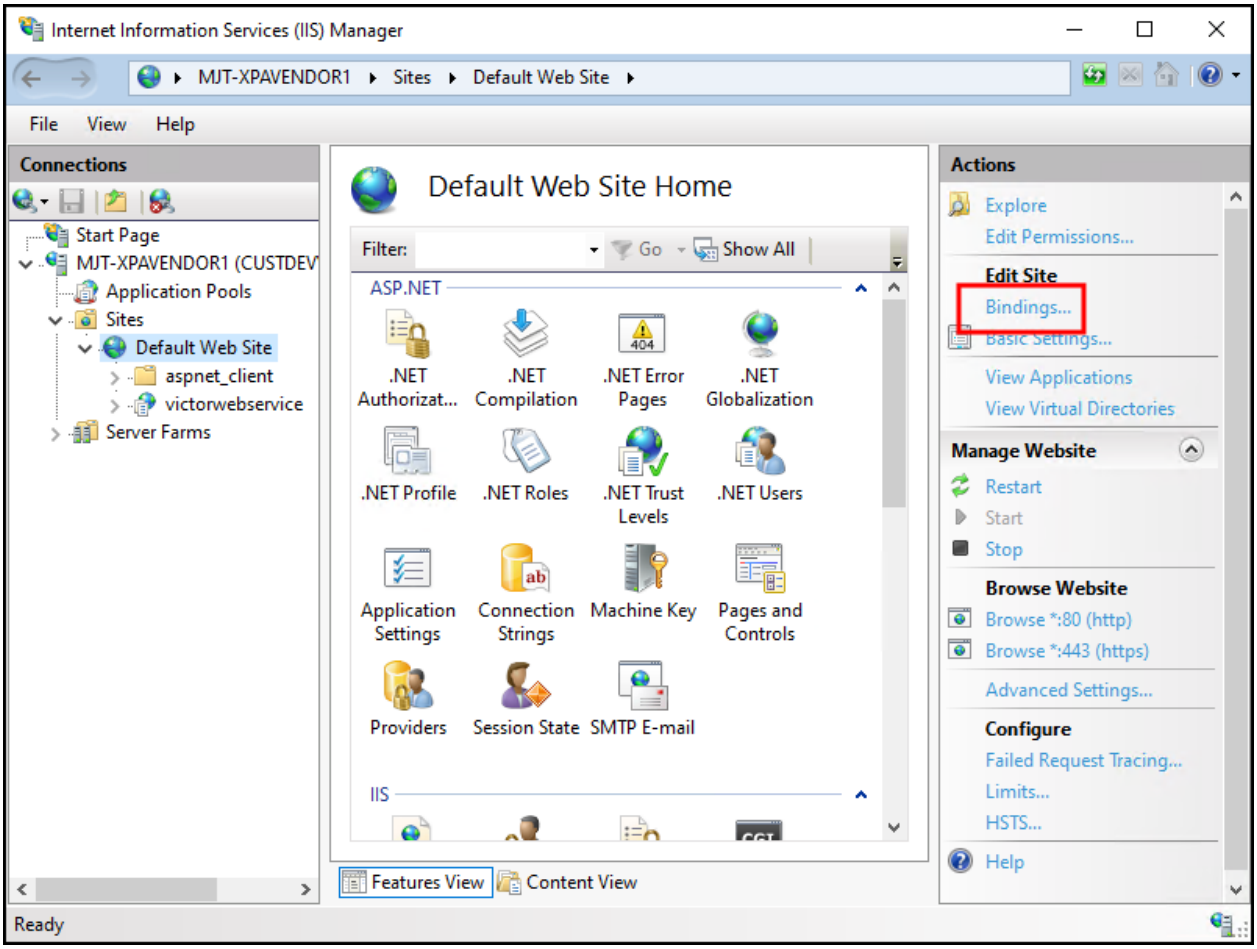
6. Complete the wizard.
7. Go back to the server with restricted access where you generated the root certificate, open PowerShell and enter the script in Appendix B, to generate a new client certificate to install on the server hosting the victor web service.
8. You will need to enter the PC name of the server hosting the victor web service, the IP address of the server, and a certificate password of your own choosing during the process of completing the script. Enter this information and complete the script.
9. By default the script generates the certificate at the **C:** file location. Copy the file and move it to the server hosting the victor web service.



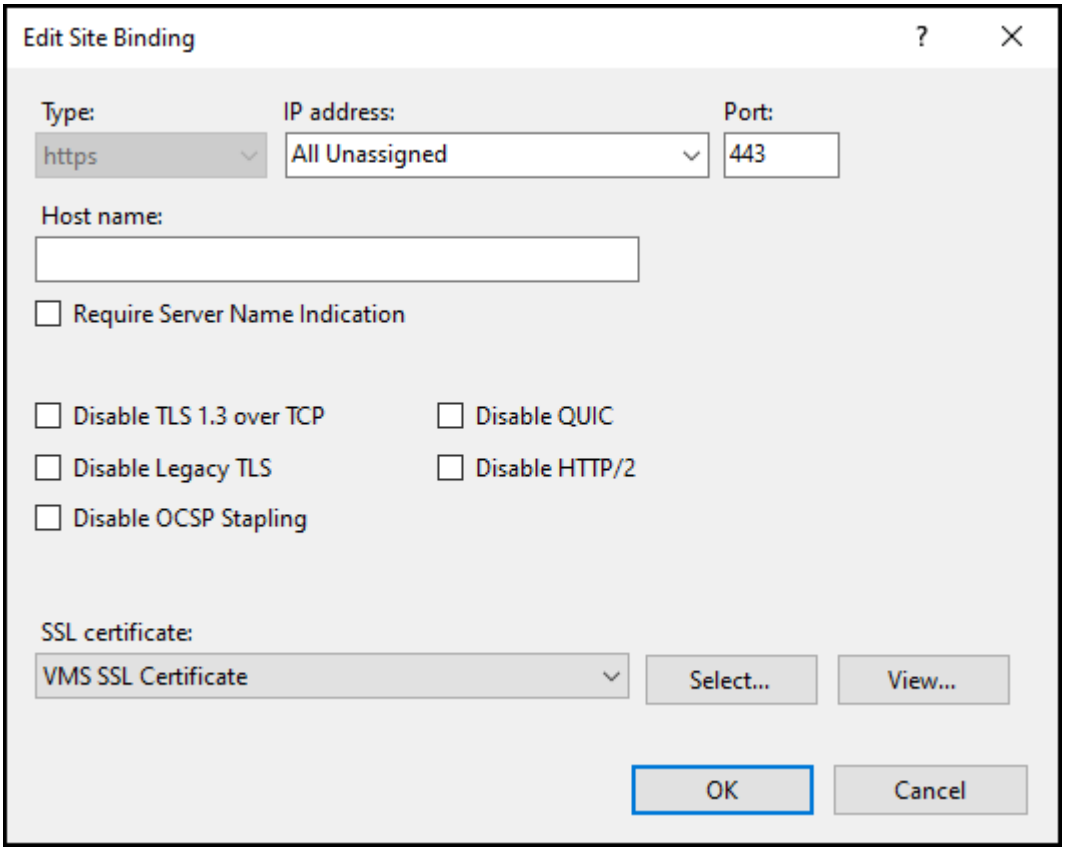
10. Go to the server hosting the victor web service and run the certificates snap-in for the local machine. Right-click the **Certificate** store within the **Personal** folder and choose to **Import** a new certificate.



11. Import the certificate into the store of the local machine. Choose the certificate file that you copied to the local server. Enter the password chosen during the script. Browse to the personal folder of the certificate store to choose that as the location for the certificate. Complete the import wizard.
12. The final step in this process involves binding the certificate to the IIS server supporting the victor web service. In the **IIS Manager** application on the victor web service host server, open the **Bindings...** menu of the **Default Web Site**.



13. Choose to edit the https binding, select the imported certificate from the **SSL certificate** list, click **OK** and close the **Site Bindings** menu.



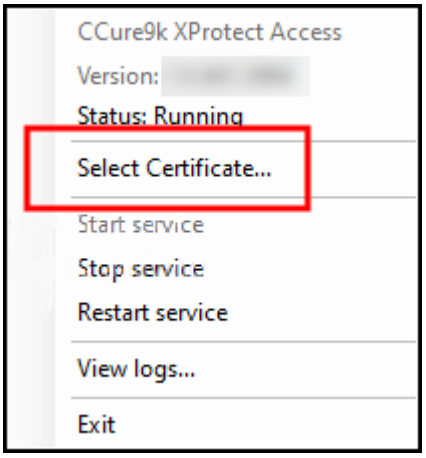
14. Now the solution is ready for secure communications between the CCure XProtect Access Service and the victor web service.

> For more information about configuring the CCure 9000 system and the victor web service for secure communications refer to the **victor Web Service User Guide** available from Johnson Controls.

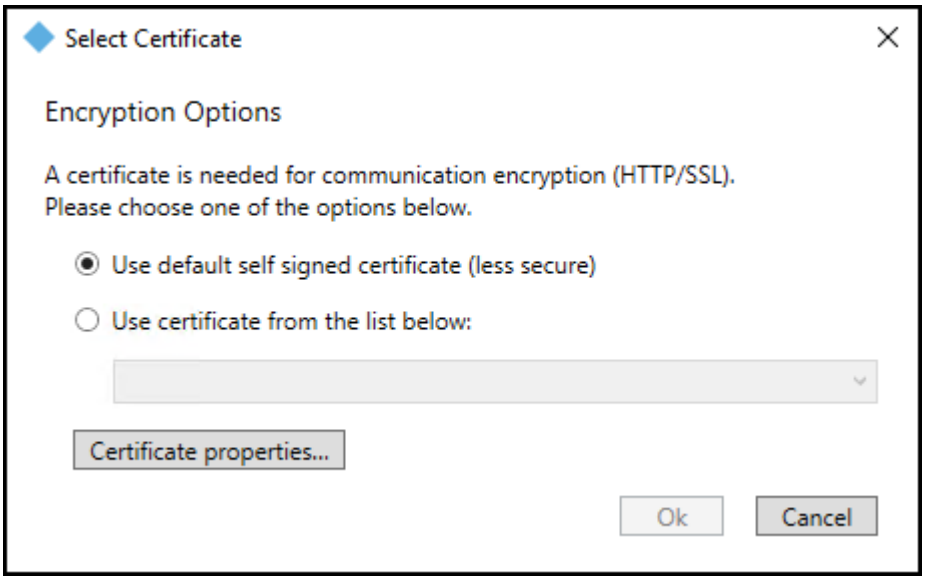
Encrypting communication between the XProtect Access service and the XProtect Event Server

In the current version of the XProtect Access CCure 9000 integration, there is a tool built into the XProtect Access service to help users manage these certificates. This process shows the steps required.

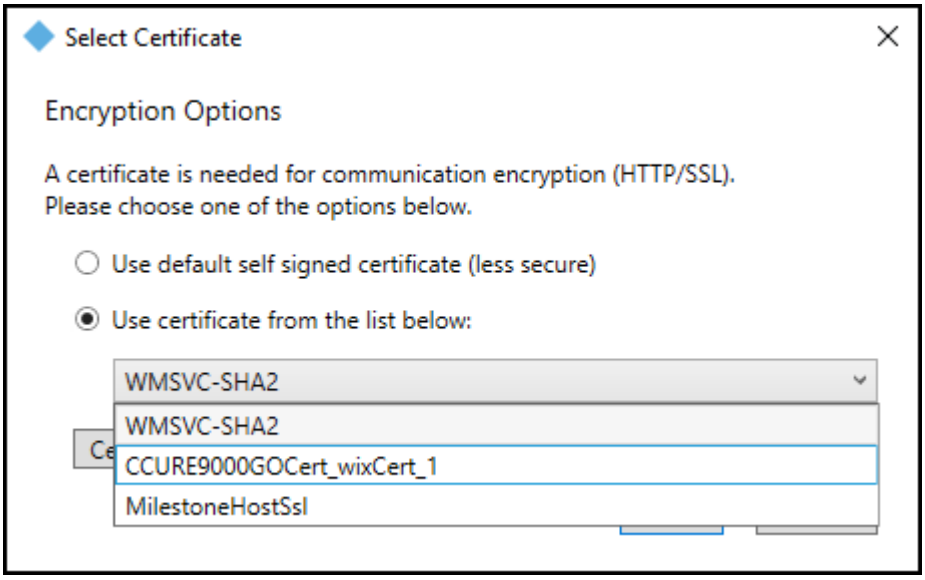
1. Go to the CCure 9000 server where the XProtect Access service is installed, right click on the XProtect Access service icon in the system tray and choose the **Select Certificate** option from the shortcut menu.



2. The **Select Certificate** window will open. There is a self signed certificate available on the server. The self signed certificate is the default selection.



3. Choose the type of certificate that meets your security requirements. Milestone recommends using a valid third party certificate if possible as this provides the highest level of security.
4. Select the **Use certificate from the list below** option and open the list to choose from the available certificates.



5. Click the **Properties** button to inspect the properties of the chosen certificate. And click **OK** to continue using the selected certificate.
6. Agree to the warning about restarting the XProtect Access service.

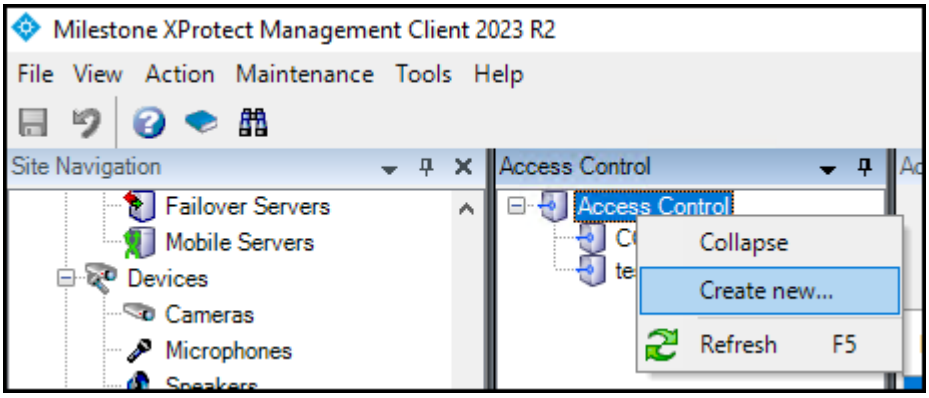
If the **Select Certificates** window has no available certificates there are several reasons for this, please consult the No certificates available in Select Certificate window on page 94 topic.

XProtect Management Client Config

Creating XProtect Access instance & establishing connection to CCure 9000

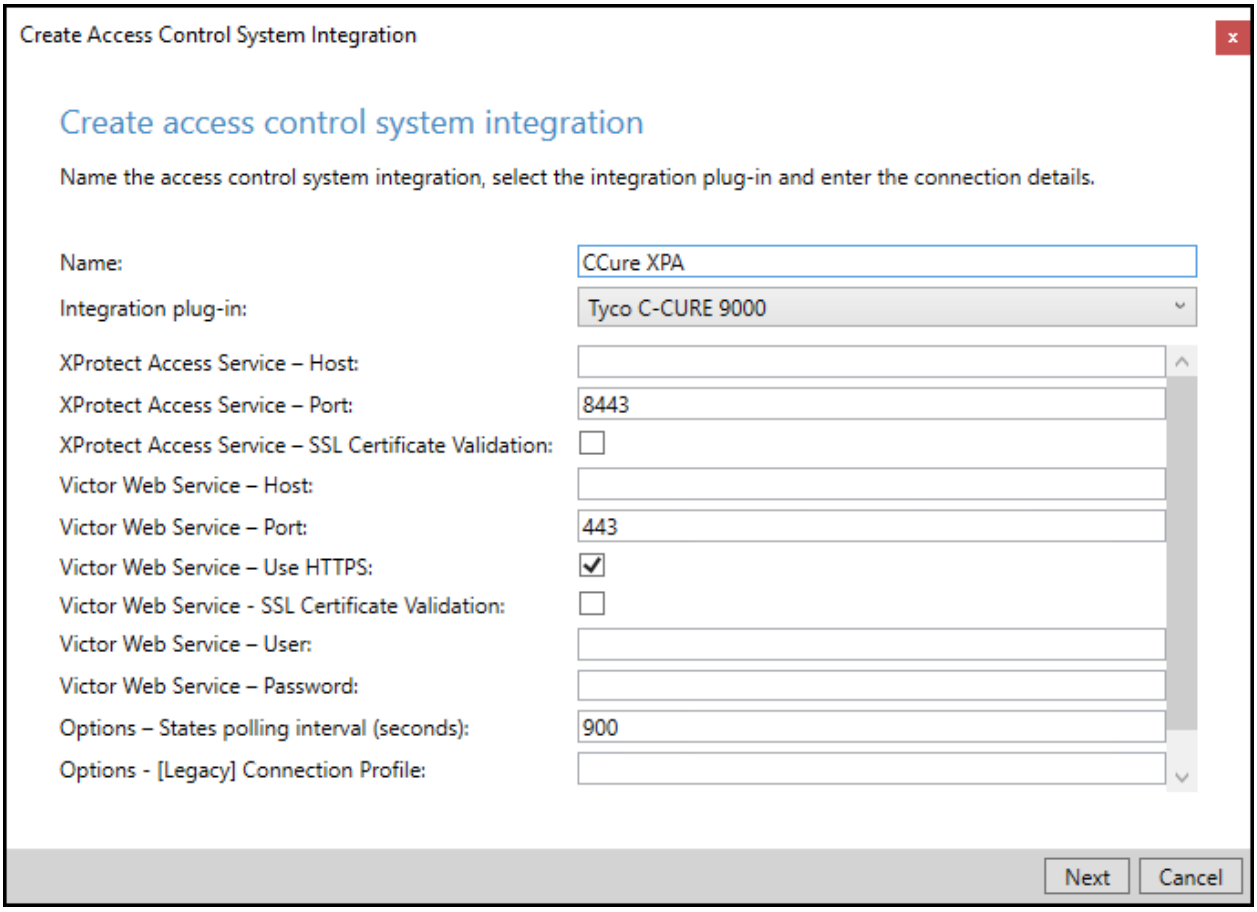
Once the CCure XProtect Access Service and the MIP Plugin are installed and configured the XProtect Access (XPA) instance can be created in the Management Client.

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

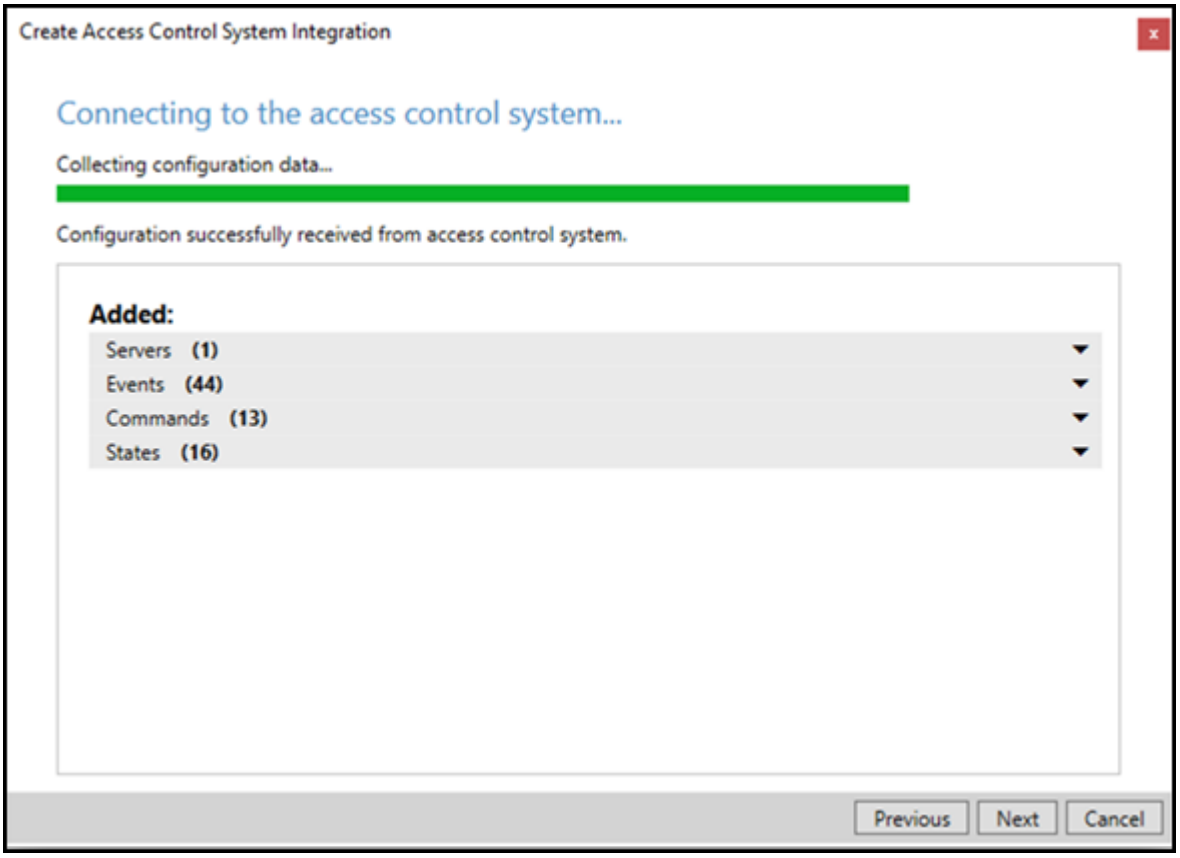


3. The XProtect Access instance creation wizard begins.
4. Enter a **Name** for the plug-in and select the CCure 9000 plug-in from the list.

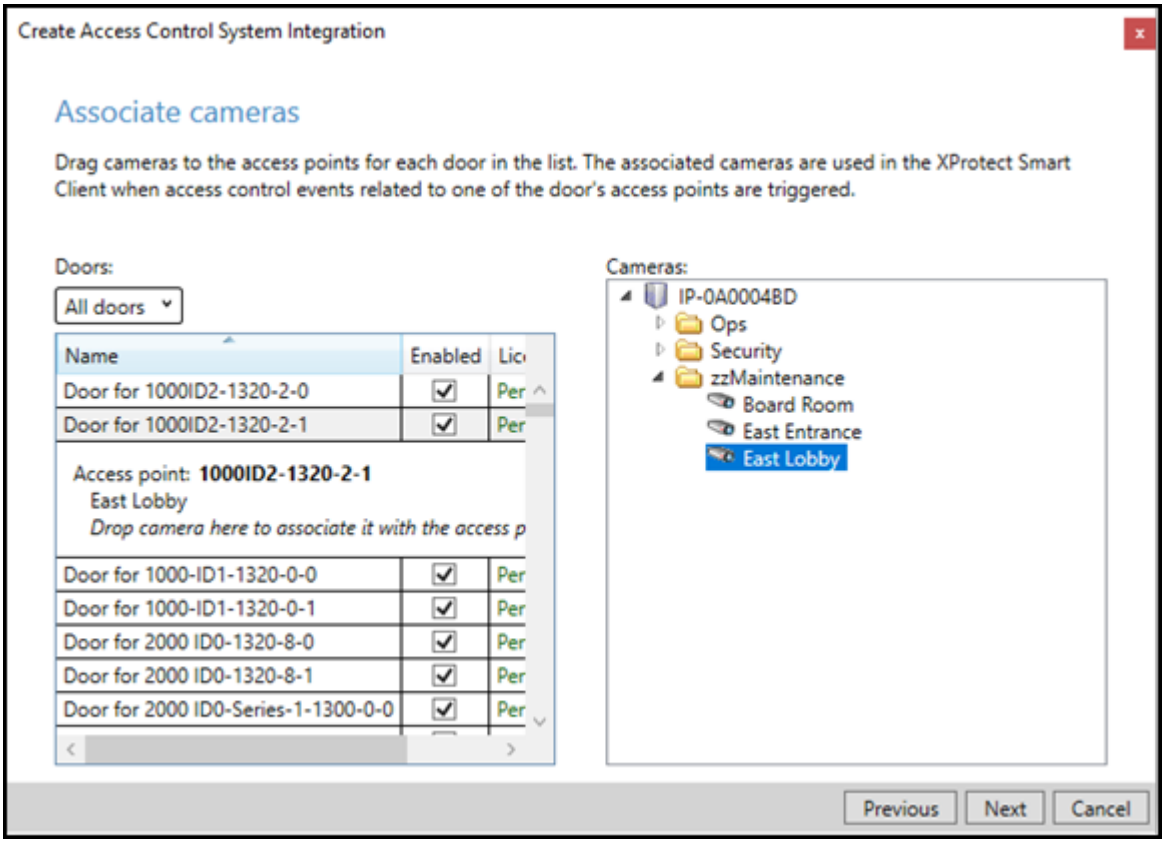
- The plug-in is named **Tyco C-CURE 9000**. After selecting the plug-in, you will have to provide credentials and parameters to configure the connection to the CCure 9000 victor web service.
- The credentials and parameters required are listed here: XProtect Access instance connection properties on page 40:



5. 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.



6. 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.
7. 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.



8. Complete the wizard to finish creating the XProtect Access instance.

XProtect Access instance connection properties

The credentials and parameters required to connect the XProtect Access instance to the CCure 9000 system are detailed below:

IT security policy can prevent login and lock the user account running theCCure XProtect Access Service if there are repeated invalid login attempts. There is a **PluginSettings.json** file installed on the server running the CCure XProtect Access Service which contains a cooldown timer setting of five minutes which helps to prevent repeated invalid logins. Access the file and modify the values to get around this setting if desired.

Property Name	Required Entry Details
Name	Custom name field

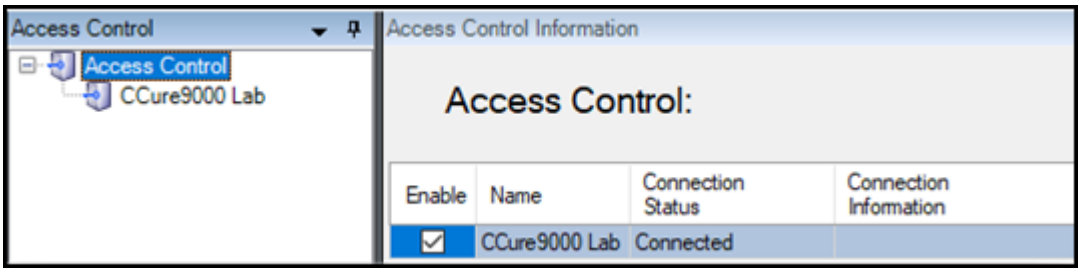
Integration plug-in	Displays the current version of the ACM MIP Plugin
XProtect Access Service Host	[Hostname.Domain.TLD] This field should contain the Fully Qualified Domain Name (FQDN) of the CCure 9000 server where the XProtect Access Service was installed.
XProtect Access Service Port	8443 is the default
XProtect Access Service - SSL Certificate Validation	Enables SSL certificate validation between the CCure XProtect Access Service and the CCure XProtect Access MipPlugin. This option is required to use a third party certificate. Not enabled by default.
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 - SSL Certificate Validation	Enables SSL certificate validation between the CCure XProtect Access Service and victor web service when a third party certificate is being used. Not enabled 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.
Options - [Legacy] Connection Profile	Used for backward compatibility with previous versions of the integration (after an upgrade). In most cases, this field must be empty.
Options – Enable performance metrics (diagnostics)	Not selected by default. Select this option to include performance statistic logging on event metadata.

The **Victor Web Service - Host** field must contain the PC name of the server where the victor web service is installed. The script used to create the certificate specifies the PC name and any other method of identification for the server - such as the IP address or the fully qualified domain name - will not work. Make sure to match the PC name from the script with the data entered in the **Victor Web Service - Host** field.

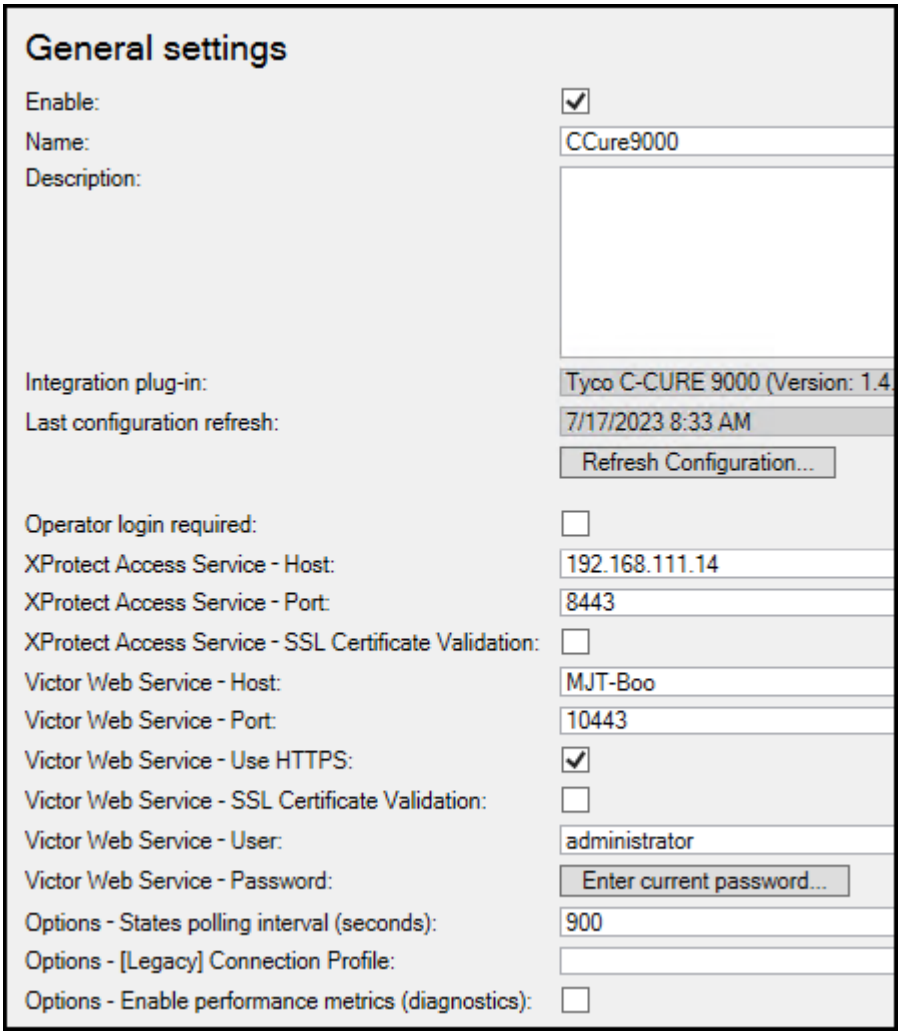
Admin Config

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.



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



A full description of all the properties available is found here: XProtect Access instance connection properties on page 40.

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.

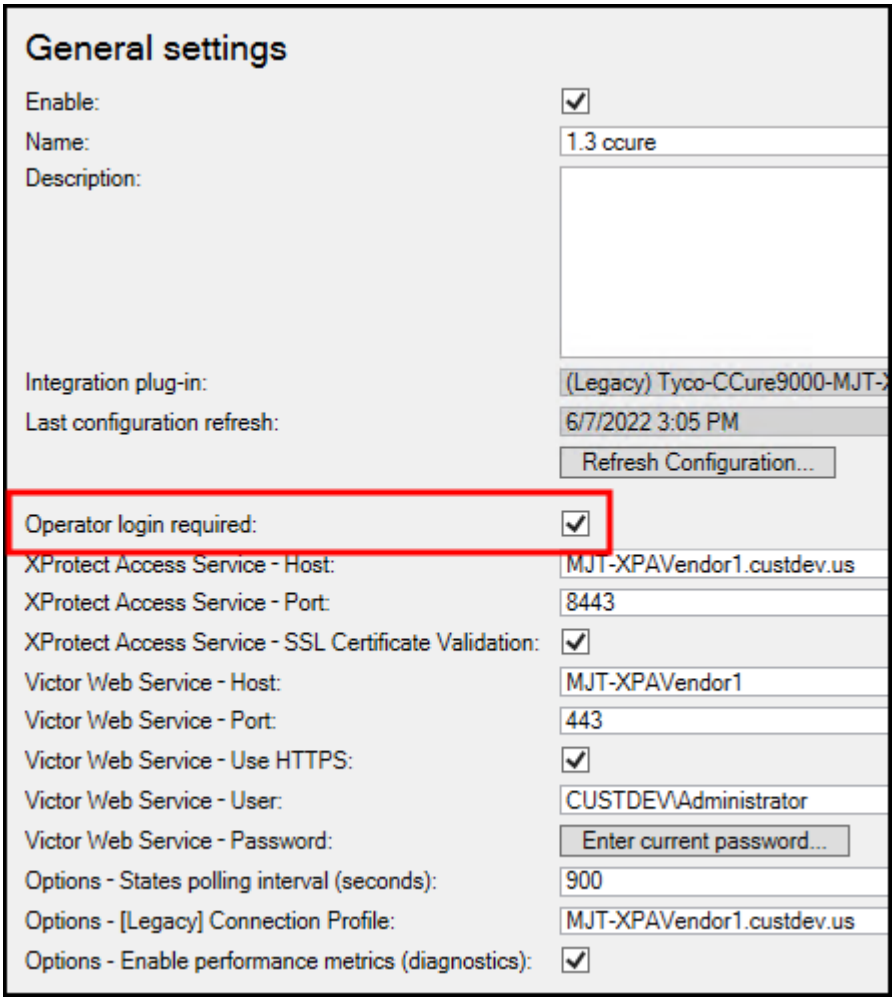
Personalized login manages two configurations. First, is the global configuration used by the Management Client. Second, is the personalized configuration used in the Smart Client. Personalized configurations are subsets of the global configuration. This helps ensure accurate event handling, command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

Requirements for Personalized login:

- XPA CCure 9000 integration version 1.1 or higher.
- CCure 9000 version 2.8 or higher

Enable/disable Personalized login:

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



There are special requirements for personalized login which change slightly based upon the version of CCure 9000. Please read the personalized login workaround topic if you want to use this feature.

Smart Client personalized login

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

After entering the user name 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 XProtect Access 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:

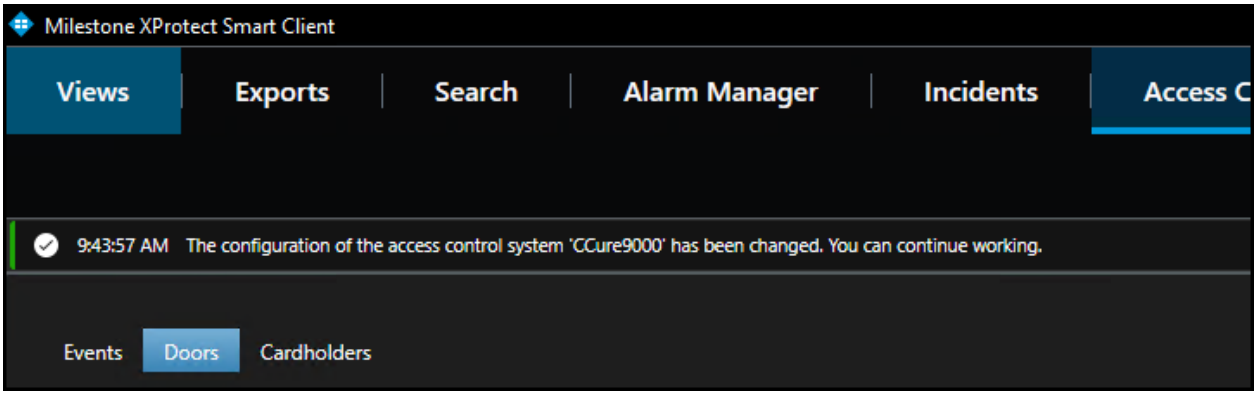
- Alarms related to hardware the user can view in CCure
- Events related to hardware the user can view in CCure
- Devices in the map element selector that the user can view in CCure

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, users can only acknowledge alarms related to hardware they can see.

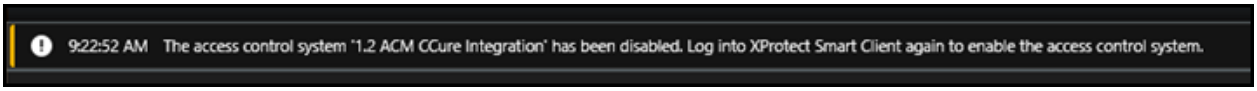
Refreshing personalized configurations

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 XProtect Access 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, the Smart Client application will have the following info message displayed.



If the permissions and CCure access rights are included in the change the following message can appear:



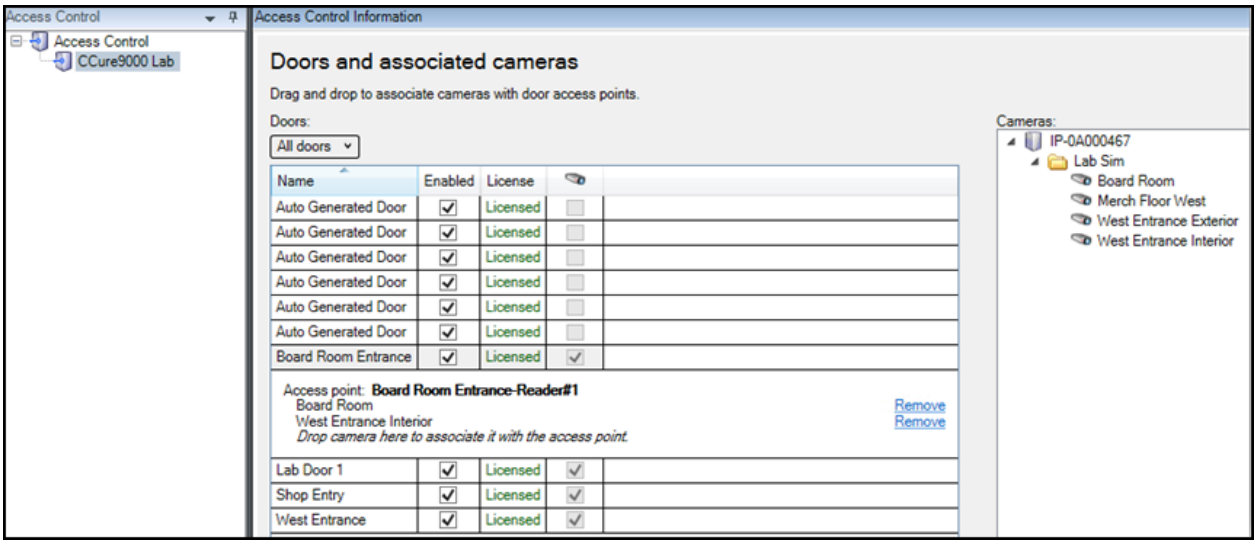
If either of these messages appear, simply follow the instructions in the message. Logging out of the Smart Client application and re-authenticating using the personalized login process will always fetch an updated configuration.

Door and camera association

In the **Doors and associated cameras** menu of the XProtect Access 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.

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



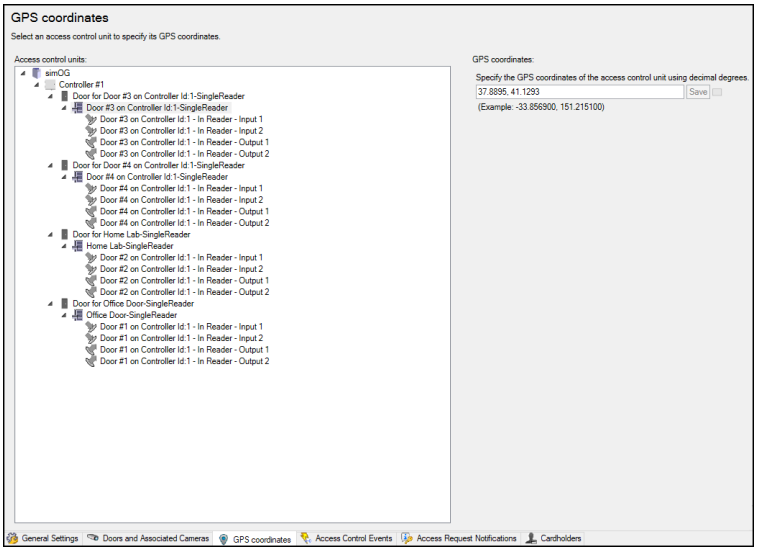
2. Click on a door. Under it all associated cameras are listed.

3. 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.
4. If required, click the **Remove** link to end the association between the camera and the door.

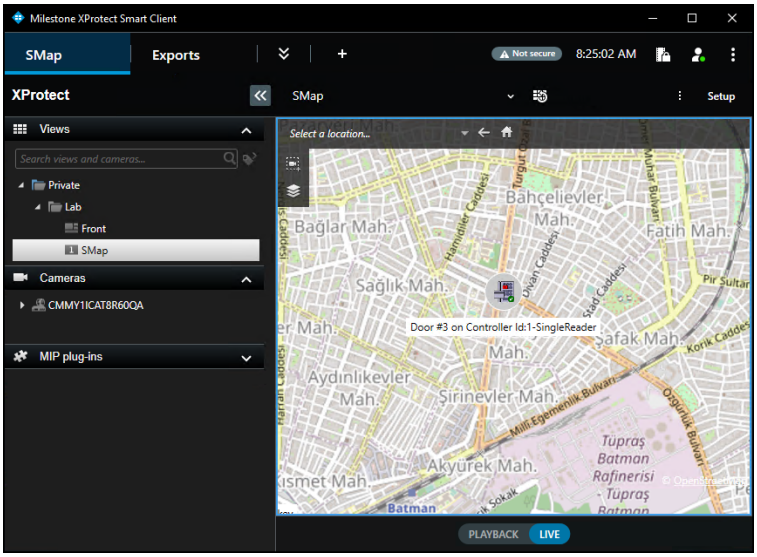
GPS coordinates

In the **GPS coordinates** menu of the XProtect Access Instance all of the access control hardware devices are listed. If the devices have been placed on the Smart Map, they have a GPS coordinate value. Using this menu, it is possible to enter in the exact GPS coordinate of your device, and it will appear on the map at the corresponding location.

1. Expand the **Access control units** device tree to find a specific device.
2. Select a device. Enter the GPS coordinate value for the device in the **GPS coordinates** field. Click **Save**.



3. Confirm your device has been placed on the Smart Map.



Find out more about configuring the Smart Map in the Smart Client, and explore all of the features available for access control devices on the Smart Map.

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.

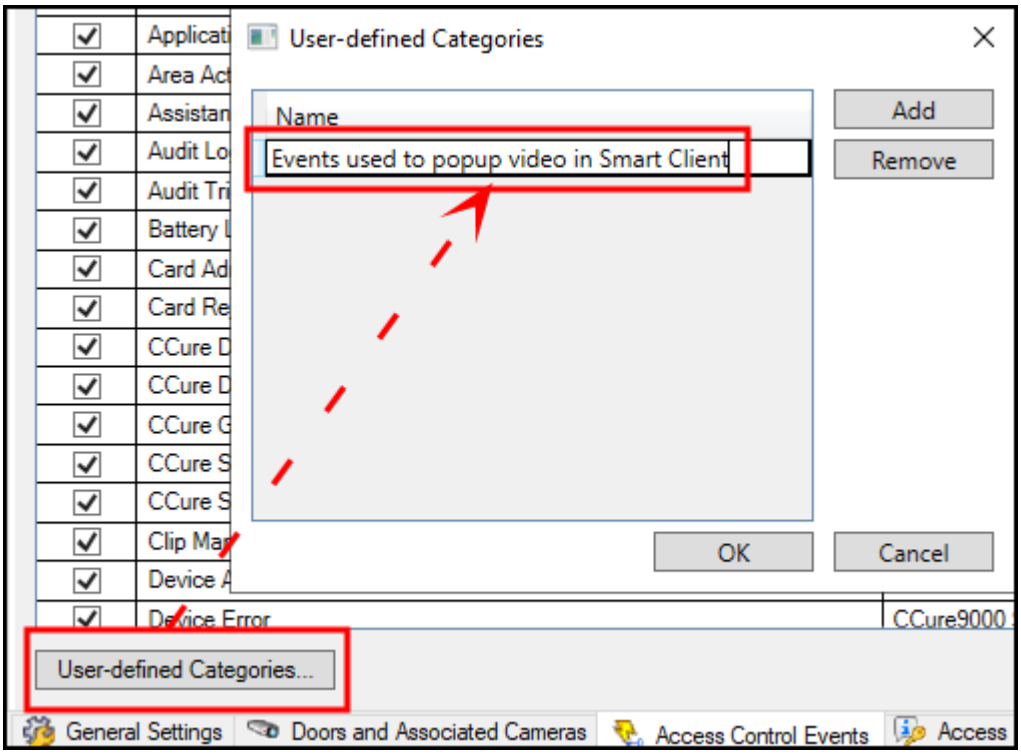
To generate XProtect alarms or rule-based actions triggered by any one of a group of individual CCure events, the events must be categorized. For example, the integration can be configured to start recording video from associated cameras based on any number of unique hardware events: “Door Forced,” “Denied, 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 XProtect Access of any event in that category.

The categories are:

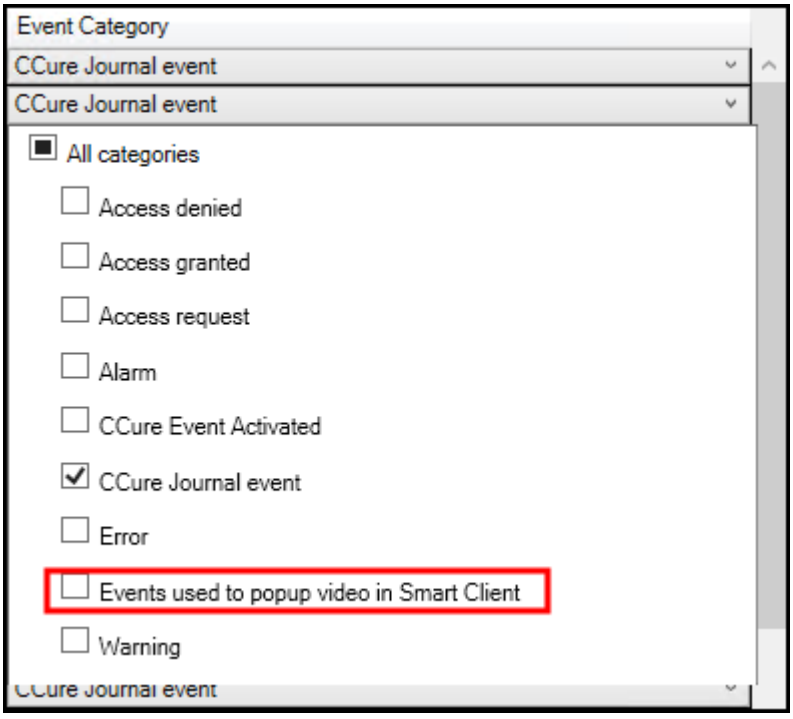
Default XProtect Access Events	CCure Events	Custom Events
• Access granted • Access request • Access denied • Alarm • Error • Warning	• CCure Event Activated • CCure Journal event	• User-defined category...

Creating a user defined category

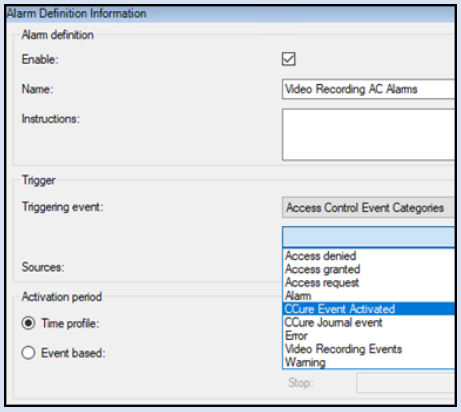
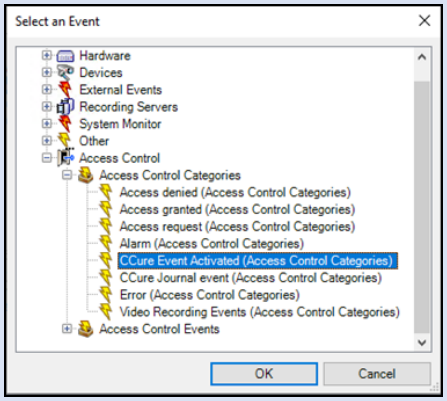
1. Go to the **Access Control Events** menu.
2. Click the **User-defined Categories** button to create your own custom event category.



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



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

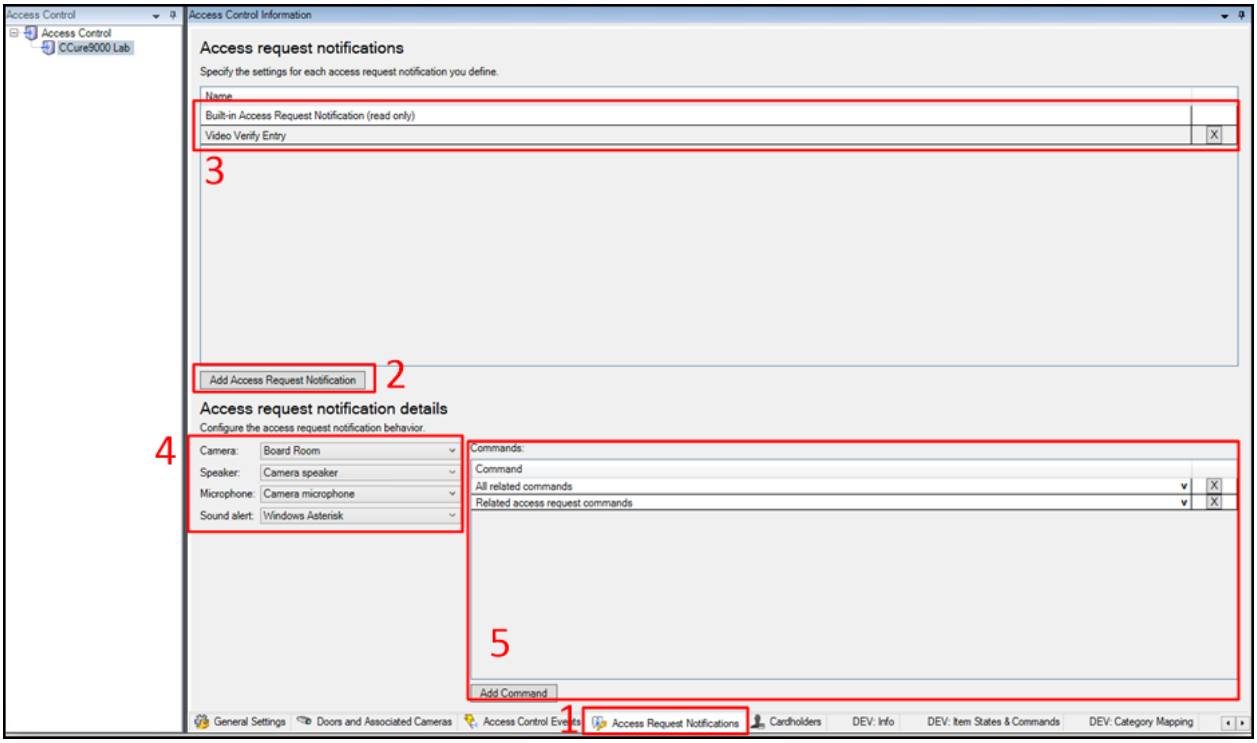
Alarm Access Control Categories Event list	Rule Access Control Categories Event list
	

Access request notifications

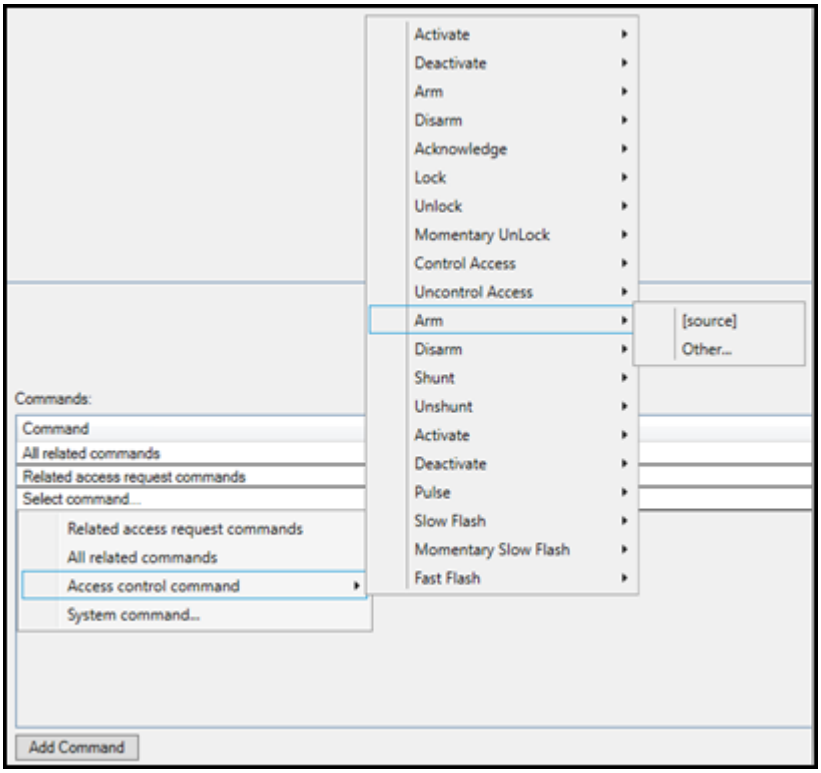
Access request notifications are pop-up notifications which appear in front of all other desktop applications for all users logged into the Smart Client with access to view XProtect Access features and devices. These notifications can be customized in the **Access Request Notifications** menu. The XProtect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

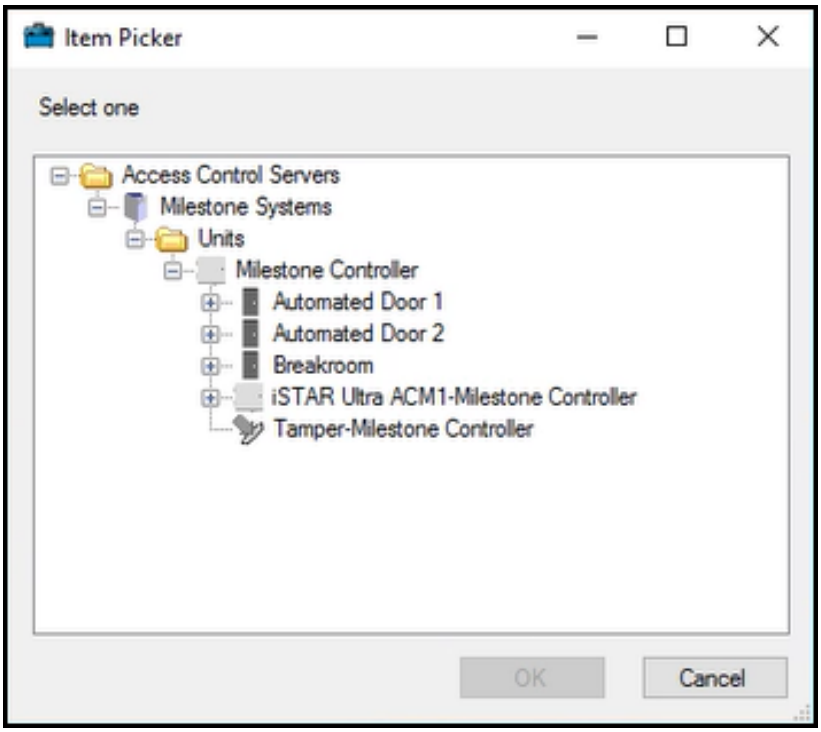
request notification.

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.



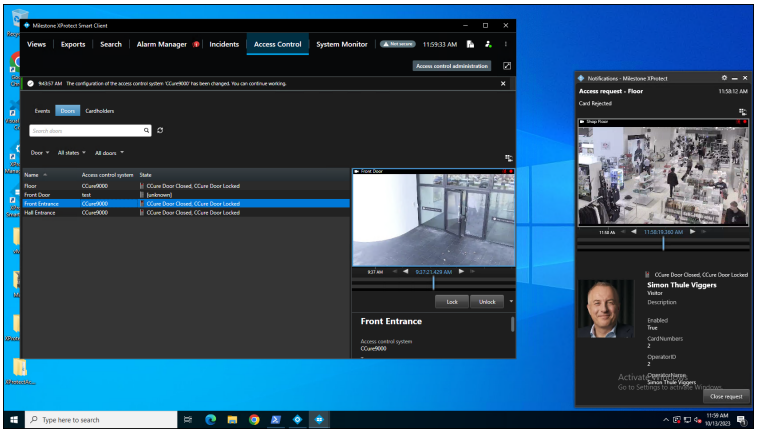
Open the **Commands** list and choose a type of command, the action the command will perform, and the hardware device to command. If the command should interact with a hardware device that is not related to the device which triggered the access request notification, choose **Other** and select from the list of all devices.





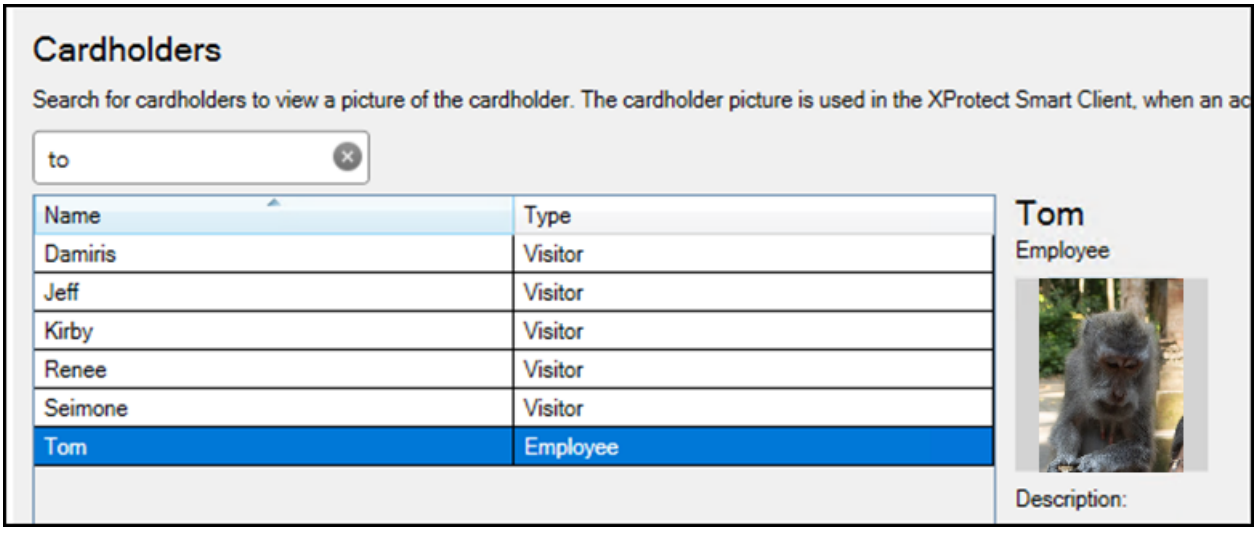
When the notification pops up on the desktop a sound will play if you choose to include a sound alert. The built-in access request notification does not include a sound alert.

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



Searching cardholders

All cardholders in the CCure system are imported from the connected server. Search for cardholders in the **Cardholders** menu of the XProtect Access 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:



Visibility of cardholder information, such as name, badge numbers, etc., is controlled within the CCure database.

Client profiles and roles explained

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.

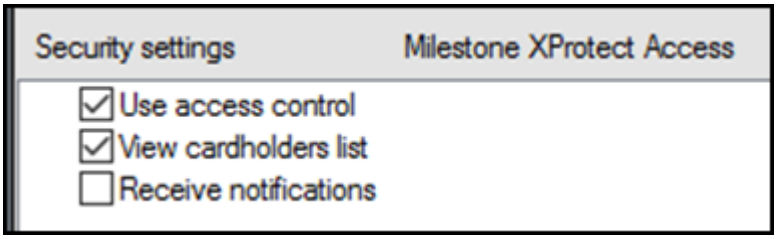
Managing client profiles and roles

1. 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.

2. 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.

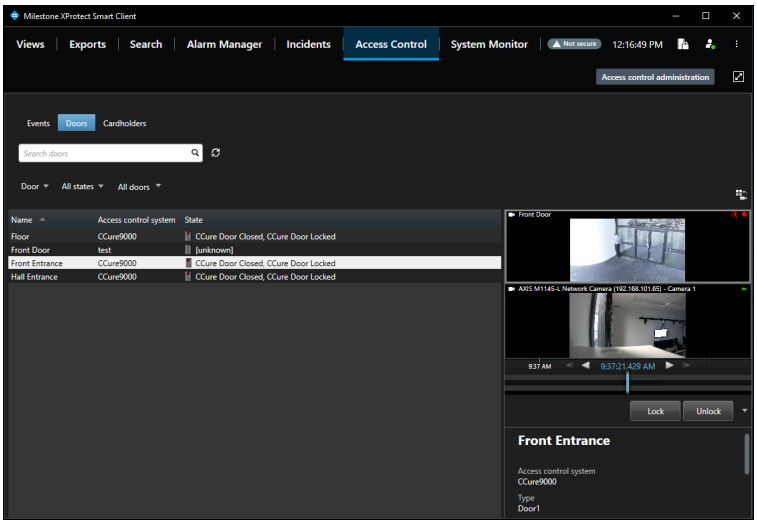


The **Receive notifications** setting is only used to enable notifications with the web client and mobile client.

Smart Client Features

Access control workspace explained

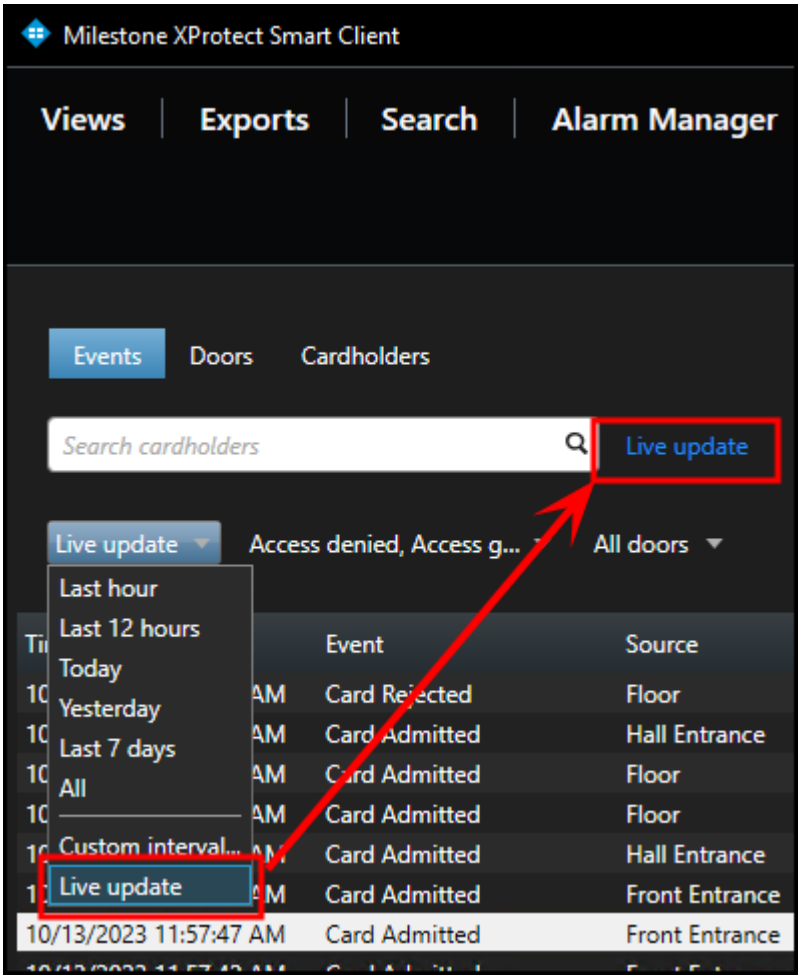
The XProtect Access CCure integration adds a new workspace, or tab, into the XProtect Smart Client. The **Access Control** workspace should appear in the Smart Client.



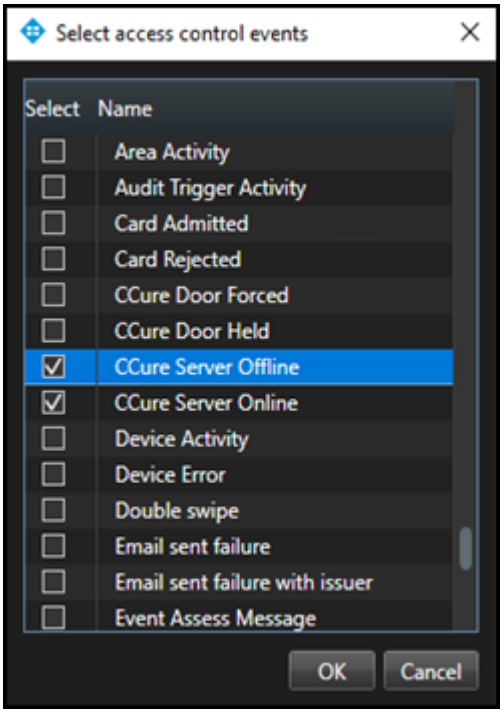
This workspace is used to search and filter events, doors and cardholders.

Access control workspace events list

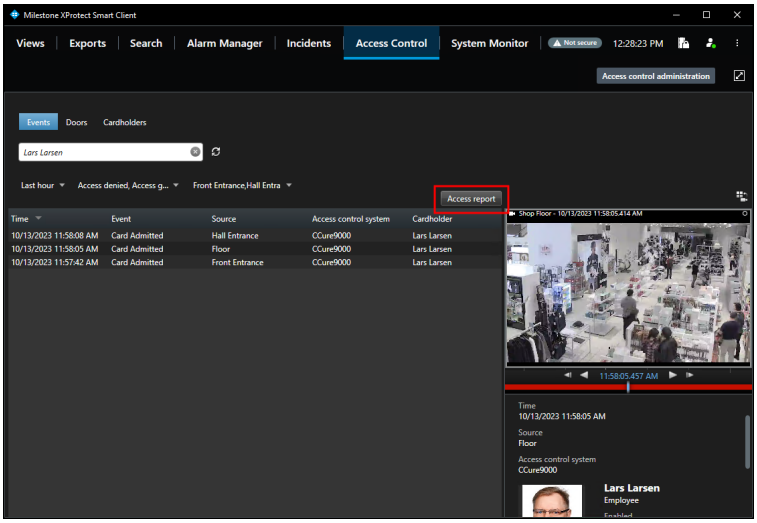
1. Go to the **Access Control** workspace of the Smart Client and select the **Events** list.
2. Select a time range, including a custom time range, or live update. Select the **Live update** time range to view a real-time display of access control events.



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



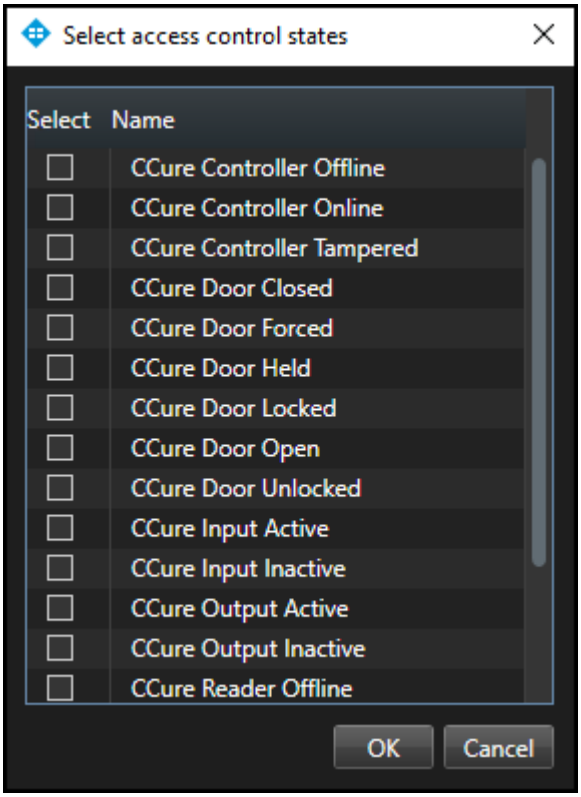
6. Filter for specific hardware devices.
7. Click the **Access report** button to create a PDF file of the events in the current list.



8. In the **Access report** window: name the report, choose a destination to save the report, include comments, and select the option to include snapshots.

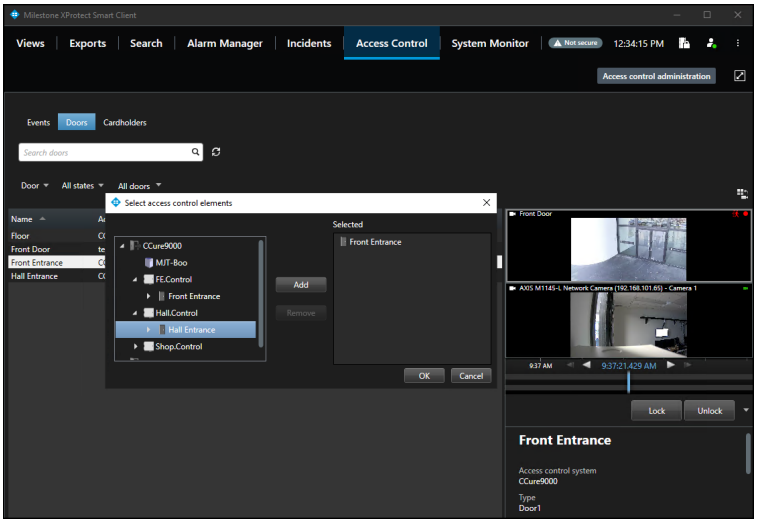
Access control workspace doors list

1. Go to the **Access Control** workspace and select the **Door** list to select the type of hardware to display.
2. Select the **Access control type...** option to open the **Select access control types** window. The default option for this list is **Door**. However, servers, and readers can also be selected.
3. Open the **All states** list to filter hardware by status.
4. Select the **Access control state...** option to open the **Select access control states** window and select from the list of all available CCure hardware states.



5. Open the **All doors** list and expand the list or select the **Other...** option to open the **Select access control elements** window.

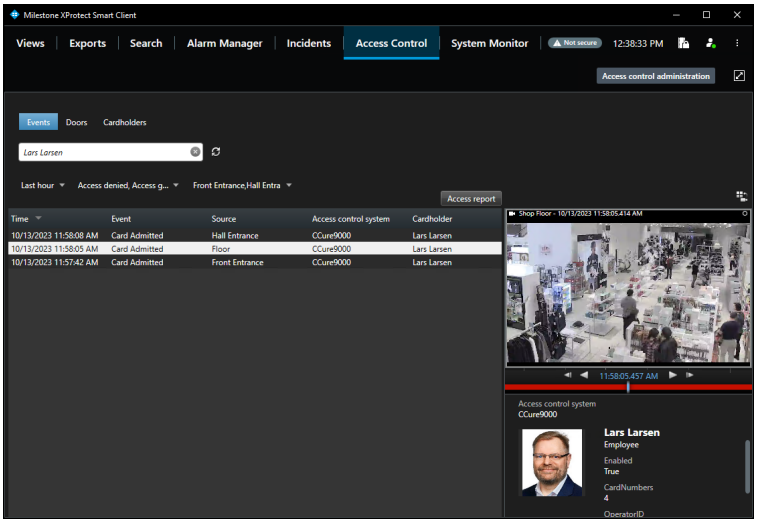
- This window provides a directory of all the CCure hardware in the system.



6. 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).
7. 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.

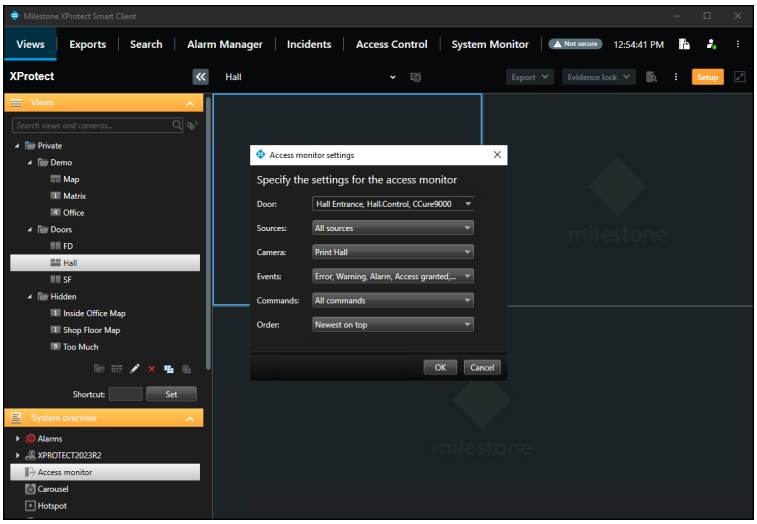
Access control workspace cardholders list

1. Go to the **Access Control** workspace of the Smart Client and select the **Cardholders** list.
2. By default, all cardholders in the system are displayed in the list.
3. Filter for specific cardholders by typing into the search field.
4. Select a cardholder to view their data.
5. Click the **View cardholder events** button to switch to the **Events** list automatically filtered to display events only from the chosen cardholder.

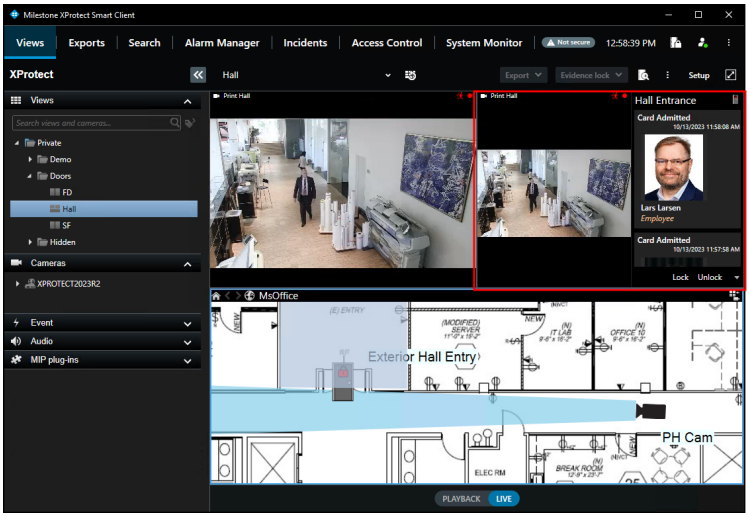


Access monitor

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:



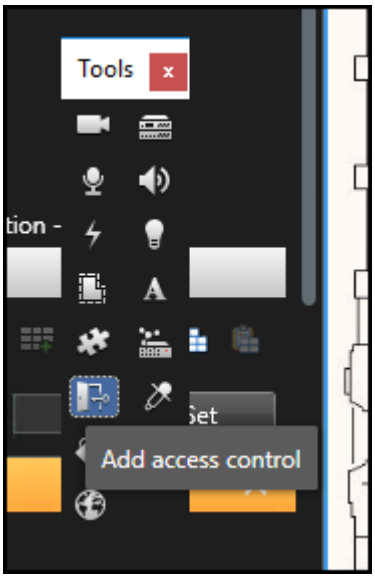
In the **Access Monitor Settings** window, open the lists to select the door, sources, cameras, events, commands, and the order in which new events appear in the access monitor. Once the door is selected, many of the other options will change, based upon the available cameras, events, and commands. The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



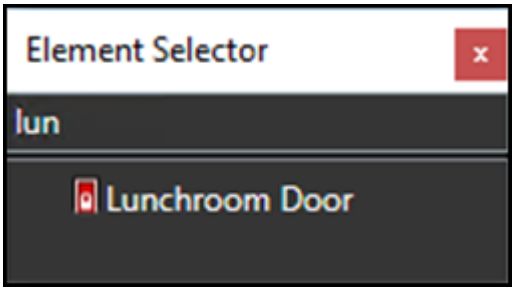
Maps

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.

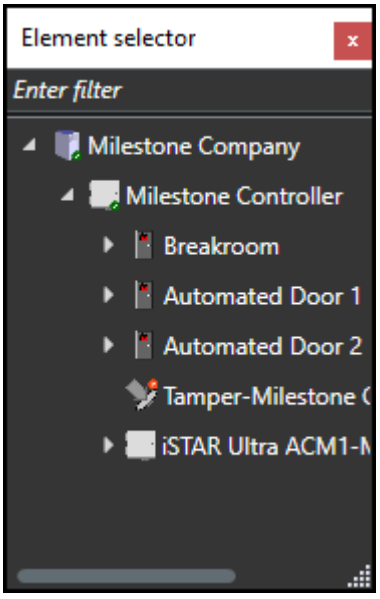
1. With the Smart Client in setup mode a **Tools** window will appear in the view pane.
2. From this window, select the **Add access control** option, which is an icon that looks like a door:



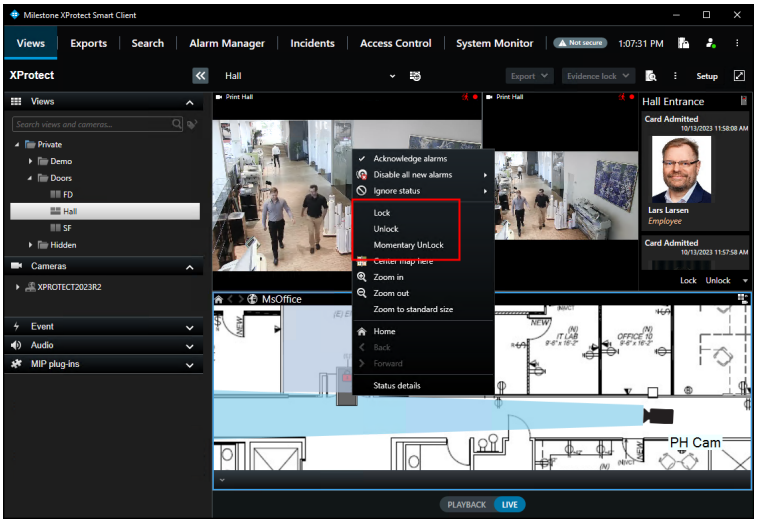
3. The **Element Selector** window will appear.



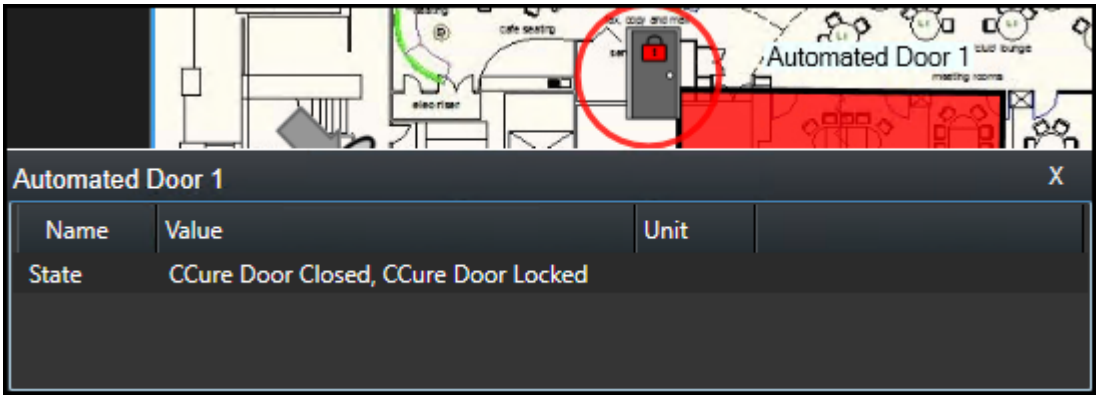
4. Type the name of a hardware device into the filter to quickly find a device or expand the servers and panels to find all available hardware icons in the system.



5. Drag the selected 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.



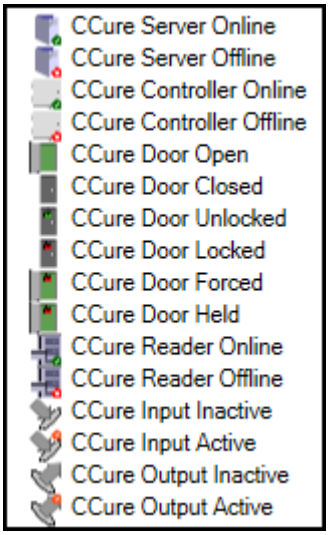
6. Right-click the device icon and select **Status Details** from the shortcut menu to view more information. The pop-up window contains all the device status information in the **Value** field.



The map icons have been redesigned to include more possible status information. If you want to know what all of the possible hardware items and status options are refer to the Map icon hardware and status details on page 64 topic.

Map icon hardware and status details

There are several different types of access control map icons that can be displayed on the standard Smart Client map. Each different type of icon represents a specific type of hardware device. Visual indicators appear on these hardware icons to display the current status of the devices they represent. The different types of hardware and status are listed in the image below.



There is a lot of functionality built into the map feature of the XProtect Smart Client, if you want to review all of the functionality available please refer to the maps section of the Smart Client user guide.

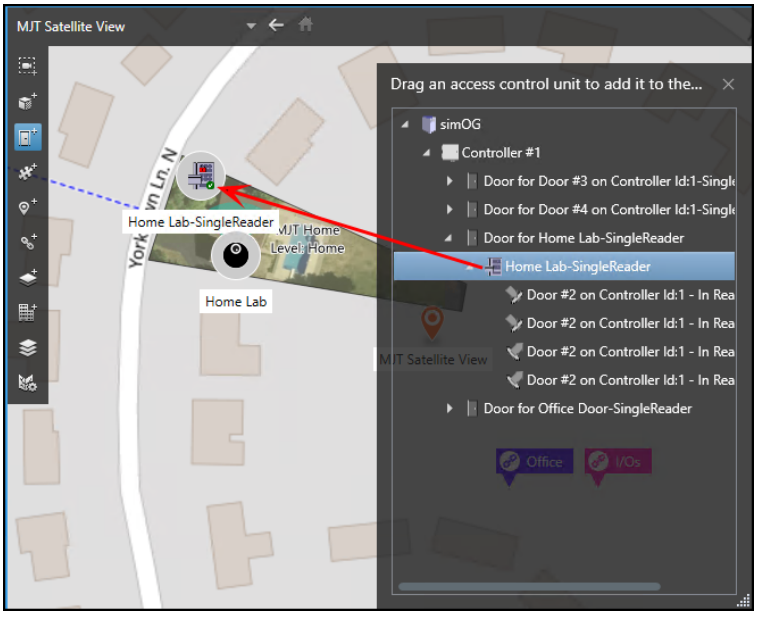
Controllers provide status information to XProtect Access to support display of tamper alarms on those device icons. For supported controllers, a red alarm status ring will appear on the icon when it is being tampered with. When the controller physically returns to a safe state, the alarm status will disappear from the icon.

Smart Map

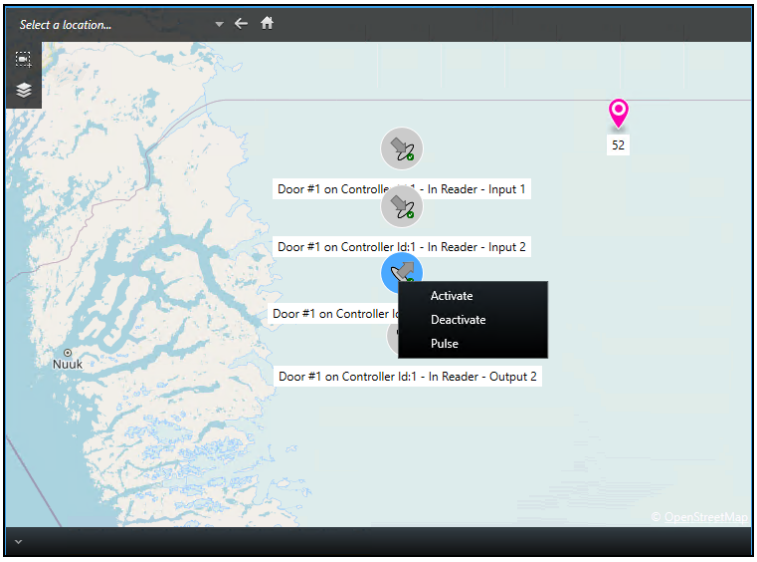
Access control devices can be placed on a Smart Map in the Smart Client. The access control device icons display the status of the devices in real time. It is also possible to interact with the devices through the context menu built into the Smart Map.

The Smart Map feature of the XProtect Smart Client has many capabilities, please refer to the Smart Maps section of the Smart Client user guide.

1. Open a view in the Smart Client that contains the Smart Map.
2. Enter Setup mode. Select the access control device menu icon.
3. Expand the hardware directory and choose a device to place on the Smart Map.

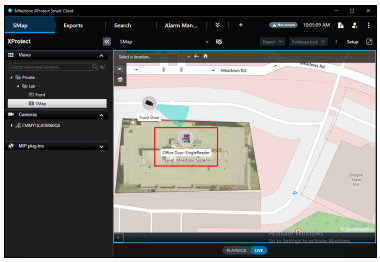
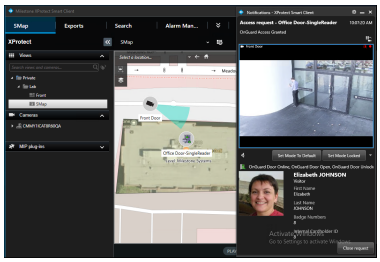
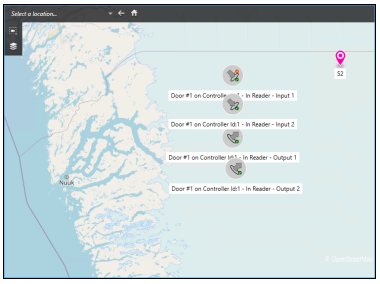


4. Right click on any device icon to choose an option from the context menu.



It is possible to add access control devices to the Smart Map from the GPS coordinates tab of the XProtect Access instance in the Management Client.

Device icons will visibly change status to reflect system events. Doors, readers, inputs and outputs can all be placed on the Smart Map.

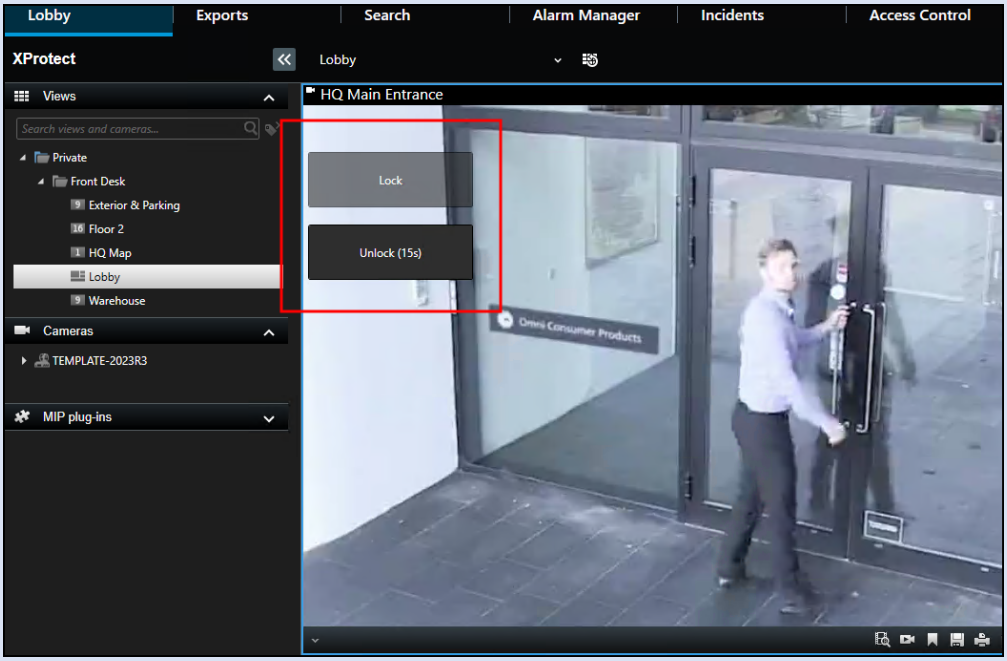
Reader Locked	Reader Unlocked	Input Triggered
		

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. Read more about how overlay buttons work in XProtect here.

Overlay buttons appear as a layer on top of the live video when you move your mouse over the individual view pane. Use overlay buttons to activate device functionality, trigger system events, trigger low-voltage outputs, start recording,...etc. This functionality is extended into the XProtect Access integrations. There are a large number of possible uses for these buttons.

The most common use case for overlay buttons and XProtect Access integrations is to allow experienced video operators the ability to add door lock and unlock functionality to the familiar Smart Client views they use everyday. The ability to add door control (lock/unlock functionality) to live views is a great way to increase the overall functionality of the entire system, and makes the integration between access control and video feel much more seamless from an operational perspective.



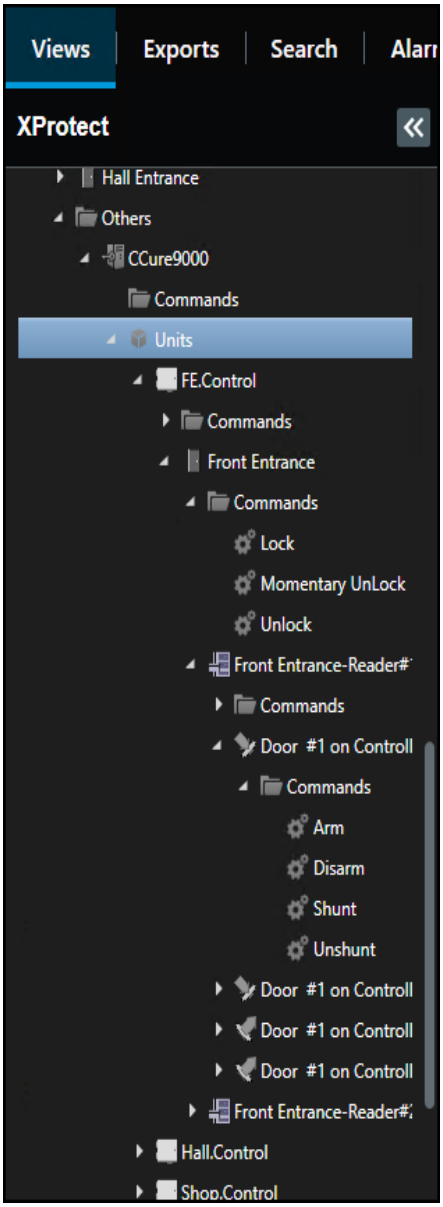
In particular, if customers want to visually verify access requests on highly secure doors, overlay buttons allow anyone who can view live video, to also have the ability to open the doors.

Other use cases can include any functionality connected to the door panel via programmable input and output connections, which can include the following:

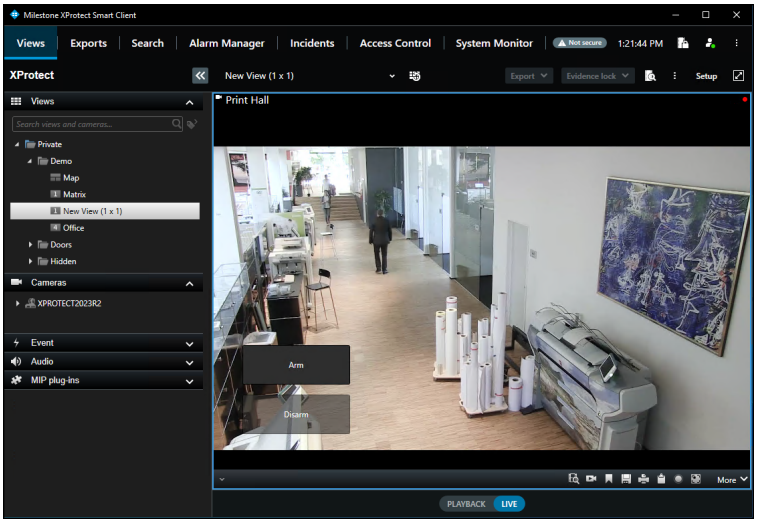
- Control lights or heating/cooling systems.
- Arm/Disarm connected intrusion alarms and other sensors.

Follow this process to add an overlay button to a view:

1. When the Smart Client is in setup mode, there is an **Overlay Buttons** panel on the left side of the client.
2. Select the **Access Control** icon.
3. Expand the **Access Control** icon to find all the doors and readers, panels, and the connected inputs and outputs in the system.

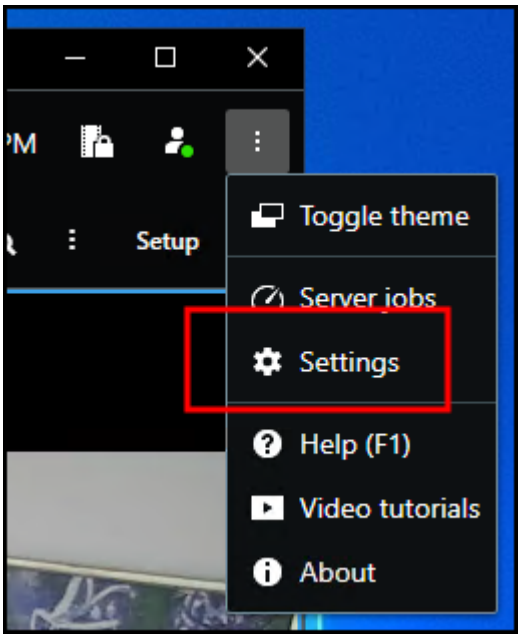


4. Select a command from the list and drag it onto the view pane.
5. Once the commands are visible on a camera view pane they can be resized, moved around, and - with a right click - the name of the command can be edited.

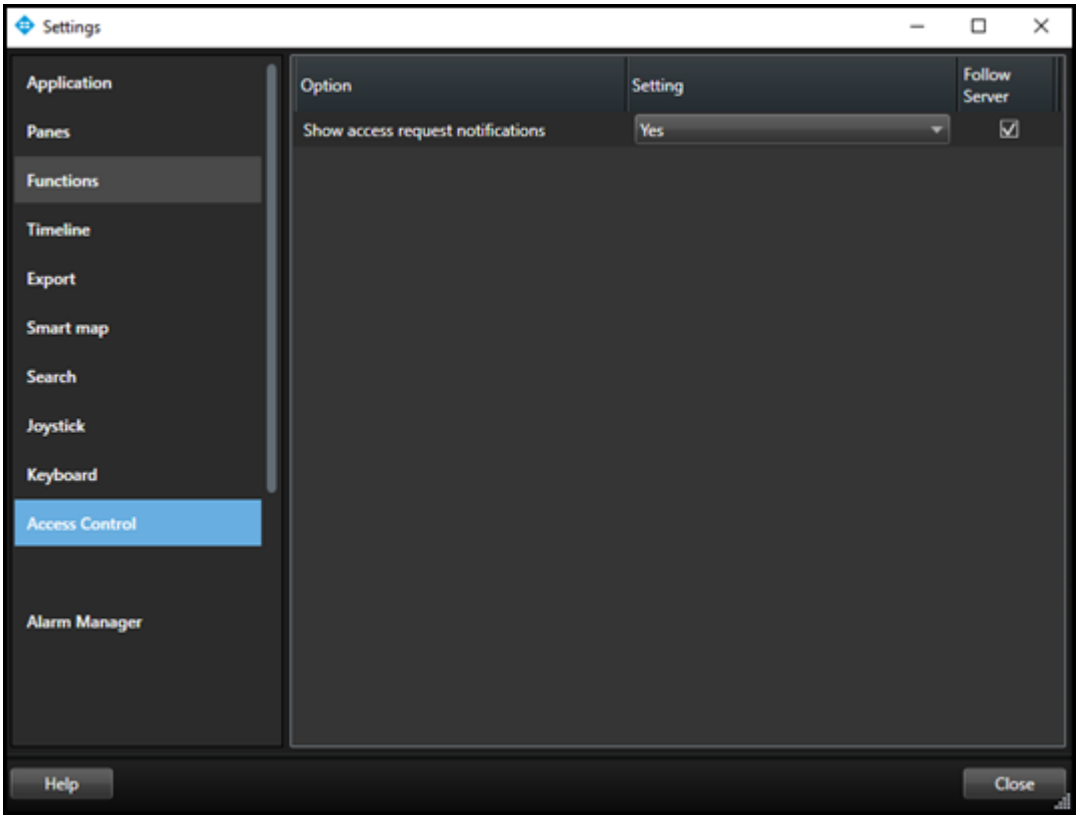


Access control options

In the upper right corner of the Smart Client application is the **Settings and more** button. Click this button and choose **Settings** from the list.



Select the **Access Control** menu in the **Settings** window. Choose to show or block access request notifications in the Smart Client.


Settings
Application
Panes
Functions
Timeline
Export
Smart map
Search
Joystick
Keyboard
Access Control
Alarm Manager
Option
Setting
Follow Server
Show access request notifications
Yes
Help
Close

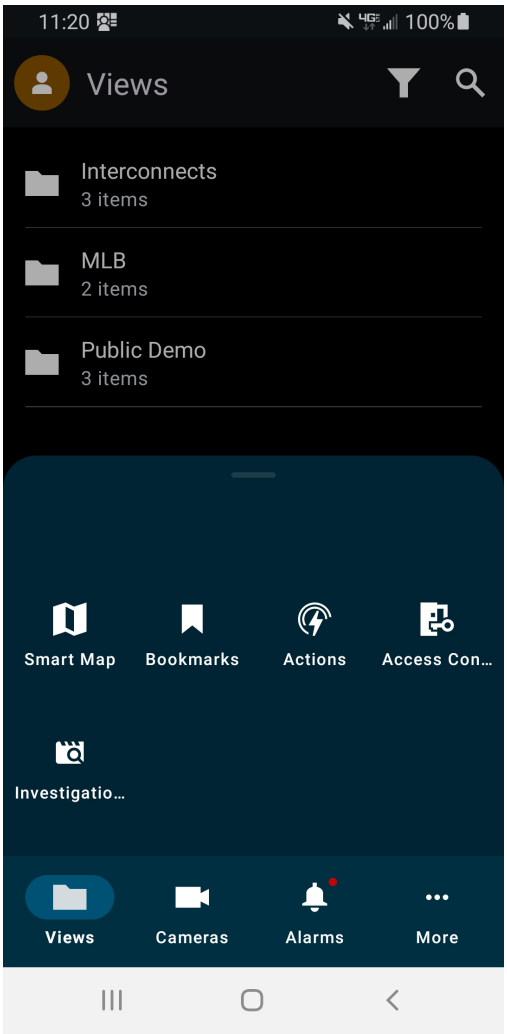
Mobile Client

XProtect Mobile

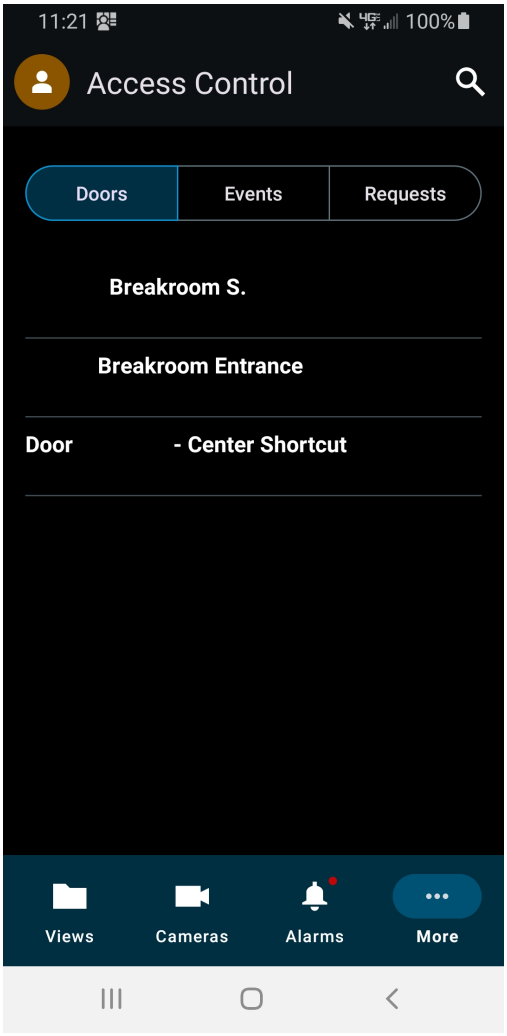
XProtect Mobile is a smartphone app that connects to your VMS system. The XProtect Access CCure 9000 Integration adds functionality to XProtect Mobile. Using XProtect Mobile, it is possible to receive a push notification from the access control system, view live video related to the notification, and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

Access control tab in XProtect Mobile

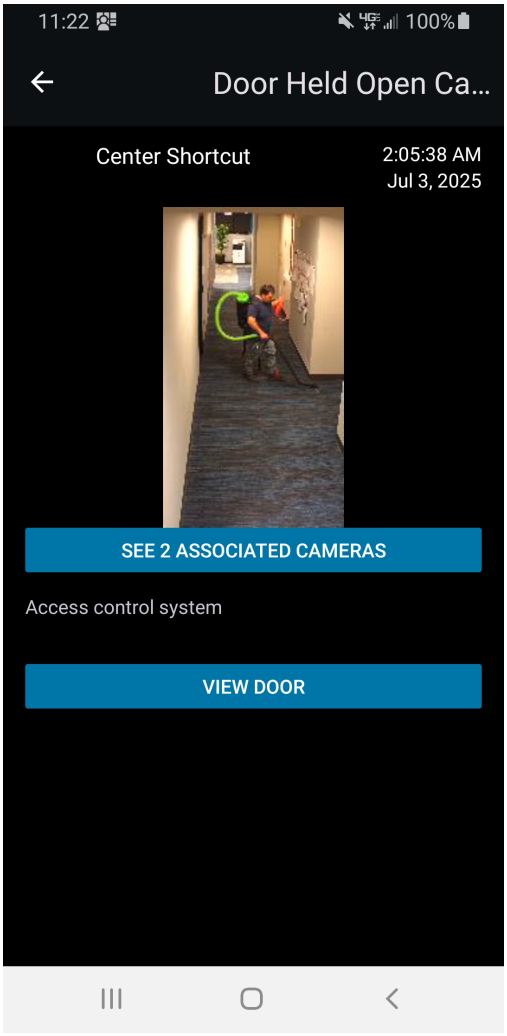
1. Log into the VMS with XProtect Mobile. The **Views** tab is presented by default.



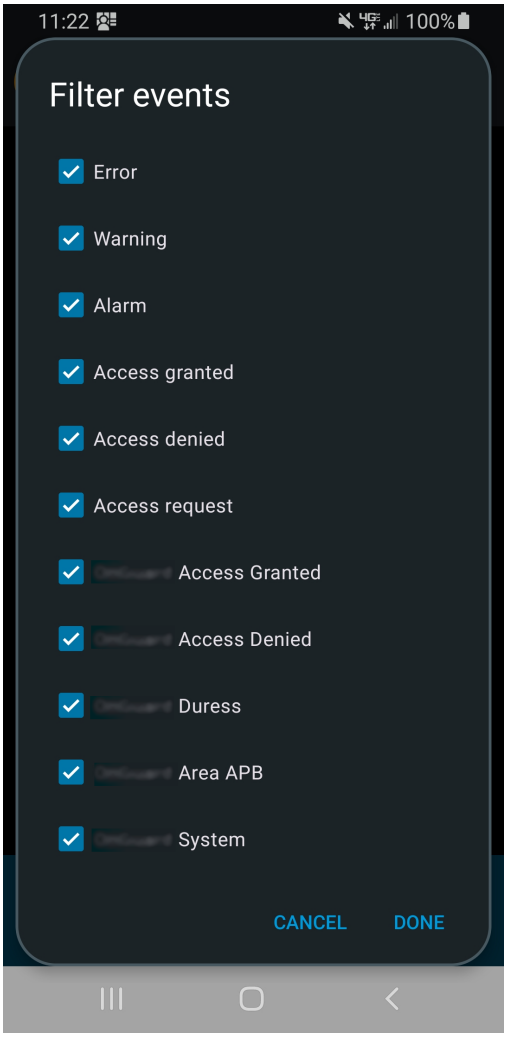
2. Select the **More** button, and the **Access Control** button in the menu of more options.
3. The **Access Control** tab shows the list of doors available.



4. Filter for specific doors or select a door to view cameras associated to that door and interact with commands available for the selected door.
5. Swipe to switch between cameras when multiple cameras are associated to a door.
6. Switch between **Doors**, **Events**, and **Access Requests**.
7. Select an event from the event list to view still images associated to the event and playback video related to the event.



8. Filter the event list.



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.

Technical Considerations

Alarm acknowledgment - explained

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

> ⚠ In some scenarios, acknowledging alarms in the XProtect Smart Client may not automatically acknowledge the alarms in the CCure system. In systems using both integrations: (i.e. 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 acknowledgment if they are acknowledged in the CCure Monitoring Station application, and the **Auto-acknowledge alarms** option was selected in the CCure event definition.

1. CCure 9000 to XProtect:

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

2. XProtect to CCure 9000:

- When an alarm is acknowledged in XProtect, the event in CCure 9000 that triggered the alarm will also be acknowledged.
- When using the XProtect Smart Client's **Alarm Manager** tab, right-click an alarm, and select **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 acknowledgment of the alarm in XProtect will impact the alarms status in CCure 9000.

Custom Alarms & Alarm Management

When using custom alarms with the CCure XPA integration there is no way to manage non-closed custom alarms individually. This means that all custom alarms which are not closed (New, Acknowledged, On-Hold) will all be changed when any one of them has it's status changed. For example, if there are two open alarms and one of them is changed so that its status is Acknowledged, both of the alarms will be Acknowledged.

Why does this happen? CCure sends all custom alarms into the XProtect Access integration with identical alarm types and identical alarm IDs. There is no way to implement a workaround that fixes this.

As of the 1.4 CU1 version of the integration, closed alarms have been excluded from all further status changes. So, if a system uses custom alarms and requires alarm management. The only way to manage them effectively is to manage each custom alarm immediately as it comes in, and always close them so they are not further impacted by state changes.

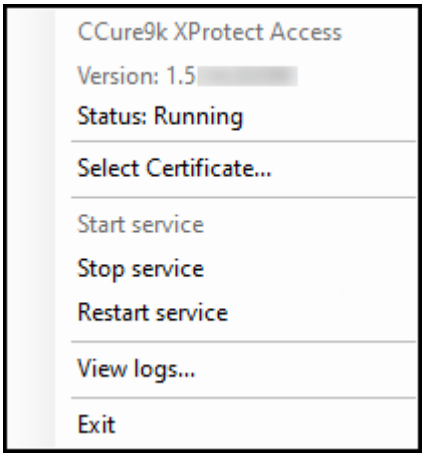
Requirements for alarm acknowledgment

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

1. 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.
2. 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, theCCure 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.
3. The CCure event must be configured to require acknowledgment and must not be in a state that prevents acknowledgment, such as **Latched**.
   - Verify individual event details in the **Configuration** menu of the **Administration Station** application for the CCure 9000 system.

Service tray icon (explained)

The CCure XProtect Access Service, that runs on the CCure server has a service tray icon with a shortcut menu used for viewing status of the service, managing certificates, launching the log viewer, and starting and stopping the service. Right-click the CCure XProtect Access Service service tray icon to view the shortcut menu.



Using the log viewer application

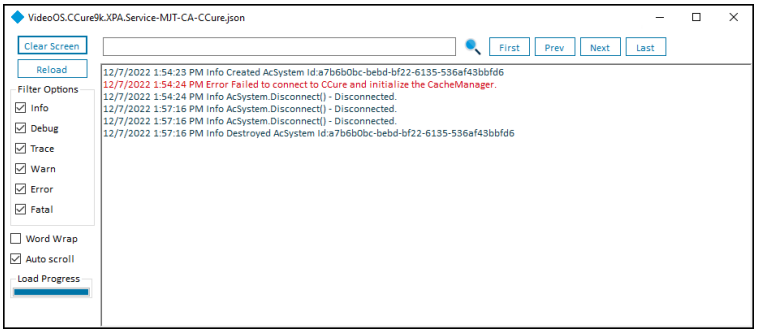
When upgrading the integration, all log levels configured in a non-default level of detail (not Info) are reset to "Info" after the upgrade. Please confirm and reconfigure the log level to the desired setting after the upgrade is complete.

1. Choose the **View logs** option from the shortcut menu of the service tray icon to launch the log viewer.

2. All available log files are in the **Logs List**. Adjust the detail level of the log using the list to the left of the **Open** button. Once you have chosen the level of detail click the **Apply** button to change the log level. The success dialog window pops up when the change is applied.

The available log levels are **Trace**, **Debug**, **Info** (default), **Warn**, **Error**, and **Fatal**. Trace shows the highest level of detail, Fatal shows the least amount of detail.

3. Click the **Open** button to launch a new window used to search through the individual log file.

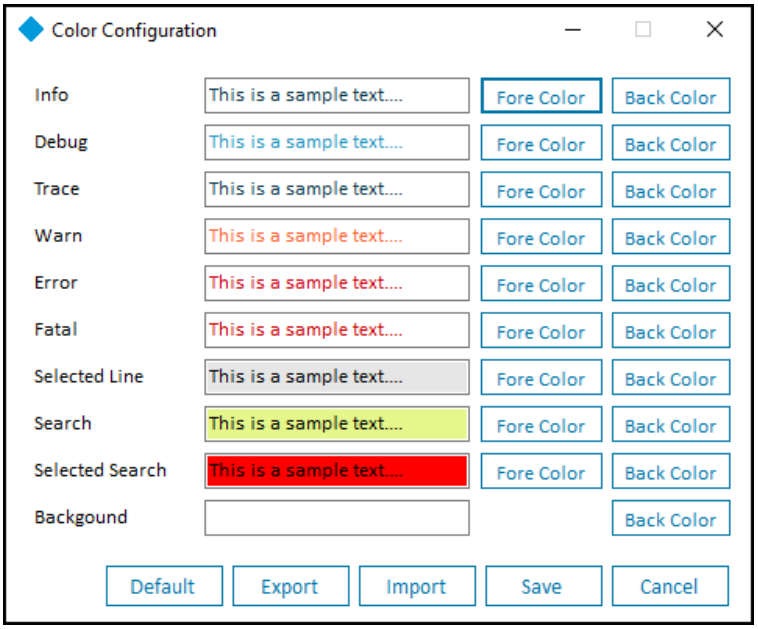


- Type in the text field at the top of the menu and hit enter or click the magnifying glass icon to start a text search. Use the **First**, **Prev**, **Next**, and **Last** buttons in the top right to navigate the search results.
- The **Clear Screen** button empties the main text display window, and the **Reload** button resets the current log file after a search. If the log file is large and takes time to load, the **Load Progress** graph at the bottom left displays the status of the load operation.
- Use the **Filter Options** menu to choose which types of log messages to display.
- The **Word Wrap** and **Auto scroll** options control the appearance and real-time behavior of the main text display window.

4. Click the **Open Log File...** button to launch a file explorer menu set to the local log file location.

> The default location of the log files is C:\ProgramData\VideoOS\VideoOS.CCure9k.XPA.Service\logs

5. Click the **About** button for version information and online access to Milestone support resources.
6. Click the **Color Configuration** button to open the **Color Configuration** menu to create a custom color scheme for the log reader. Custom color schemes are saved, exported, and imported with this menu. The Default button removes any customized configurations and applies the default settings.


Color Configuration
Info
This is a sample text....
Fore Color
Back Color
Debug
This is a sample text....
Fore Color
Back Color
Trace
This is a sample text....
Fore Color
Back Color
Warn
This is a sample text....
Fore Color
Back Color
Error
This is a sample text....
Fore Color
Back Color
Fatal
This is a sample text....
Fore Color
Back Color
Selected Line
This is a sample text....
Fore Color
Back Color
Search
This is a sample text....
Fore Color
Back Color
Selected Search
This is a sample text....
Fore Color
Back Color
Backgound
Back Color
Default
Export
Import
Save
Cancel

Troubleshooting

Basic support checklist

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

Simple items can lead to support calls if overlooked. Below is a short list of those items. First are the items to check on the XProtect Access system, followed by a list of things to verify on the CCure system. For both, make sure the versions of the CCure system and the XProtect system are supported.

XProtect Access

This set of items are helpful for resolving all troubleshooting issues.

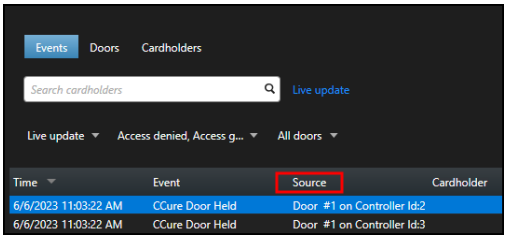
- Check that the doors in XProtect Access are licensed.
- Check that the doors in XProtect Access are enabled.
- Verify the XProtect Access Service is running.
    - Check the service tray icon on the server where the XPA service is installed to verify.

- Make sure the Event Server connection to the XPA service is connected.
- Double check that the credentials used for the victor web service user and password fields are correct.

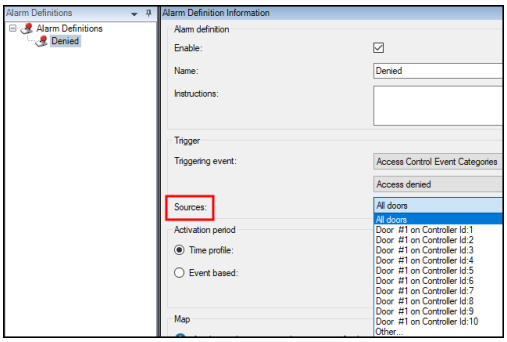
The next set of issues are helpful for issues related to events, alarms, and status changes not being received between the two systems.

- Verify all required doors and other devices from the CCure system are added to the XProtect Access system.
    - As devices change over time, it's suggested to refresh the configuration from the General Settings tab.
- Check that events are displayed in the Smart Client access control workspace Events List.
    - Make sure there are no filters applied which might be changing the results.
- Check that events are being displayed in the Management Client when the Live Events dev tab is displayed.

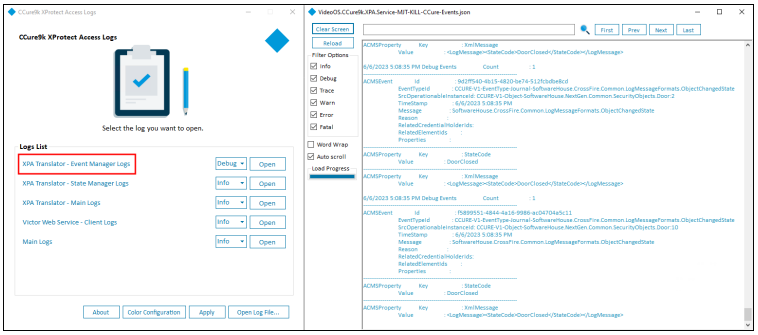
- Match the Source of events appearing in the Smart Client access control workspace to any Alarms defined in the Alarm Definition menu of the Management Client.
    - Smart Client event source location:



    - Management Client Alarm Definition source location:



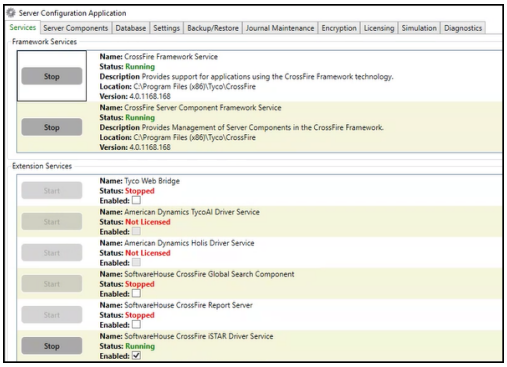
- Open the log viewer application and check the following logs to verify your events are received by the XProtect Access Service:
    - XPA Translator - Event Manager Logs
        - Change the log level to Debug and Apply the change. Send some events into the system and then Open the log file.



    - Open the MIP Plugin logs at this location to verify that the events are received by the Event Server:
        - C:\ProgramData\VideoOS\VideoOS.CCure9k.XPA.MipPlugin\VideoOS.Event.Server\logs

CCure

- Check that the required CCure 9000 services are running. Open the Server Configuration Application and check that these services are **Running**.
    - CrossFire Framework Service
    - CrossFire Server Component Framework Service
    - SoftwareHouse CrossFire iSTAR Driver Service

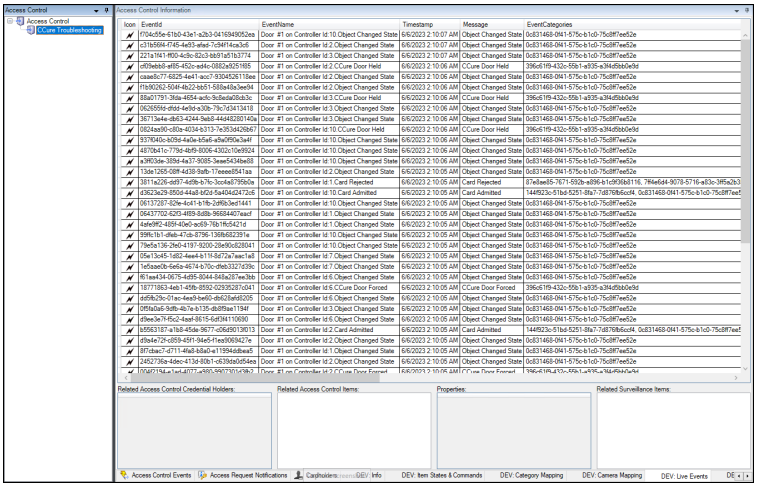


- Verify the victor web service is running.

> It is also possible to obtain victor web service SDK samples which can be used to test and validate the performance of the CCure integration. These samples, and the SDK itself can be downloaded from the CCure 9000 Connected Partner Program portal. Once logged into the portal download the Partner Package for the version of CCure you have installed, and the SDK and the samples will be included.

XProtect Access developer tabs (explained)

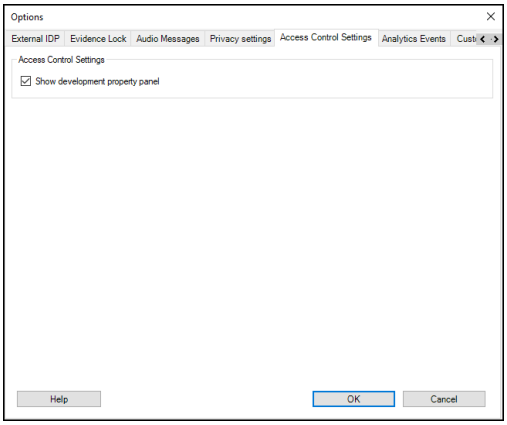
Hidden tabs are built into the XProtect Access instance in the Management Client. These tabs contain helpful information when troubleshooting.



Enabling developer tabs

Take these steps to enable the hidden developer tabs built into the XProtect Access instance.

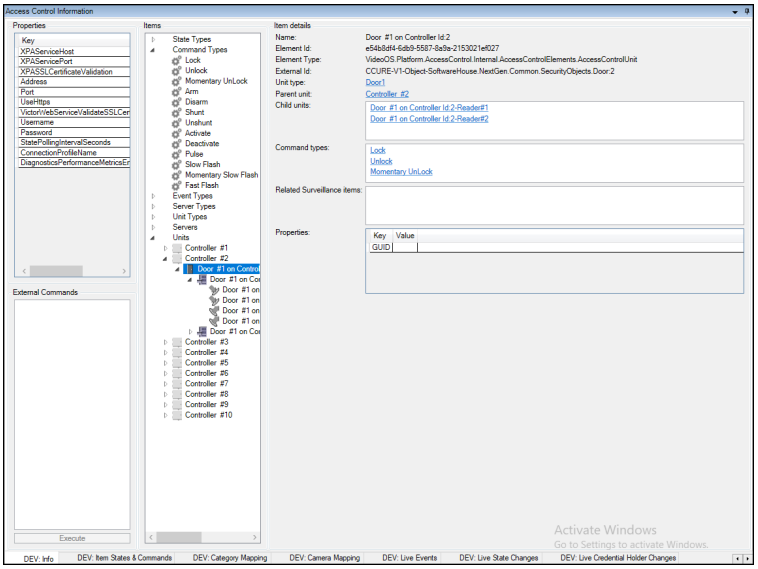
1. Select **Options** from the **Tools** menu of the Management Client.
2. Go to the **Access Control Settings** tab of the **Options** dialog and select the **Show development property panel** option.



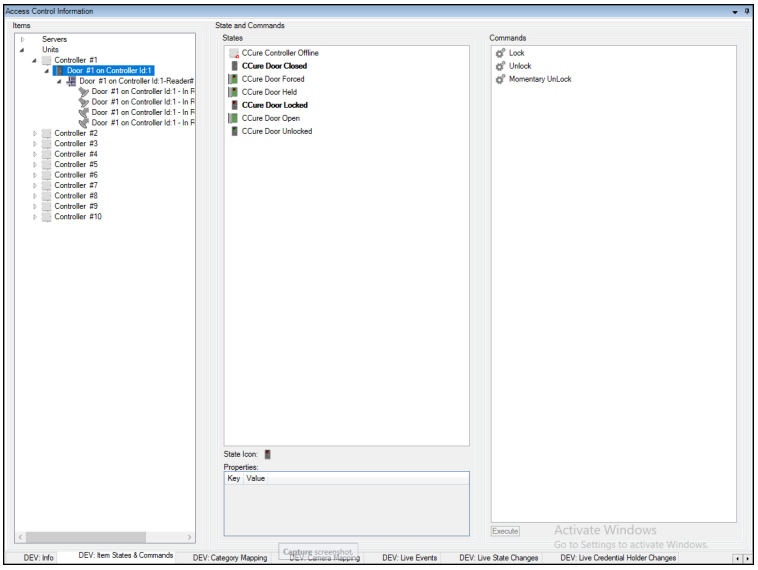
Developer tabs (reference)

Below is a description of how to use each of the hidden developer tabs available within the XProtect Access instance.

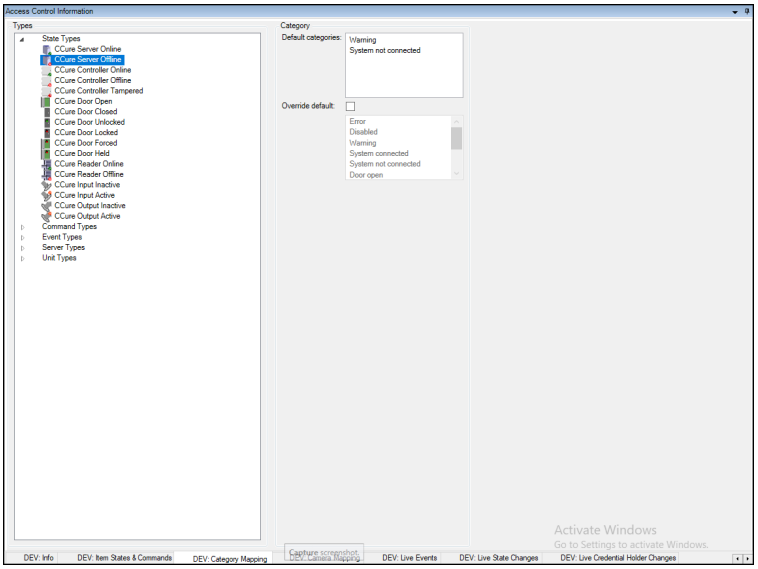
Tab Name	Description
DEV: Info	This tab has the entire hierarchy of servers, devices, statuses, commands, and events in the system. Selecting an individual object allows for identification of any properties associated to it.



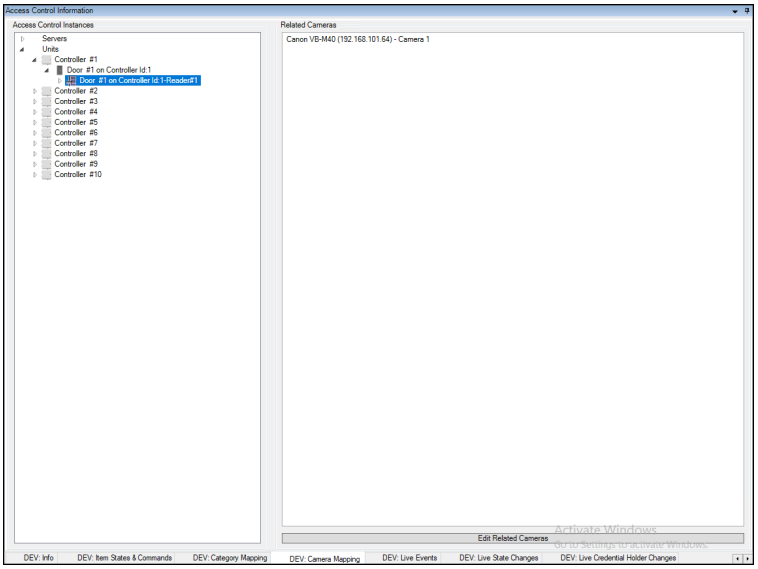
DEV: Item States & Commands	This tab shows all devices and servers in the system. Select a device or server to view all associated commands and possible statuses. The current state of the device or server is displayed in bold.



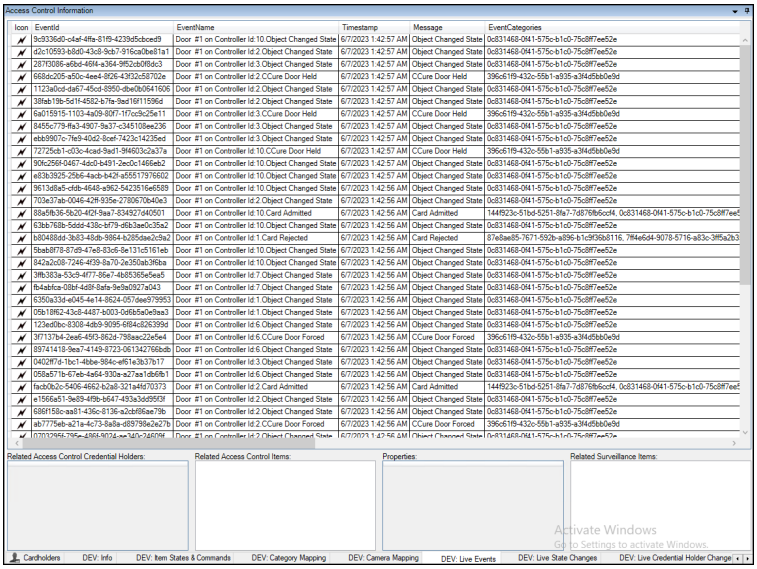
DEV: Category Mapping	The Category Mapping tab is primarily used for debugging during development making sure that the Events, Commands, States, Servers, and Devices are mapped correctly between CCure and XProtect.



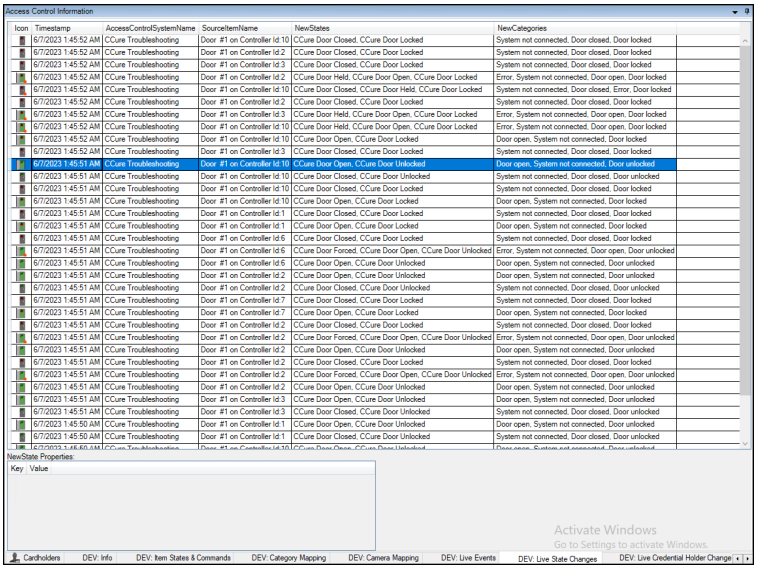
DEV: Camera Mapping	This tab displays the current camera to device mapping used in the XProtect Access instance.



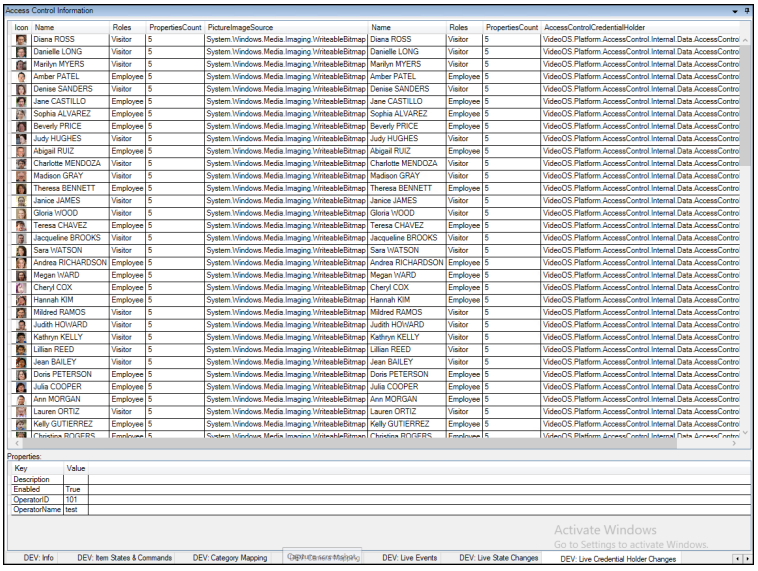
DEV: Live Events	This tab will display live events as they're received by the XProtect Access system when selected. If the client is closed, or the user switches to another view, the Live Events tab won't retain any memory of the events displayed. This memory-less behavior is something all three Live tabs have in common.



DEV: Live State Changes	This tab displays the live status changes of devices and servers. This tab has no memory.



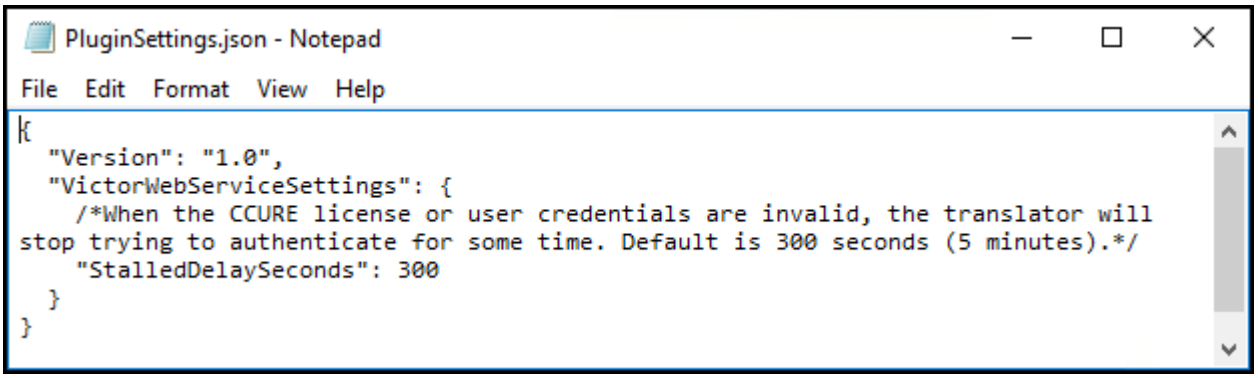
DEV: Live Credential Holder Changes	This tab shows all credentials added to the XProtect Access system. This tab has no memory.



Failed log-in cool-down setting

Repeat failed log-in attempts of the CCure XProtect Access Service account as it attempts to log into the CCure 9000 system can trigger internal security policies and lock the service account - preventing successful authentication. To prevent this a **PluginSettings.json** file is installed on the same machine where the CCure XProtect Access Service is installed. This JSON file defines the time allowed between log-in attempts. The default is 300 seconds, or 5 minutes, and the plugin settings JSON file can be found at this location:

C:\ProgramData\VideoOS\VideoOS.CCure9k.XPA.Service\Translators\CCure

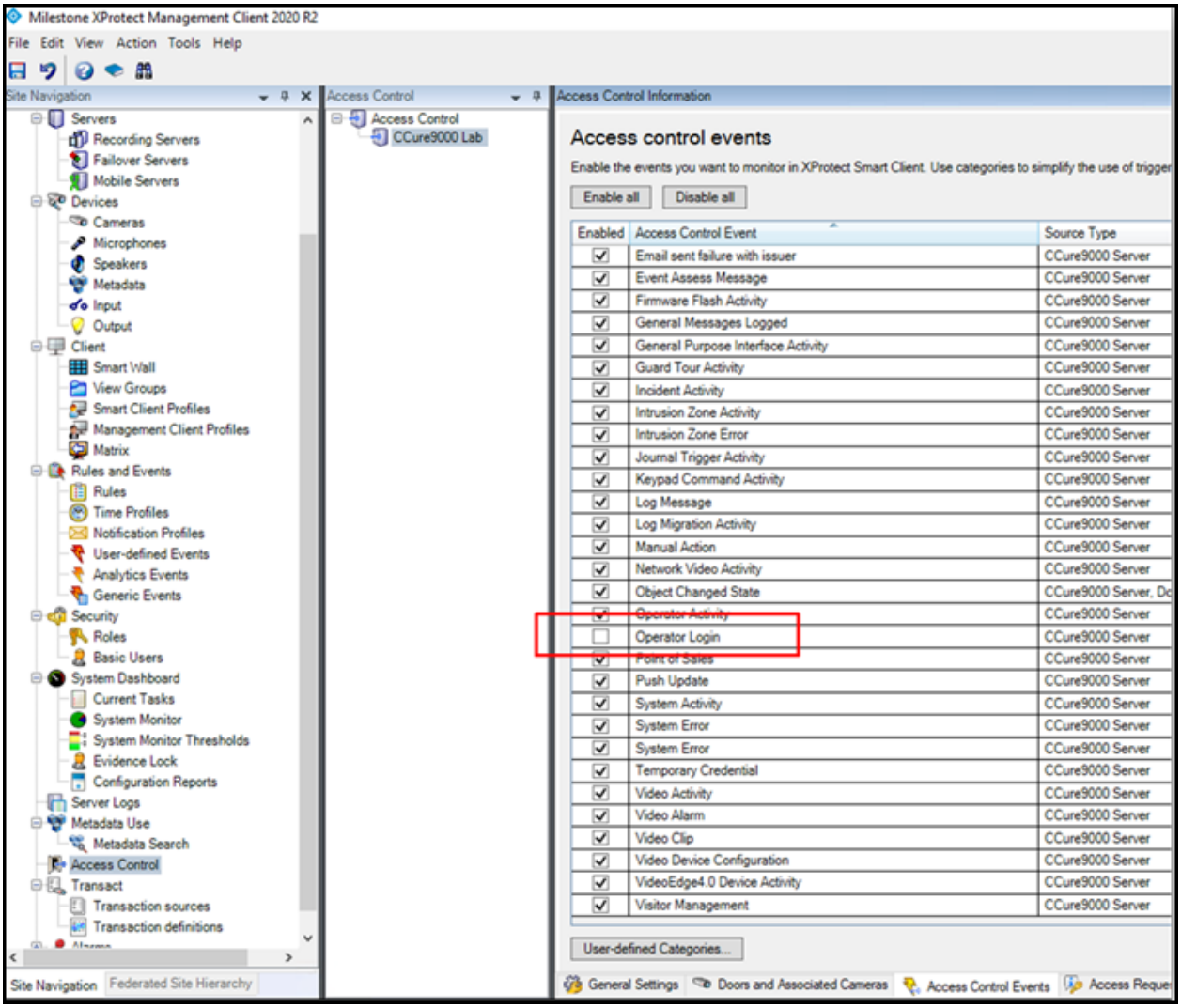


Upgrading from 1.1 with operator login events

For integrated systems upgrading from version 1.1 of the XProtect Access plugin to the 1.3 or higher 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 current versions.

To check status of this event:

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



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 XProtect Access integration monitors.

However, this default behavior only changes on newly created XProtect Access 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.

Upgrade to Plugin version 1.4 or newer fails

If the upgrade installation to the latest plugin, or any plugin version 1.4 or newer, fails, and the CCure 9000 system has already been upgraded to version 3.00.1 or higher (3.10 included), there is a simple workaround available to fix this scenario. Here we will describe why this happens and how to fix the situation.

For versions of the integration 1.4 and newer there is a new license requirement, these plugins are only designed to work with the web service API license type. Older plugins (1.3 or lower) were able to work with the previous license type - SDK license. It is recommended to first upgrade the XPA plugin software prior to upgrading the CCure system from a version that used the SDK license (2.9 and older) to a version that uses the web service API license (3.00.1 and higher). However, in situations where the XPA plugin was not able to be upgraded prior to the CCure software upgrade there is a way to fix this situation.

The following process will restore the XPA integration functionality, if the upgrade to the latest plugin fails because the CCure software was upgraded before upgrading the plugin.

1. Locate and rename the following .dll file on the CCure server: **C:\Program Files (x86)\Tyco\CrossFire\SoftwareHouse.CrossFire.Common.Objects.dll**
2. Uninstall the older version of the plugin (1.3 or older) using the Control Panel uninstall process.
3. Change the .dll file name back to its original name.
4. Install the desired latest version of the XPA plugin.

CCure 9000 XProtect Access instance not displayed in XProtect Management Client

If XProtect is unable to communicate with the CCure 9000 XProtect Access 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 XProtect Event Server
3. Stop the Milestone XProtect Access Service
4. Ensure CCure 9000 is running successfully. This may require restarting services.
5. Start the Milestone XProtect Access Service
6. Start the XProtect Event Server and wait for it to fully start.
7. Start the Management Client

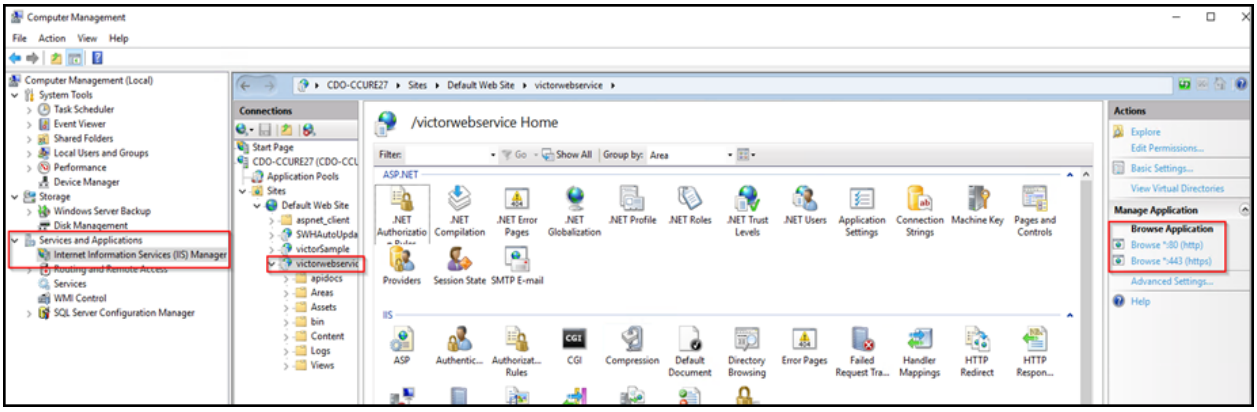
If the instance still does not appear in the Management Client, investigate the logs (see Using the log viewer application on page 77) to discover the specific cause.

CCure 9000 XProtect Access integration looking for secure connection with victor web service

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

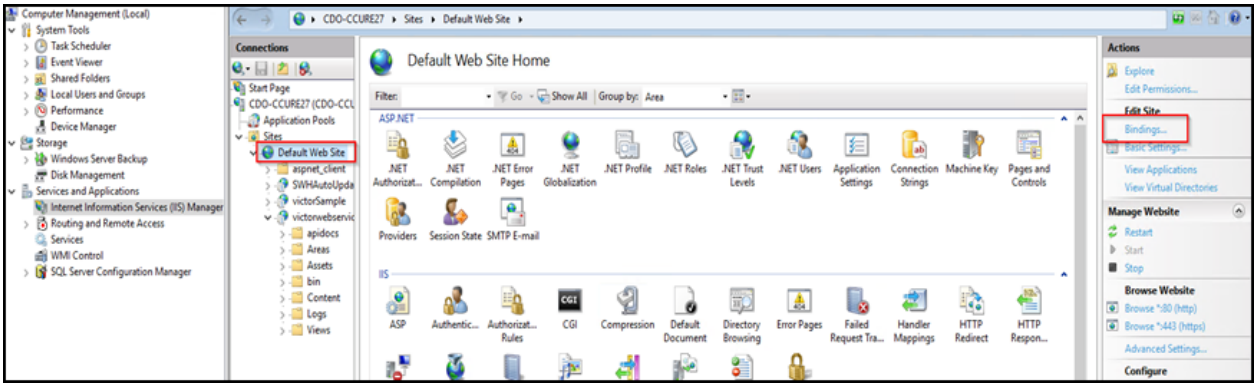
A certificate must be provided and configured in IIS for the CCure 9000 victor web service to accept secure HTTPS connections on port 443. Contact CCure 9000 engineering and support resources to verify the CCure 9000 system is configured to enable secure communications.

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.

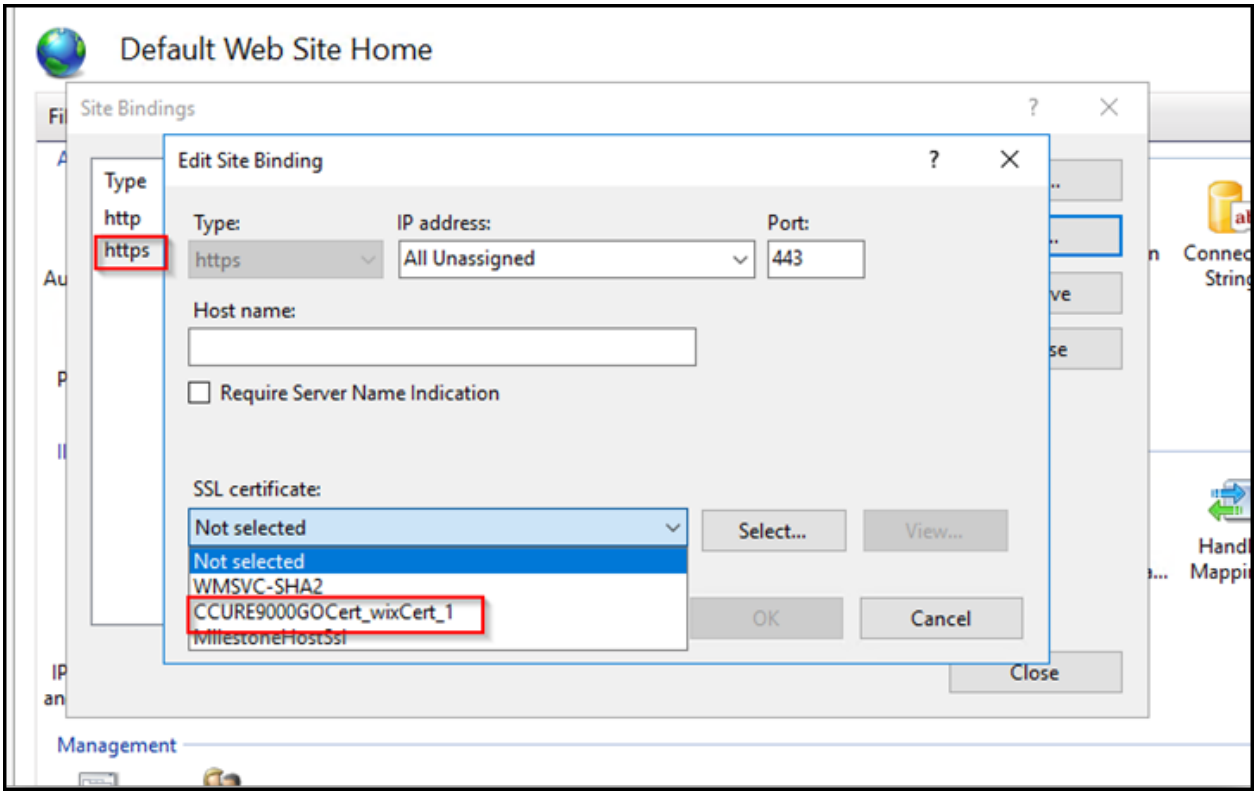


Select the **Services and Applications** directory and the **Internal Information Services (IIS) Manager** menu. Expand the directory to find the **victorwebservice** website. Click on the **browse *.443** link to validate if HTTPS is working. This opens a browser and authenticates using TLS at the specified 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 select **https (port 443)** and click **Edit**. Open the **SSL certificate** list and select the appropriate certificate. The certificate allows authentication using secure ports (443).



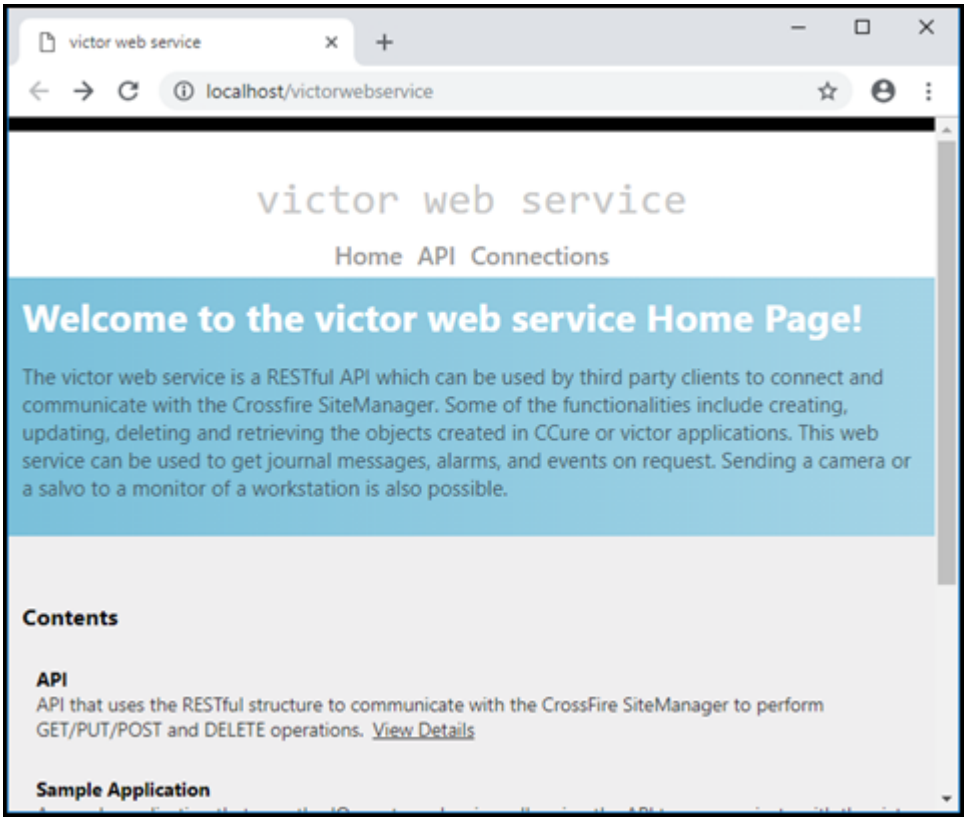
CCure 9000 XProtect Access instance cannot communicate with CCure 9000

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:

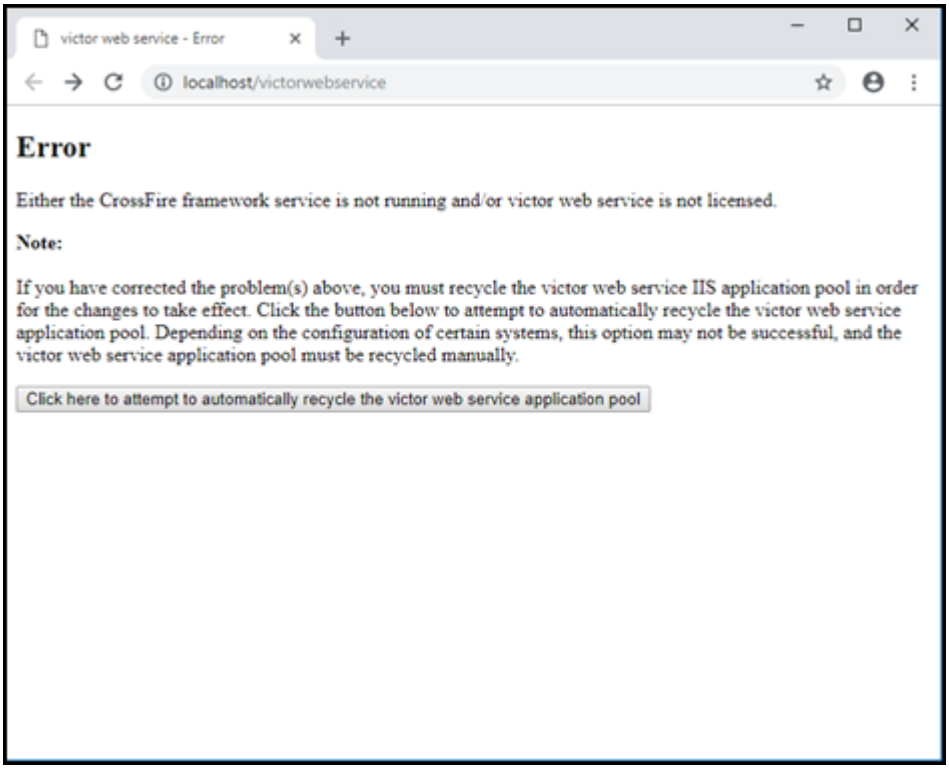
1. Go to the CCure 9000 server
2. Open a web browser and go the address below:

- **http://localhost/victorwebservice/**

3. If the browser opens a page similar to the one below, everything is okay with the victor web service



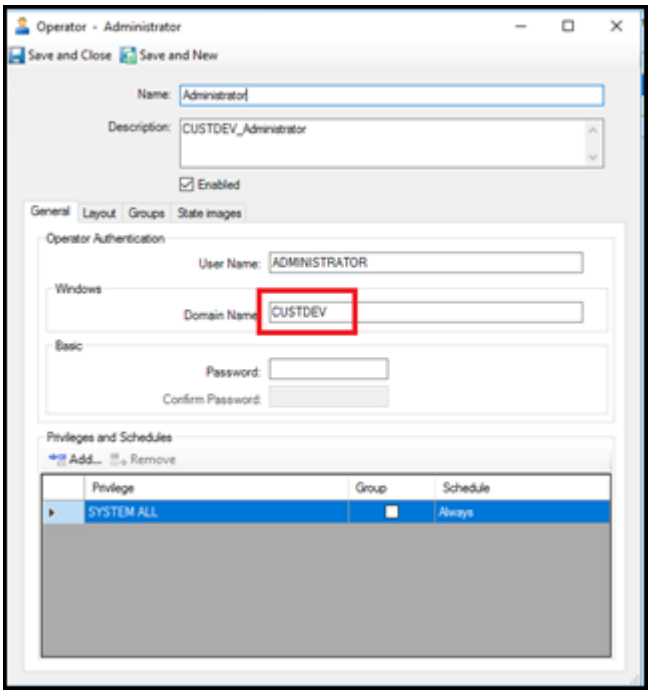
4. If the browser leads to an error message similar to the one seen below, click the button shown on the page to recycle the victor web service application pool



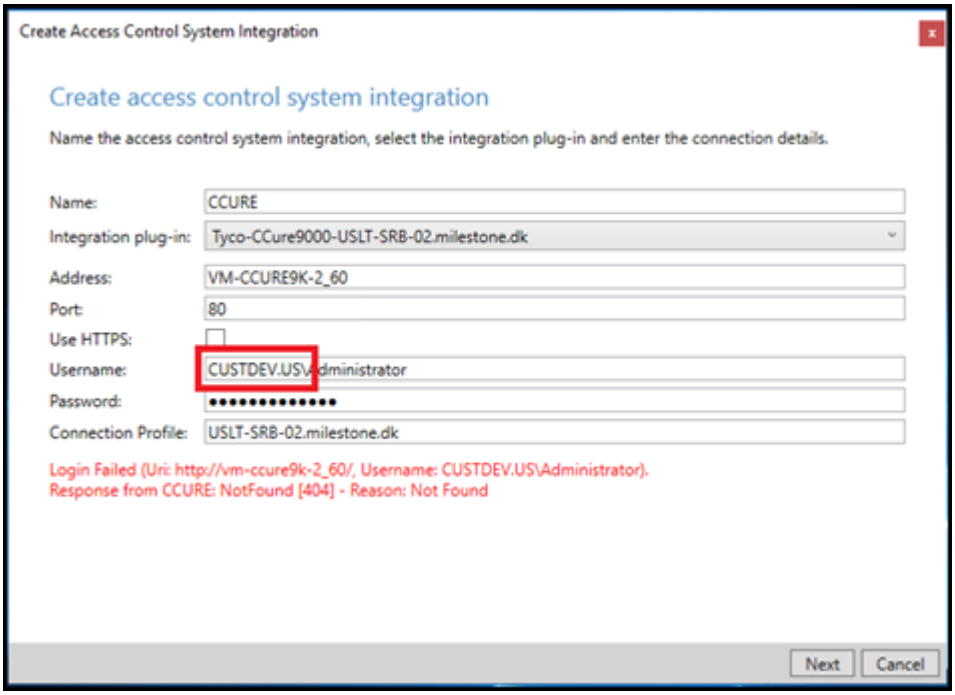
Login fails with CCure 9000 when using a multipart domain user

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.

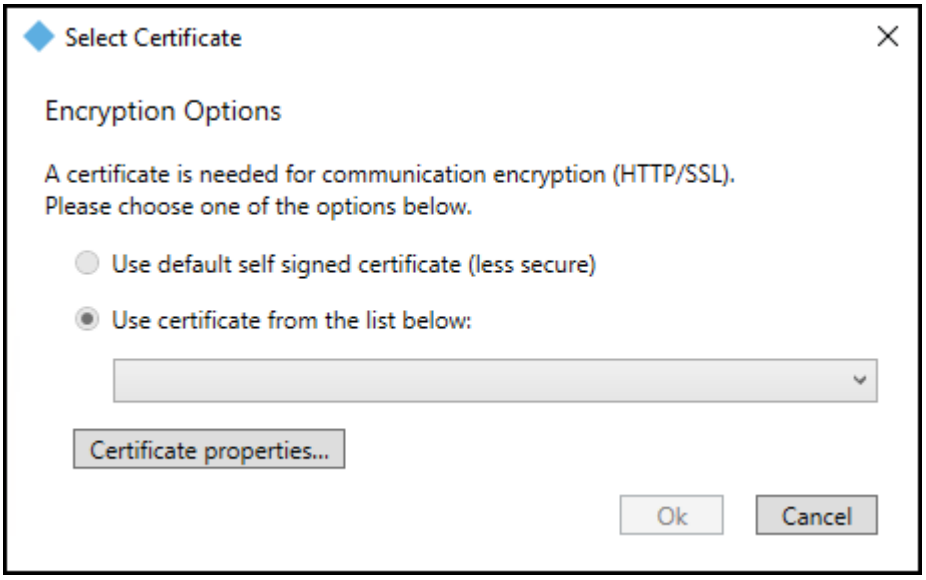


The same exact domain name protocol must be used in both places for login to succeed.

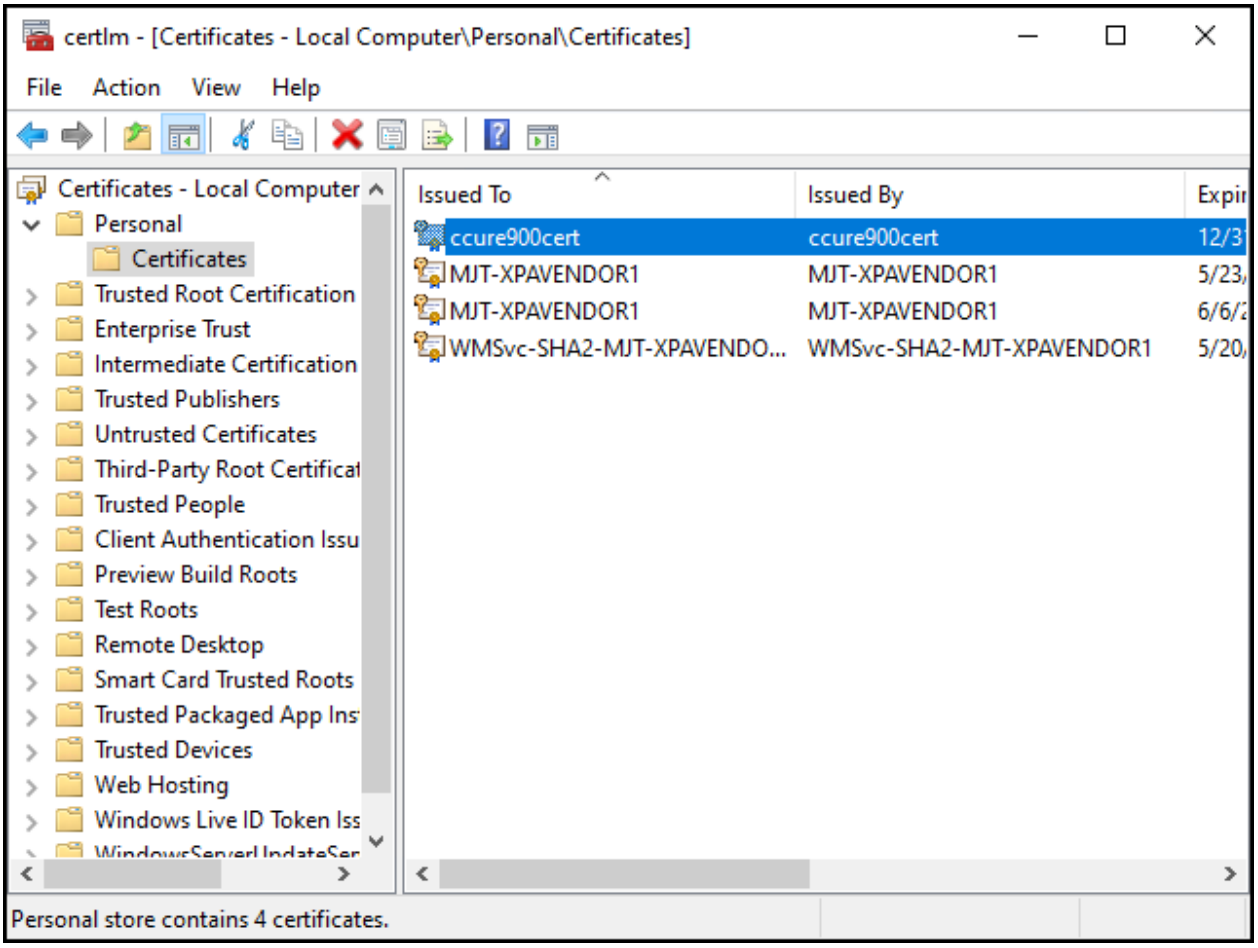
No certificates available in Select Certificate window

After installing the XProtect Access service on the CCure 9000 server there may be no certificates available in the **Select Certificates** window. This topic explains why this can happen, and how to fix it.

1. If there are no options available to select, or simply no valid certificates for use, you may notice because both the default and third party options are unable to be selected.



2. Check to make sure that the XProtect Access service installed on the CCure 9000 server is running. If the service hasn't started after the initial install, it won't have been able to check for available certificates.
3. It is possible that the default certificate, and any third party certificates, were removed or misplaced from the local personal certificate store. Check the local personal certificate store for certificates.
4. Run the **certlm.msc** command, expand the **Personal** folder and select the **Certificates** folder to view all available certificates.



If you need to create a new self-signed certificate, or install a new third party certificate, please refer to the XProtect VMS certificates guide:

https://doc.milestonesys.com/2023r1/en-US/portal/htm/chapter-page-certificates-guide.htm

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 2.80 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 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.

```
# Run this script once, to create a certificate that can sign multiple server SSL certificates

# Private certificate for signing other certificates (in certificate store)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyusageProperty All `
                                            -KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS CA Certificate' `
                                            -TextExtension @("2.5.29.19={critical}{text}ca=TRUE")

# Thumbprint of private certificate used for signing other certificates
Set-Content -Path "$PSScriptRoot\ca_thumbprint.txt" -Value $ca_certificate.Thumbprint

# Public CA certificate to trust (Third-Party Root Certification Authorities)
Export-Certificate -Cert "Cert:\CurrentUser\My\$($ca_certificate.Thumbprint)" -FilePath "$PSScriptRoot\root-authority-public.cer"
```

```powershell
# Run this script once for each server for which an SSL certificate is needed.
# Certificate should be executed on the single computer where the CA certificate is located.
# The created server SSL certificate should then be moved to the server and imported in the
# certificate store there.
# After importing the certificate, allow access to the private key of the certificate for
# the service user(s) of the services that must use the certificate.

# Load CA certificate from store (thumbprint must be in ca_thumbprint.txt)
$ca_thumbprint = Get-Content -Path "$PSScriptRoot\ca_thumbprint.txt"
$ca_certificate = (Get-ChildItem -Path cert:\CurrentUser\My\$ca_thumbprint)

# Prompt user for DNS names to include in certificate
$dnsNames = Read-Host 'DNS names for server SSL certificate (delimited by space - 1st entry is also subject of certificate)'
$dnsNamesArray = @($dnsNames -Split ' ' | foreach { $_.Trim() } | where { $_ })

if ($dnsNamesArray.Length -eq 0) {
    Write-Host -ForegroundColor Red 'At least one dns name should be specified'
    exit
}
$subjectName = $dnsNamesArray[0]
$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Join '&'

# Optionally allow the user to type in a list of IP addresses to put in the certificate
$ipAddresses = Read-Host 'IP addresses for server SSL certificate (delemited by space)'
$ipAddressesArray = @($ipAddresses -Split ' ' | foreach { $_.Trim() } | where { $_ })
if ($ipAddressesArray.Length -gt 0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Join '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}

# Build final dns entries string (e.g. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={text}$dnsEntries"

# The only required purpose of the sertificate is "Server Authentication"
$serverAuthentication = '2.5.29.37={critical}{text}1.3.6.1.5.5.7.3.1'

# Now - create the server SSL certificate
$certificate = New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificate `
                                         -FriendlyName 'VMS SSL Certificate' -TextExtension @($dnsEntries, $serverAuthentication)

# Export certificate to disk - protect with a password
$password = Read-Host -AsSecureString "Server SSL certificate password"
Export-PfxCertificate -Cert "Cert:\CurrentUser\My\$($certificate.Thumbprint)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password

# Delete the server SSL certificate from the local certificate store
$certificate | Remove-Item
```

helpfeedback@milestone.dk

About Milestone

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 Systems 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 Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.