Brivo Access Control Module for XProtect Installation, Setup, and User Guide

Brivo and Milestone have developed this integration to allow our mutual customers to benefit from closer communication between our systems. Below is a step-by-step guide for dealers detailing the pre-requisites for enabling this integration.

I Pre-Requisites

II Configuration

Pre-Requisites

Software and Licensing

- Microsoft® Windows® 10 Pro (64 bit)
- Microsoft® Windows® 10 Enterprise (64 bit)
- Microsoft® Windows® 10 Enterprise LTSB 2016 (version 1607 or later)
- Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core
- Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard, and Datacenter
- Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard, and Datacenter

Milestone XProtect System Requirements

- Must be a Licensed Milestone Dealer
- XProtect Express+, Professional+, Expert, Corporate 2020 R1 (20.1a) or above
- Milestone Event Server - The Event Server is included as part of your Milestone installation

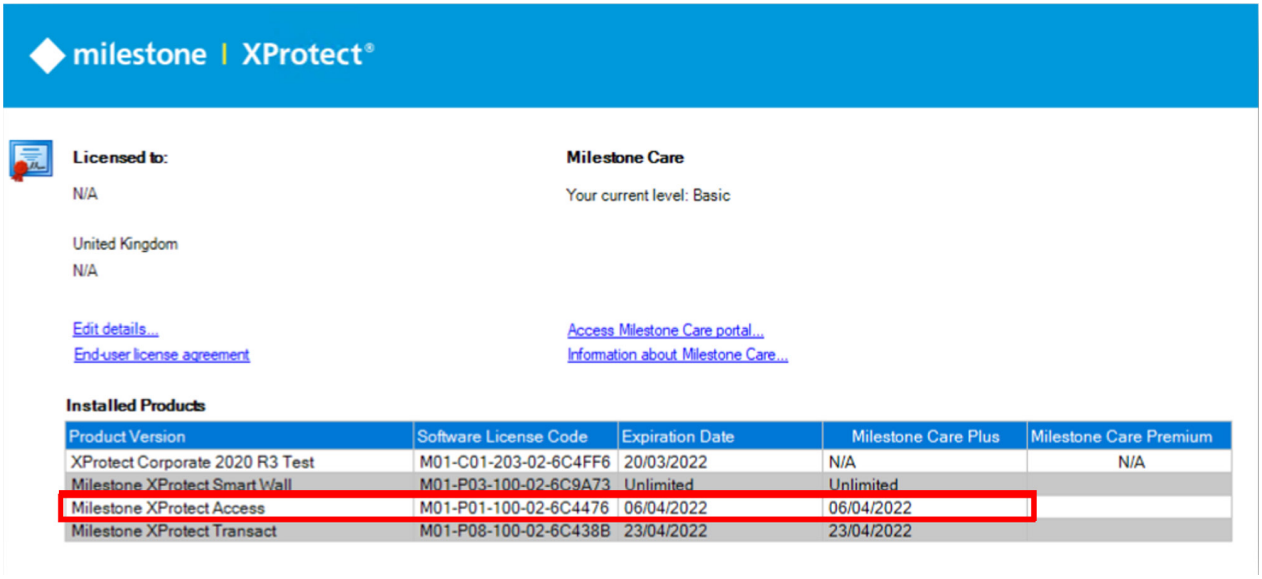
  Note - If this component has not been installed with your version, follow steps found in troubleshooting at the end of this document.

- Milestone Access Licenses applied to your XProtect base license - XProtect Access does not run as a trial license by default. If you want to add a trial license to your XProtect license, you must consult Milestone Sales Support at purchase@milestonesys.com or create a sales request on the Milestone website. Otherwise, purchase from a Milestone partner as below.

Licenses

SKU ID	Name	MSRP (EUR)
XPABL	XProtect Access Base License (BL)	129.00
XPADL	XProtect Access Door License (DL)	39.00

Open the Milestone Management Client and ensure that you have XProtect Access Licenses associated with the installed Milestone version before installation of a ORBNET trial system. If nothing is listed here then you will not be able to use the ORBNET Systems Plugin as XProtect Access is not enabled as part of the trial version of the ORBNET installation, you must request a trial license or purchase beforehand from Milestone.



Brivo Access

- Super Administrator account access to Brivo Access
- Administrator created for Brivo Access with correct role and door access for integration
- API Key which needs to be requested from Brivo
- Application API Client ID and Client Secret generated via Brivo Onair
- Brivo Access subscription for Milestone XProtect Access Integration

Orbnet Systems

- Installer – 'Brivo Access for XProtect Setup.msi'

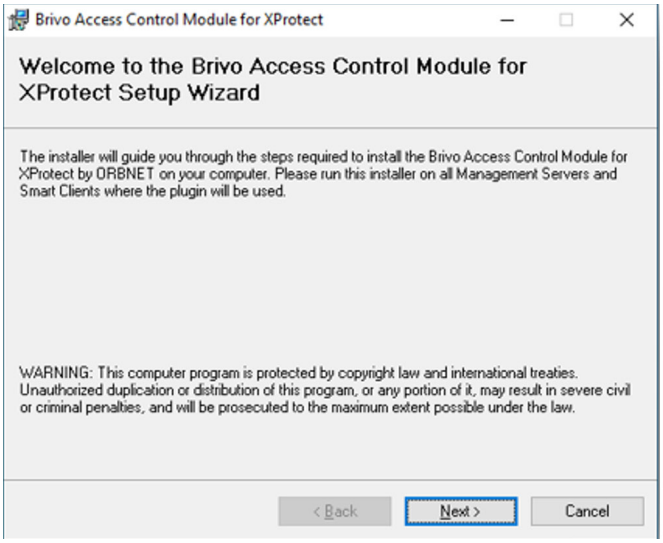
  Download links will be provided by Brivo with your API key

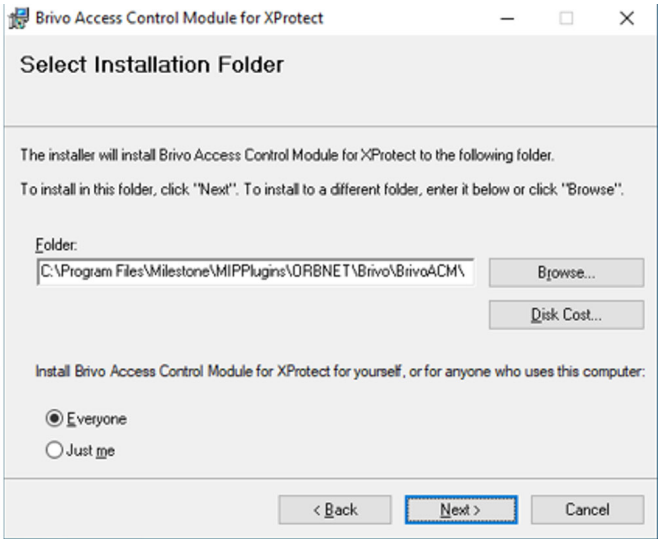
- Installer – 'Brivo Event Proxy Setup.msi'

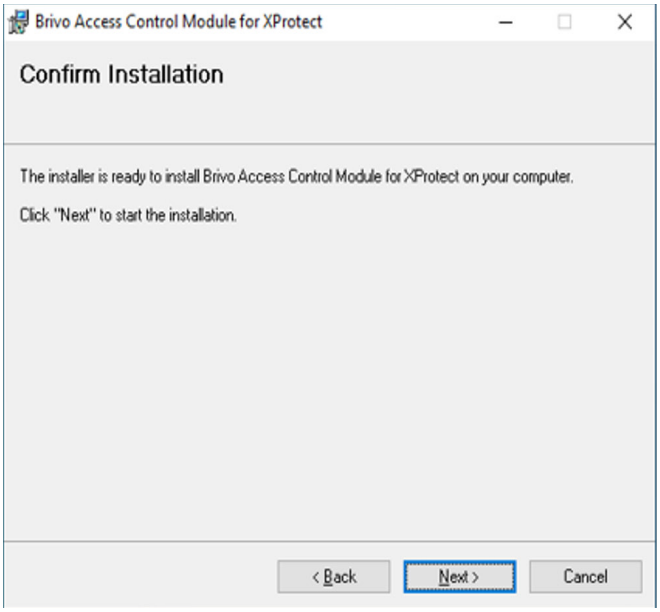
  Download links will be provided by Brivo with your API key

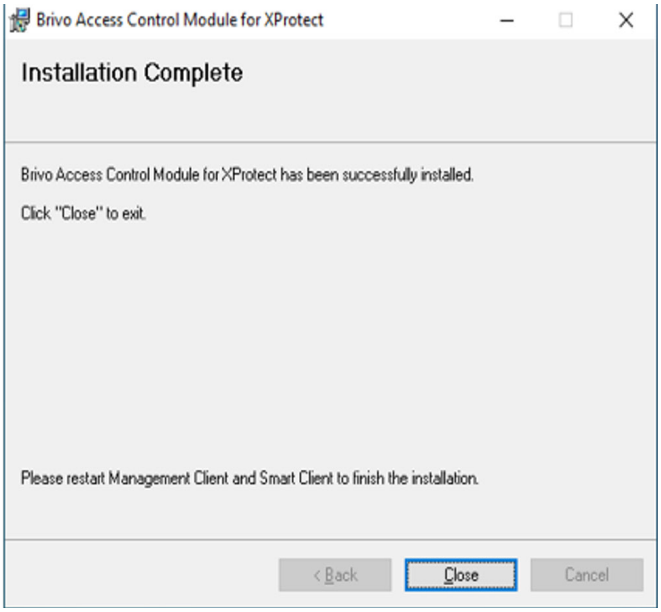
Installation of Brivo for XProtect Access

Begin with the server/machine running the XProtect Management and Event Server. Close any open Milestone Smart or Management Clients first. Place the 'Brivo Access for XProtect Setup.msi' in a folder on the desktop and double click to start the Install.

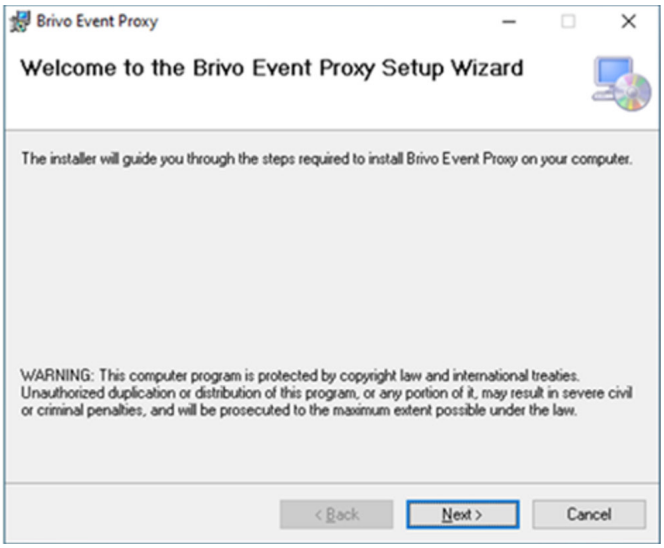


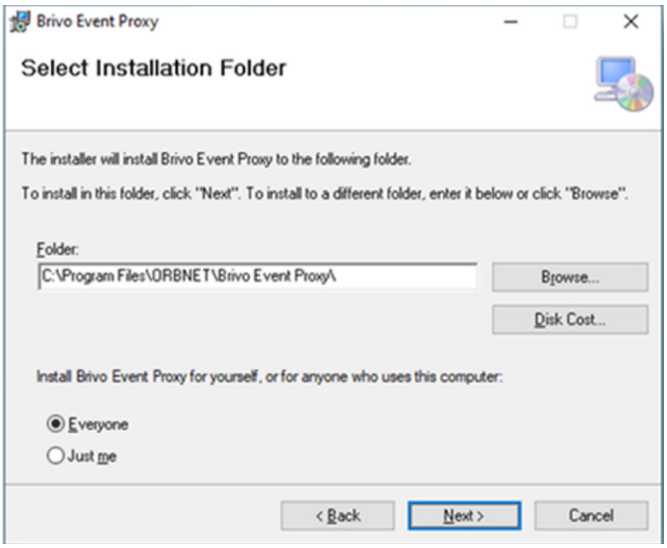


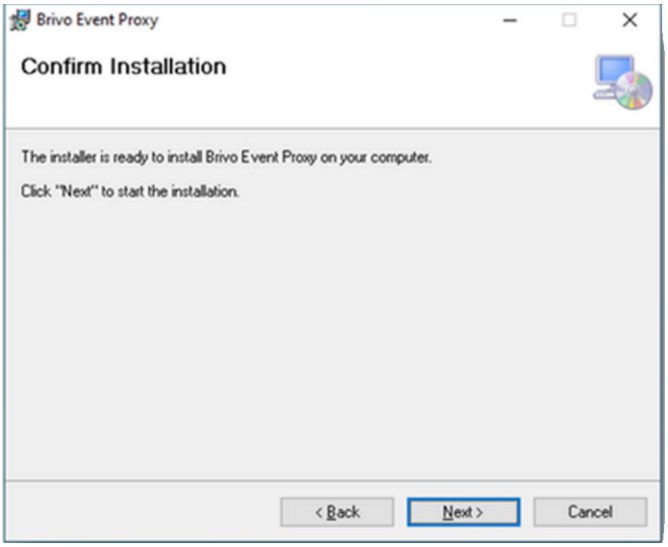


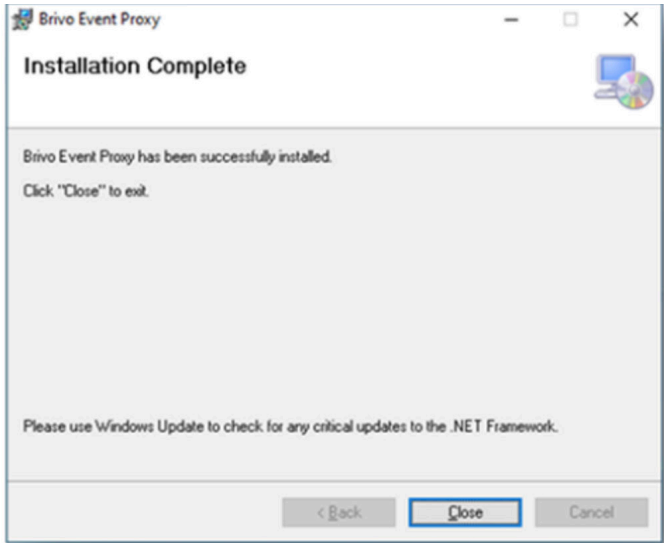


Once complete run the **'Brivo Event ProxySetup.msi'** installer to complete the event proxy connection setup. As default the installation is completed using NT AUTHORITY\Network Service. If the Milestone system does not have access to the internet, please install this on an accessible server with internet access.









Configuration

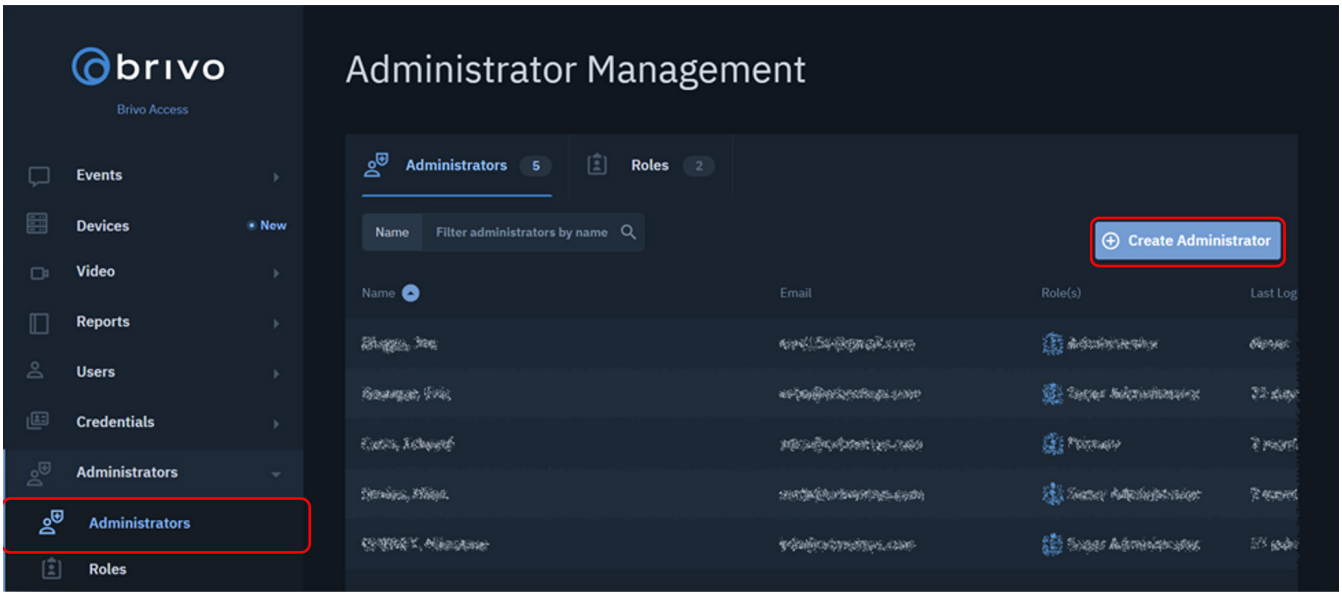
Brivo Access Control

New Administrator Setup

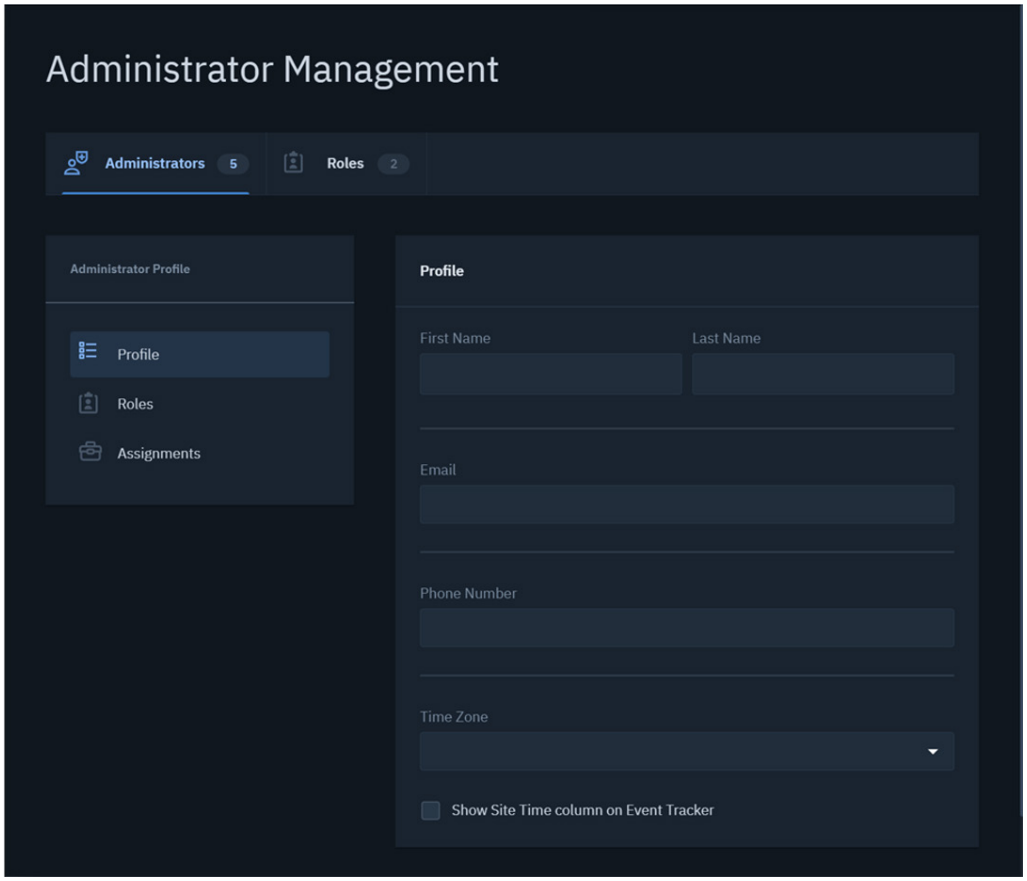
It is recommended to create a new user account within Brivo for the connection to the Milestone Access module. This will allow better management of the doors to be included and controlled.

In this example, a user was created called 'Milestone ORBNET' with access to all doors intended to be included in Milestone. The user was assigned as an **Administrator**. This is the lowest level of administrator account recommended for this integration.

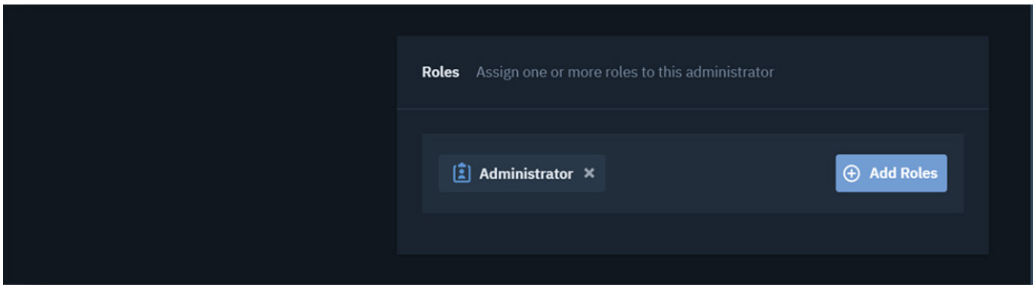
To create a new Administrator account, select **Administrators** from the main menu. From the page that lists the current Administrators user details, find the **Create Administrator** button and select it.



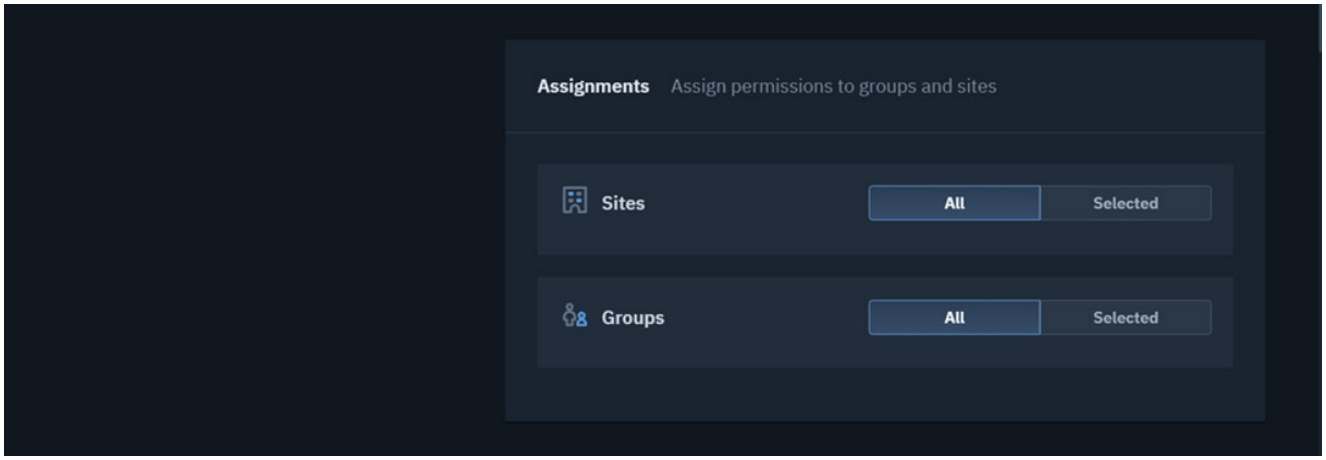
Under **Administrator Management**, add the relevant details for this new account.



For the **Roles** section, we recommend the default **Administrator** profile. A custom role will be covered in the next section, if required.



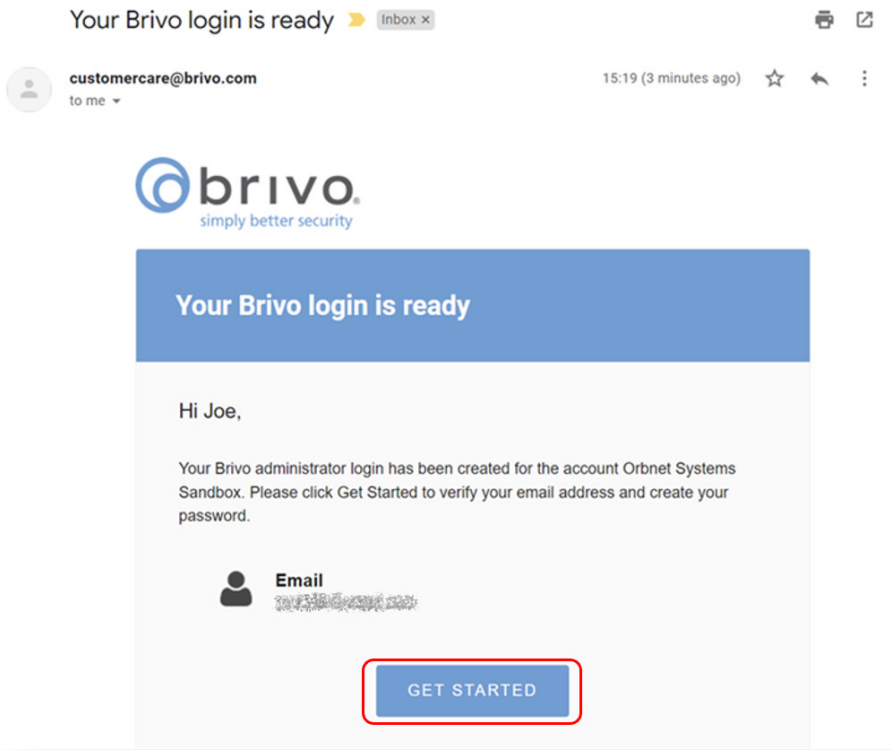
For the **Assignments** section, please select all Sites and Groups relevant to the Milestone integration.



Click **Create Administrator** at the bottom of the page to finish.

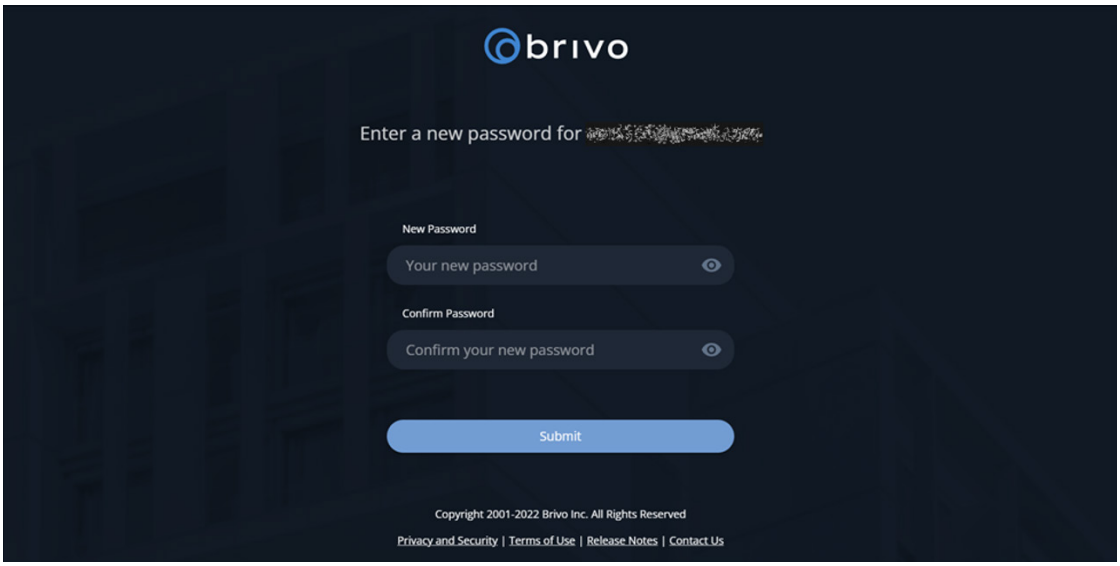
An email will be sent to the email address used to set the password for this account.

Select **GET STARTED**.



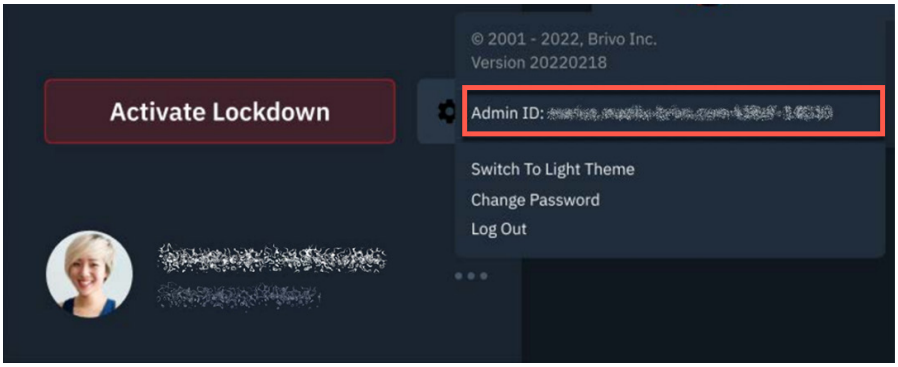
This will take you to a webpage to set the password for this user.

Take a note of the user **Password** for the next step of installation.



Once setup you will need to login with this account so to access the account **Admin ID**. At the bottom left of the Brivo Access page, press the three dots for more account options. Here the **Admin ID** will be shown.

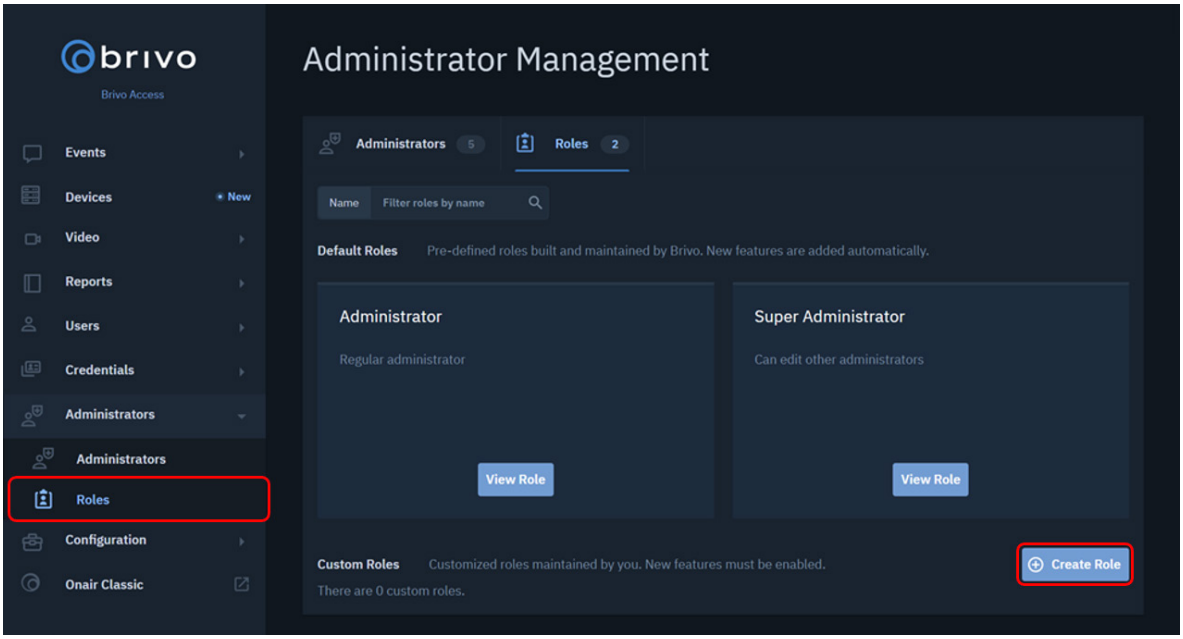
Take a note of the **Admin ID** for the next step of installation.



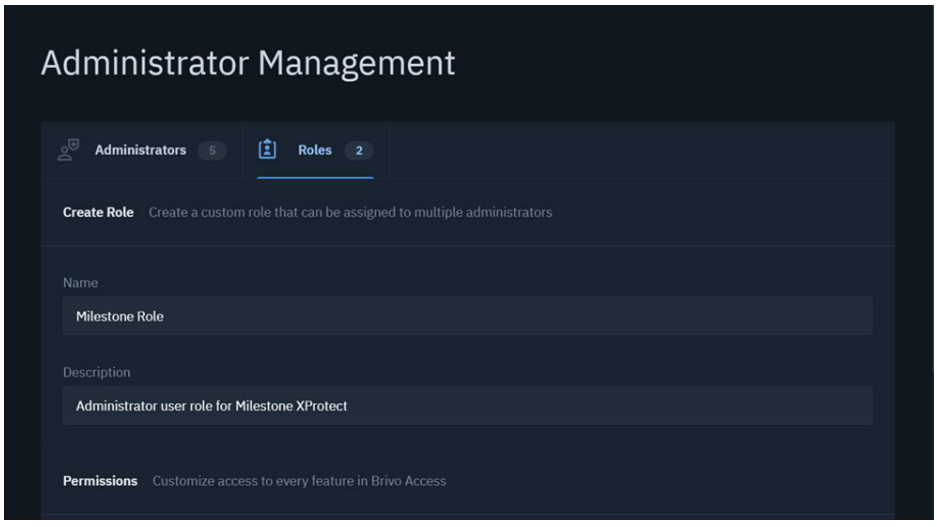
Custom Administrator Role Setup

This step is optional, for **Roles** we recommend the default Administrator profile. If you would prefer to have a custom role to limit access, please follow the below to provide the minimum level of account access.

In Brivo Access, select **Roles** under the **Administrators** tab. Next, select **Create Role** from the bottom right.



Add a **Name** and **Description** for this new **Role**.

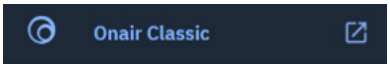


Update the **Permissions** for this role as below. **Create Role** and apply to the new Administrator account.

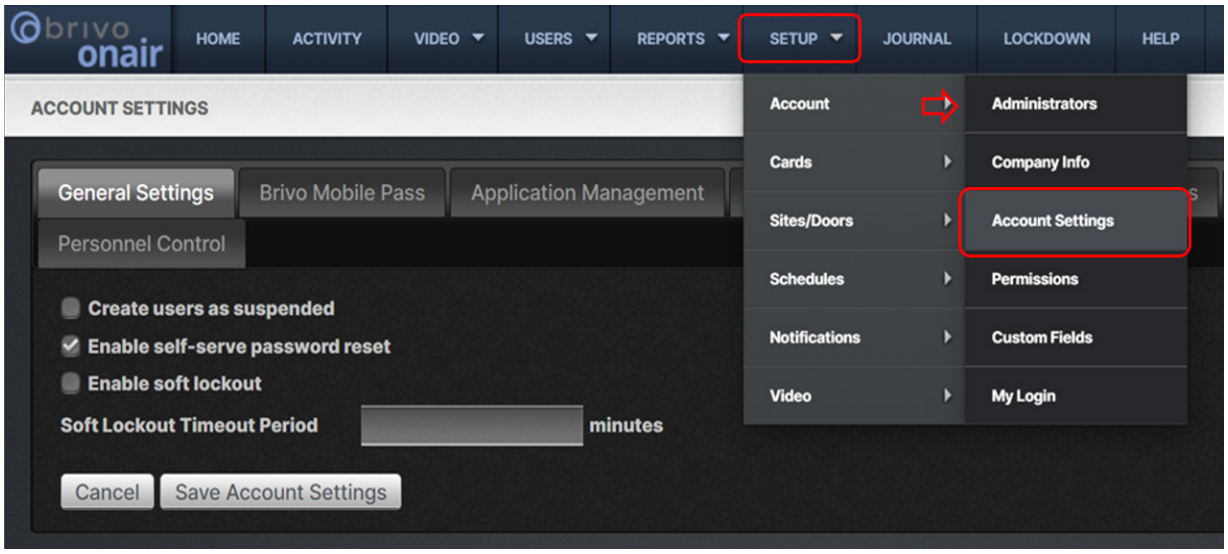
Permissions	Access
Onair Classic	Full
Event Tracker Table	Full
Journal	Full
Snapshot Log	[No Access]
Device Status	Full
Live Video	[No Access]
Classic Reports	Full
Users	Full
Groups	Full
Badging	[No Access]
Card Bank	Full
Notifications	Full
Configuration	[No Access]
Roles	[No Access]
Lockdown	Full
Manage Account Settings	[No Access]

API Application Setup

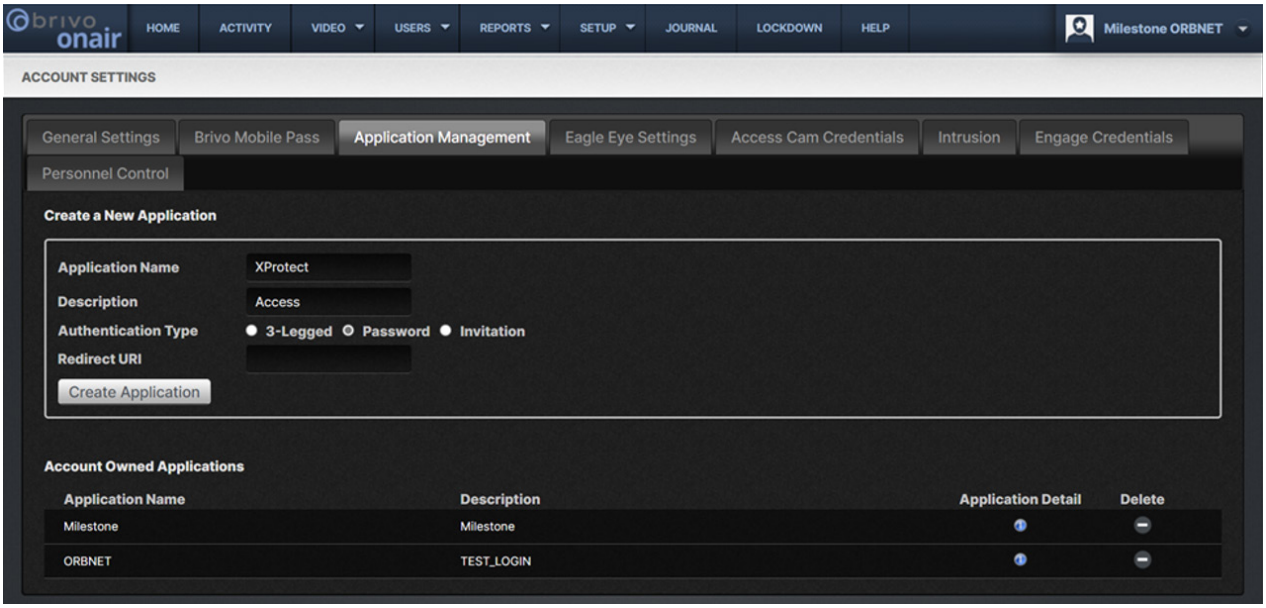
Currently some settings for this module are only available from Brivo Onair. For Brivo Access users select Onair Classic to access this section from the menu.



Within Onair as a Primary or Senior Administrator go to **Setup > Account > Account Settings** then select **Application Management**.

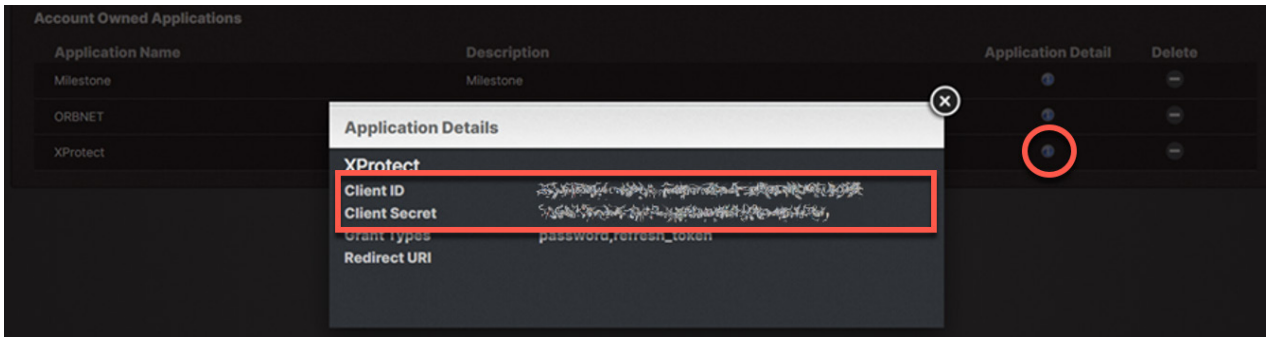


From **Application Management**, use the **Create a New Application** section , Add an **Application Name** and **Description** and select **Password** for the **Authentication Type**. Next press the **Create Application** button.



The new application will be added to the list, then select the **Application Details** icon.

Take a note of the **Client ID** and the **Client Secret** for the next step of installation.



API Key

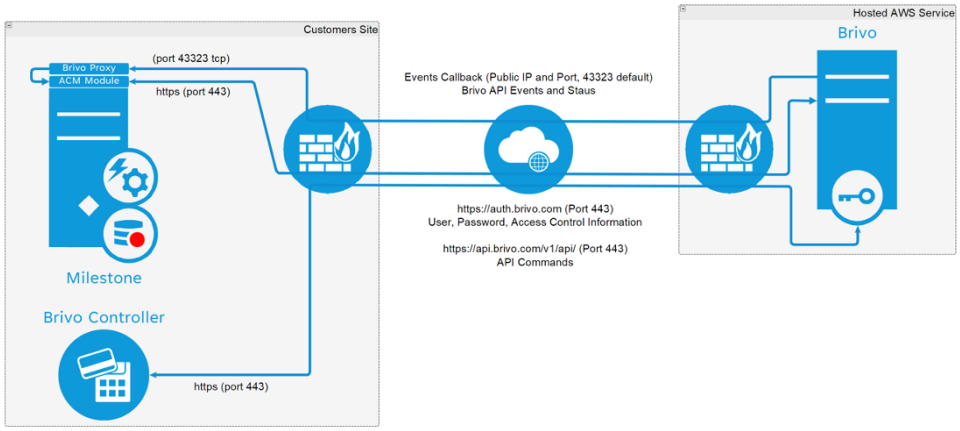
Please complete an **API Account Access Agreement Form** from your Brivo dealer to gain access to this API key.

Event Callback External Access

Network Schematic

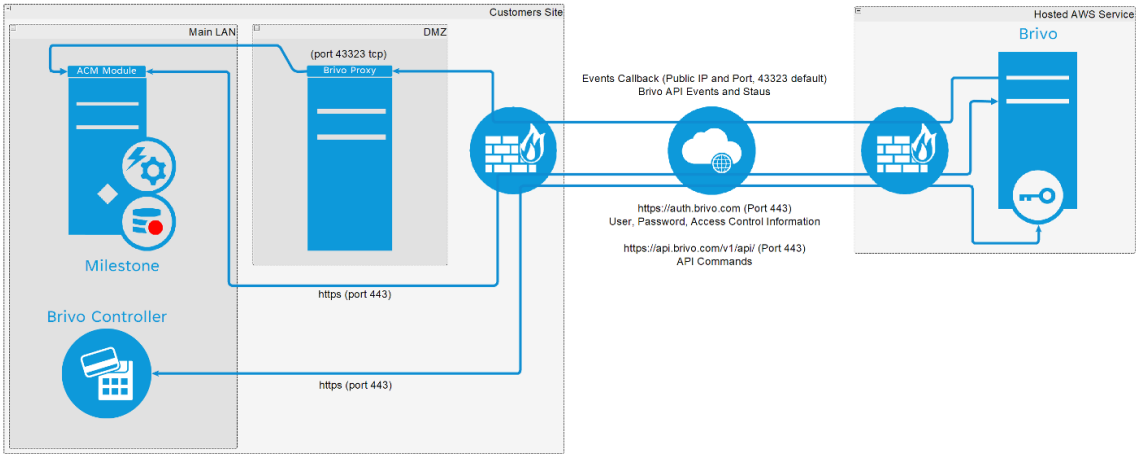
In a standard installation, both the **Brivo Event Proxy** (Used for Brivo Event Callback) and **Milestone Management** would reside on the same server. This would be for a system where the Milestone server is internet facing.

Brivo Access Control Module for XProtect



For an installation where the Milestone server has no access to the internet, a secondary machine would be used to bridge the connection to the internet. Generally, this would be in the demilitarized zone (DMZ) but would depend on the site network installation. This would be where the **Brivo Event Proxy** would be installed.

Brivo Access Control Module for XProtect
Network DMZ Model



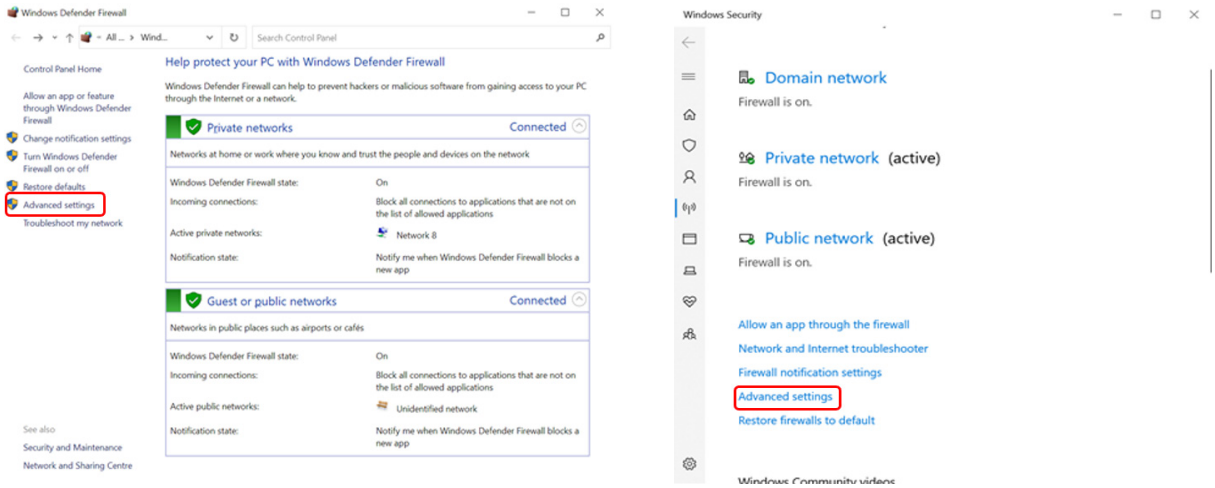
Windows Security

Please seek permission from the organization before implementing any security changes. The IT Security team may wish to complete this or a similar task on a centrally managed system.

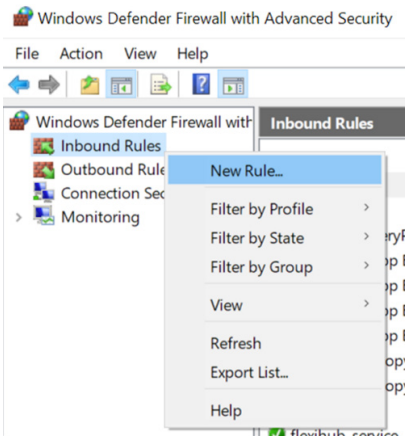
This example uses the default Windows Defender software firewall interface. The features of software firewalls differ so the setup will likely be different for the software firewall used in your installation. Please refer to the user guide of your firewall for further information.

This integration requires an external internet-based service to communicate with the Milestone server on a Transmission Control Protocol (TCP) port. This will communicate directly to the Brivo Event Proxy installed on the server or bridged to a server in a Demilitarized Zone (DMZ). Both methods will require an inbound TCP port to be set up to allow access on one or both servers.

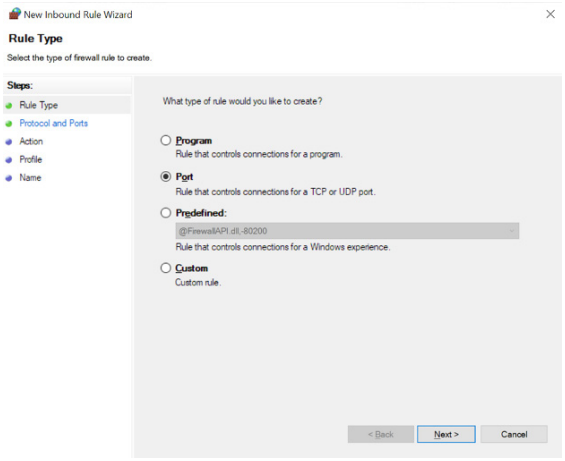
Navigate to **Windows Defender Firewall** or **Windows Security** then select **Advanced Settings**.



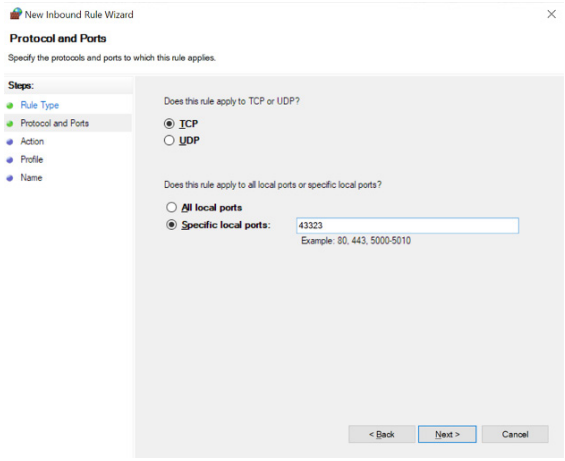
Select **Inbound Rules** then right click to select **New Rule**.



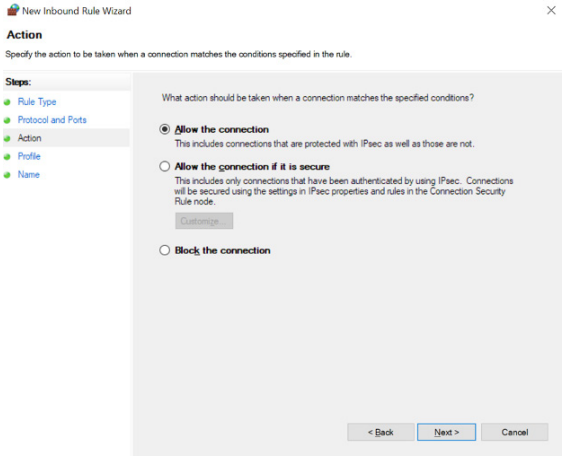
Rule Type = **Port**



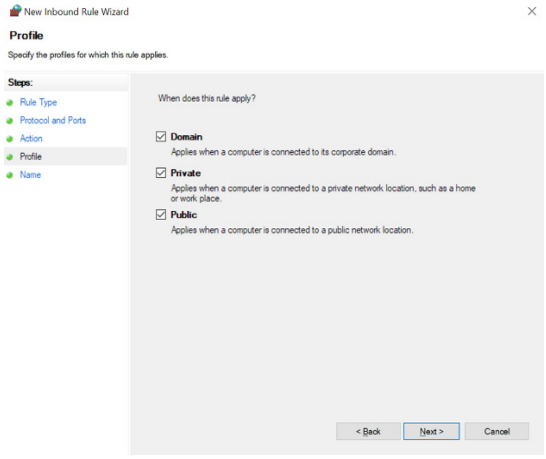
Protocol and Ports = **TCP, 43323**



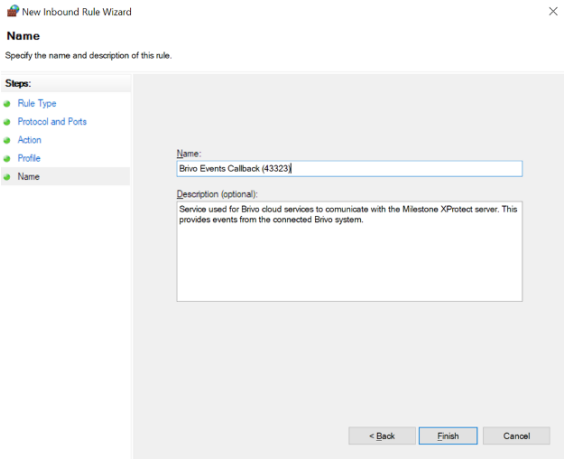
Action = **Allow the connection**



Profile = **Select all that apply**



Name = **Brivo Events Callback (43323)**



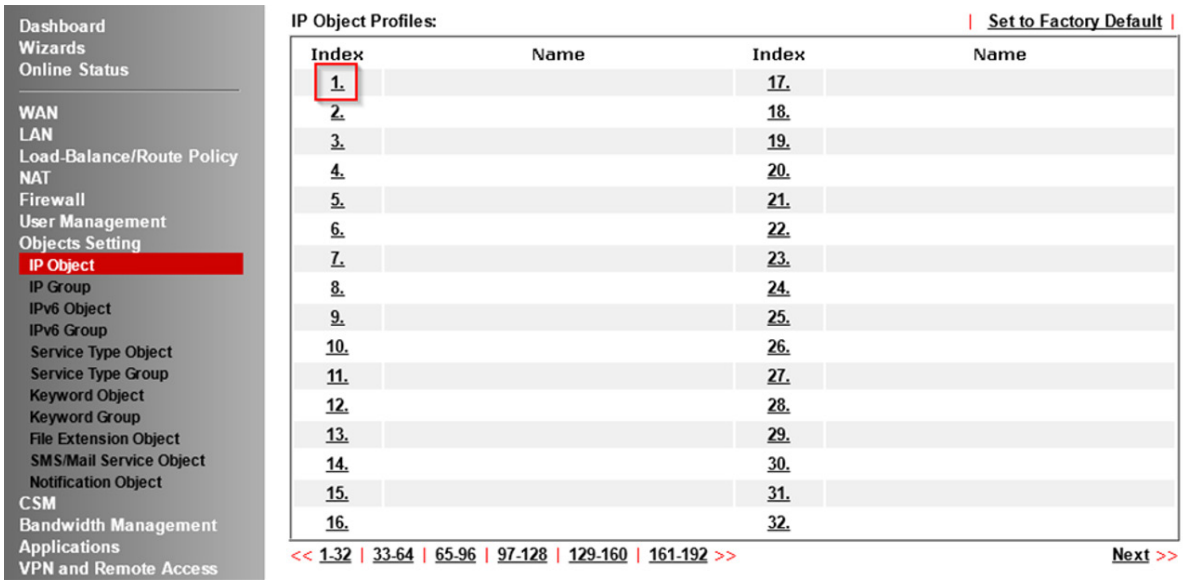
Network Firewall Setup

Please seek permission from the organization before implementing any security changes. The IT Security team may wish to complete this or a similar task on a centrally managed system.

This example uses a standard basic router/firewall interface from a well-known manufacturer. The features of firewalls differ so the setup will likely be different for the firewall used in your installation. Please refer to the user guide of your firewall for further information.

Add an inbound IP restriction (Optional but recommended).

Go to **Object Settings > IP Object** and click on the first available index number:



Set a name for this service and leave the Interface default unless your setup requires this to be changed.

In the IP Object, there are three Address Type settings:

Single Address, **Range Address** and **Subnet Address**.

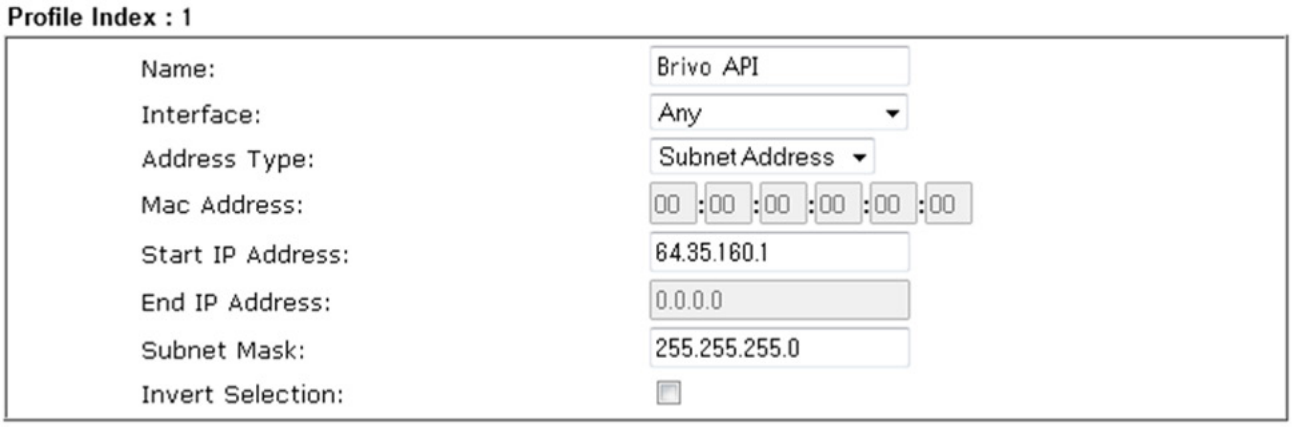
For this example, **Subnet Address** would be selected. The Brivo services span several IP address ranges and subnets, depending on where this site installation is in the world and the server running the service at the time will depend on what IP communicates with your Milestone XProtect system.

This service will fall into 64.35.160.0/24 registered to Brivo Systems, LLC (Listed in ARIN).

REF: https://rdap.arin.net/registry/entity/BRIVO-1

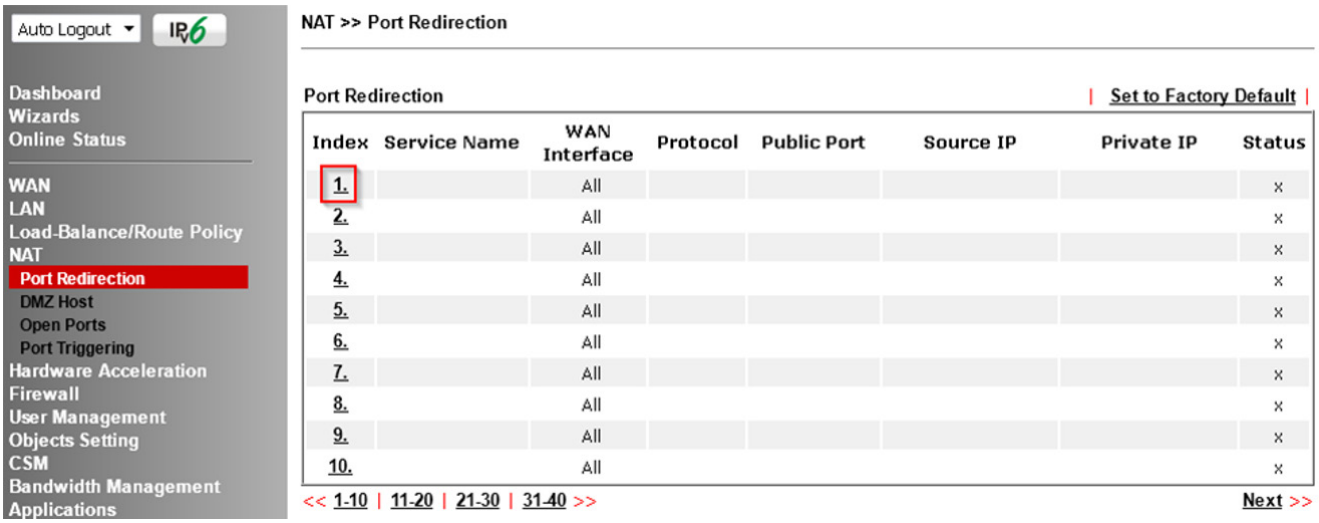
REF: https://who.is/whois-ip/ip-address/64.35.160.0

As this is a /24 subnet there are 256 usable IP addresses. The first usable IP address is 64.35.160.1 with the subnet added as 255.255.255.0.



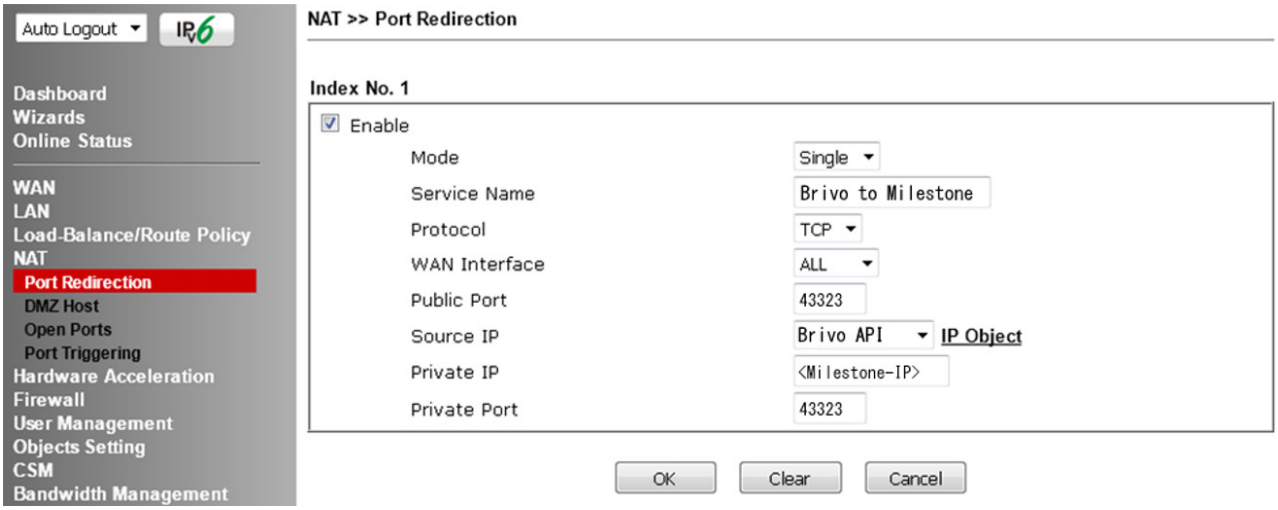
Add a **Port Redirection / Port Forwarding (Required)**.

To configure a Port Redirection NAT rule on the router, go to **NAT > Port Redirection** and click on the first available Index number:



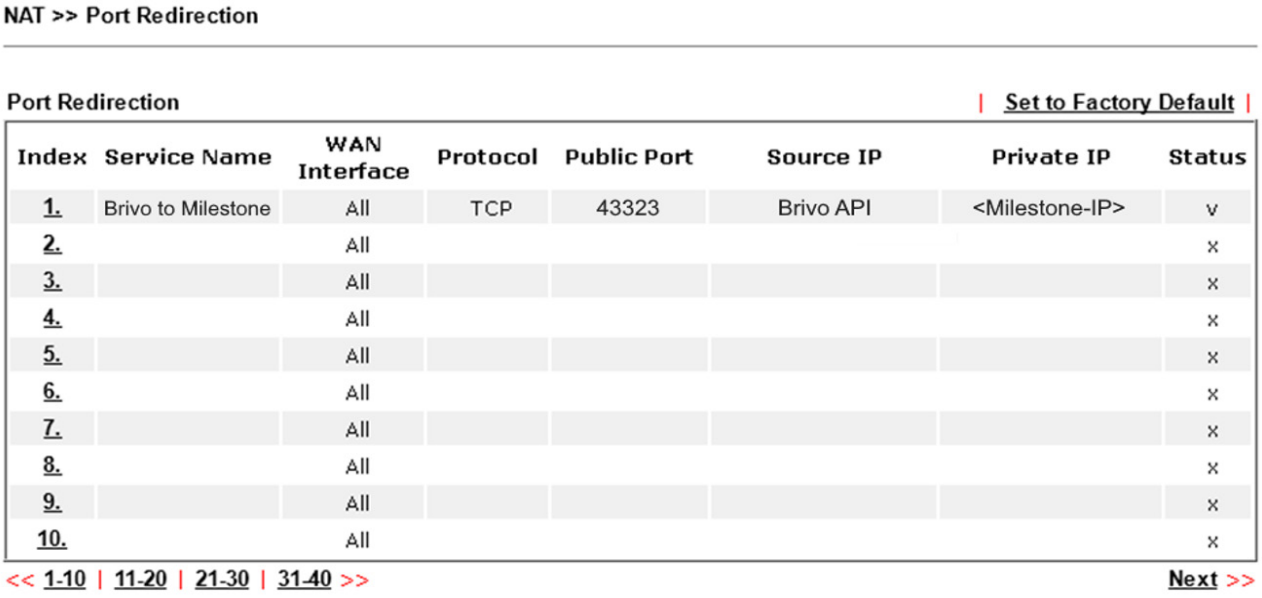
In the **Port Redirection** entry, configure these settings:

- **Mode**: Set this to Single to open a single port
- **Service Name**: This is used for display purposes to identify the NAT rule
- **Protocol**: Select TCP
- **WAN Interface**: The Internet connection that the port will be opened to
- **Public Port**: This is the external port. In this example, the port forwarded is the same externally as internally
- **Source IP**: If setup select the IP Object created for the Brivo API, otherwise select Any
- **Private IP**: This is the LAN IP of the server that will respond (E.g. Milestone or DMZ Server)
- **Private Port**: This is the port number for the service that the router will send to the LAN IP



Click **OK** to save the rule, this will show in the rule list as enabled. The router/firewall will now forward requests received on that port to the internal server if the IP address matches the Source IP.

If configured, the Source IP will display with the created Brivo service, otherwise this will show as **Any**.



Use a test service like https://www.whatismyip.com/port-scanner/ to confirm the port is accessible. The Source IP will need to be set to **Any** to use this tool, so be sure to change back once completed.

Take a note of the **Public IP** and **External Port** used for the next step of installation.

Milestone Management

Check List

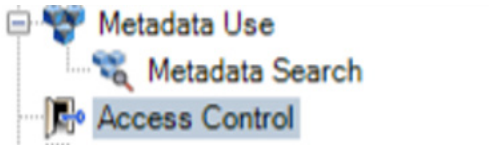
Before you get underway with the Milestone Management setup, please go through this list, and check off each item to ensure everything is ready to get the integration module working right away. Links to the relevant sections have been provided.

Step	✓	Link
Make a note of the number of doors to be used with Milestone		n/a
List the doors with the associated camera(s) in Milestone		n/a
Milestone Access License purchased or demo		Milestone Access
Milestone Access License applied to your Milestone server		Milestone Access
Brivo Access Control Module for XProtect purchased		Brivo Access
New Brivo Senior Administrator account created		Brivo Administrator Setup
Brivo Admin ID and Password noted for new account		Brivo Administrator Setup
Brivo API Application created		API Application
Brivo API Client ID and Client Secret noted		API Application
Brivo API key created or requested		API Key
Brivo API key noted		API Key
Windows Firewall rule setup for Brivo Event Proxy		Windows Security
Network Firewall rule setup for Brivo Event Proxy		Network Security
Make a note of the public IP and port used to access		Network Security
Installation of Brivo Event Proxy and Module for XProtect		Module Installation

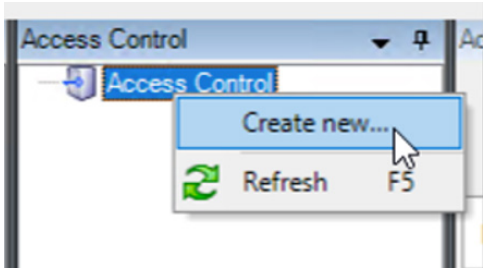
Access Control Setup

This integration allows for XProtect Access to connect your access control system directly to Milestone's XProtect VMS. It is designed to fit perfectly with any XProtect product. No matter your installation size, with XProtect access you can control your video cameras and access your control system from a central interface.

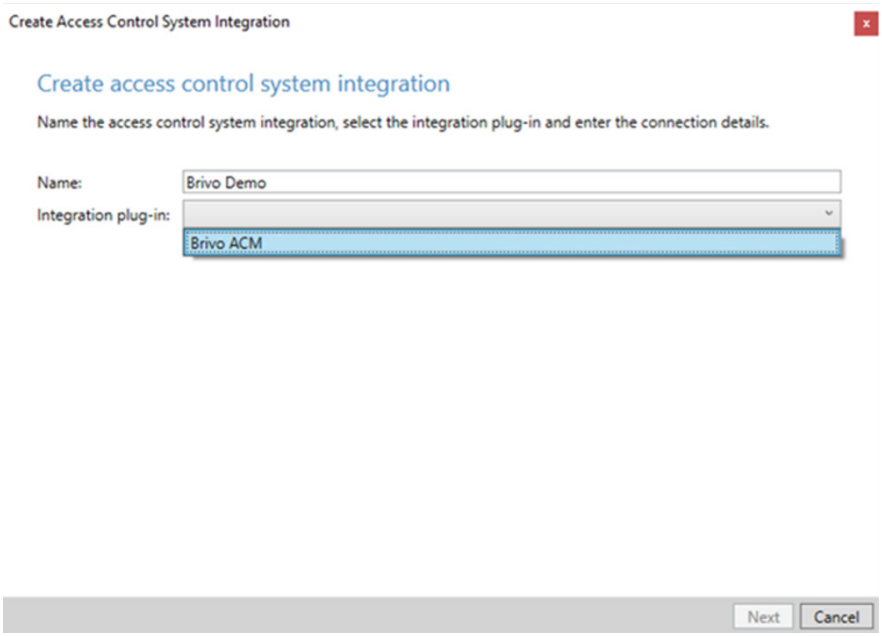
Select the **Access Control** entry in the Milestone Management Client tree



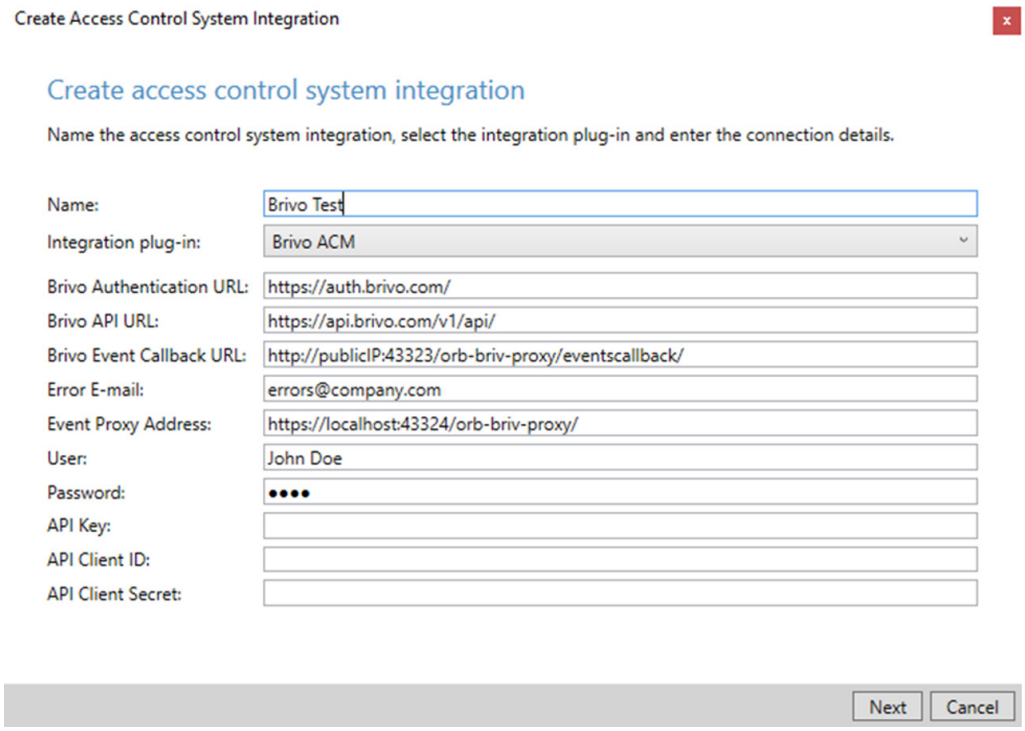
Right-Click **Access Control** and select **Create new....**



Define a **Name** for your Access Control System. Select the Brivo ACM V2 from the drop-down.

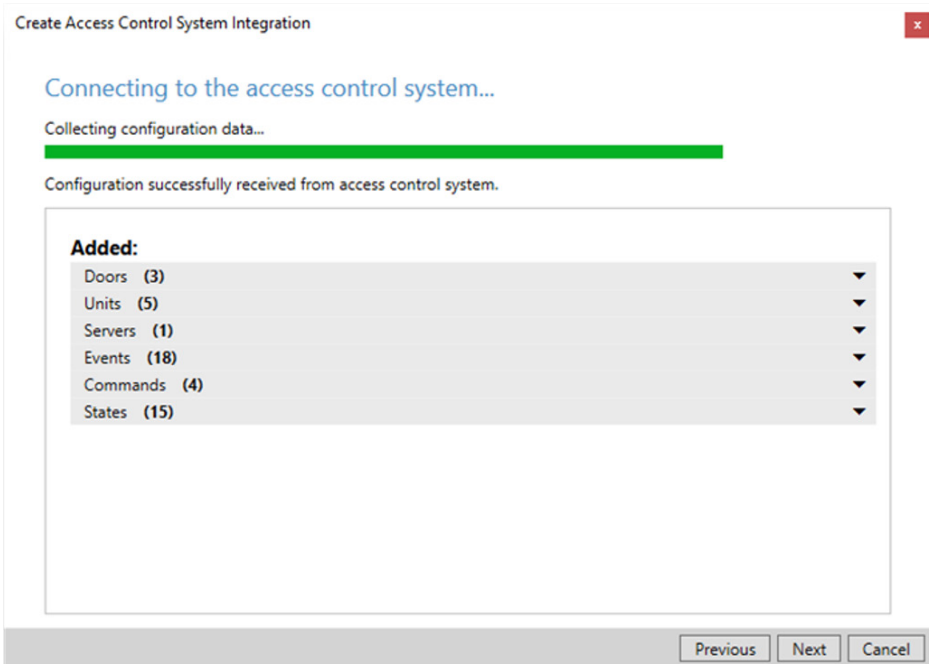


This will present the default configuration page for this access integration module.

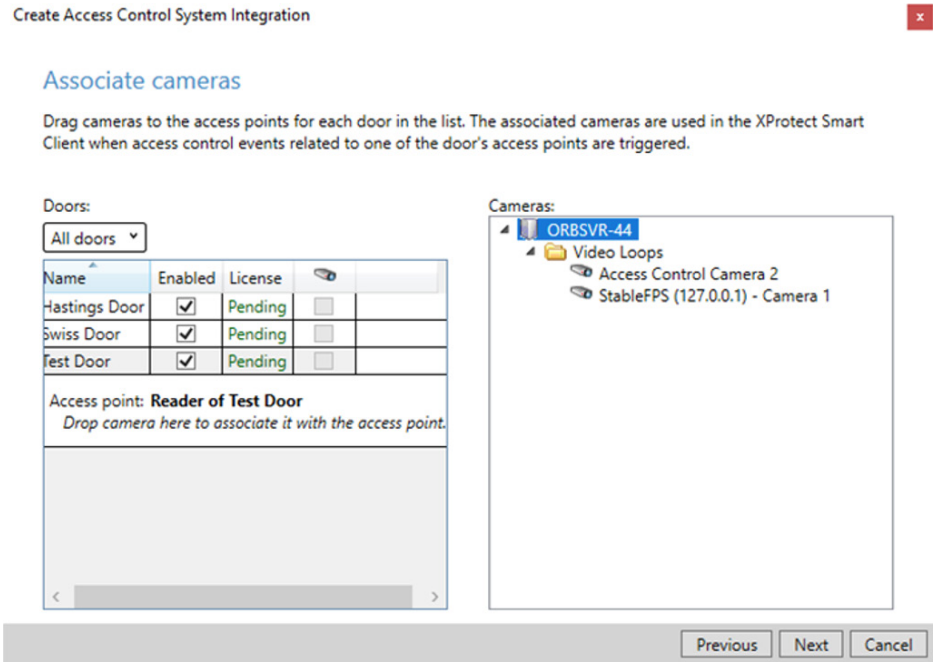


Brivo Authentication URL:	https://auth.brivo.com/ no requirement to change
Brivo API URL:	https://api.brivo.com/v1/api/ no requirement to change
Brivo Event Callback URL:	Update with the external/public IP and port used for this service
Error E-mail:	Emails sent from the Brivo cloud service related to errors
Event Proxy Address:	Local IP address, port used for the Event Proxy (Event Callback)
User:	Brivo Access user account ID (not the email address)
Password:	Brivo Access user password (Used with email address login)
API Key:	From Brivo developer account or requested (24 characters)
API Client ID:	From API application created in Onair Account
API Client Secret:	From API application created in Onair Account

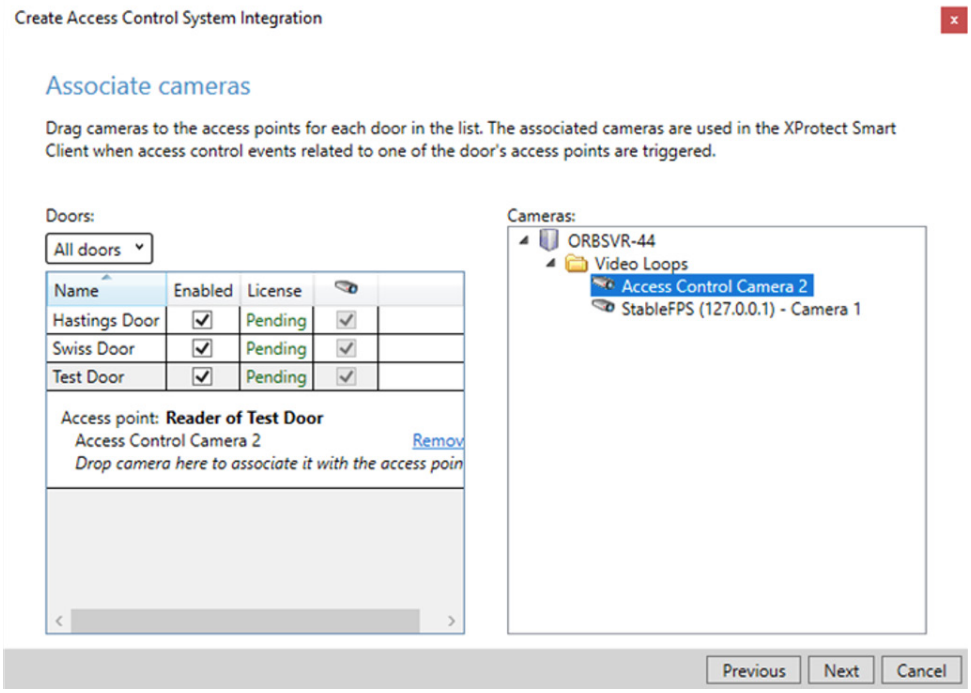
Connection to the system will now be completed and the permitted configuration will be received.



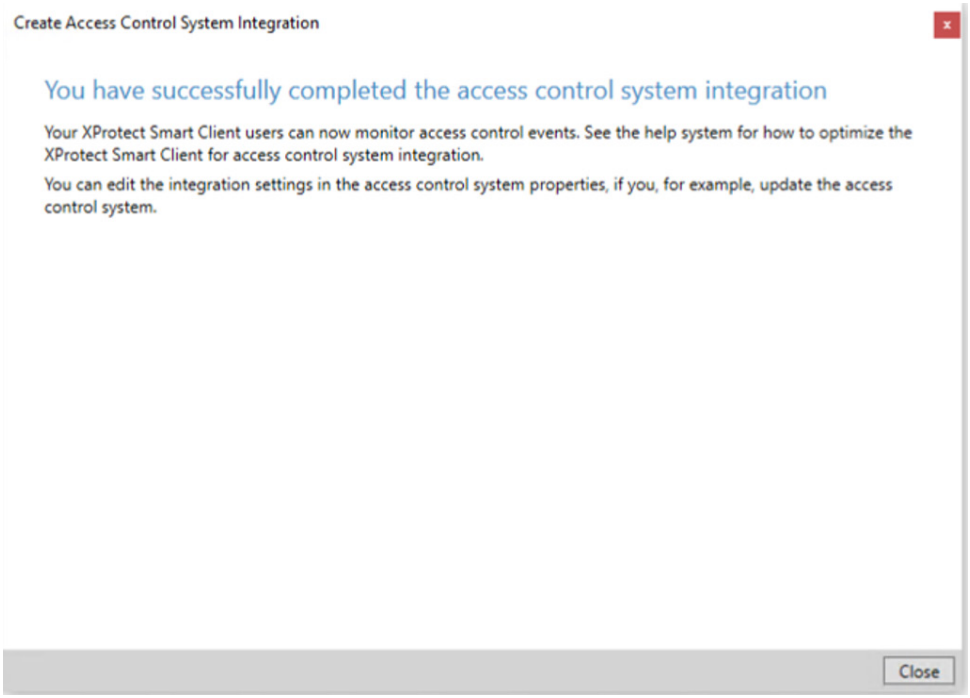
Expand the available Milestone cameras and drag and drop the associated camera to the access doors.



Once added, click **Next**.



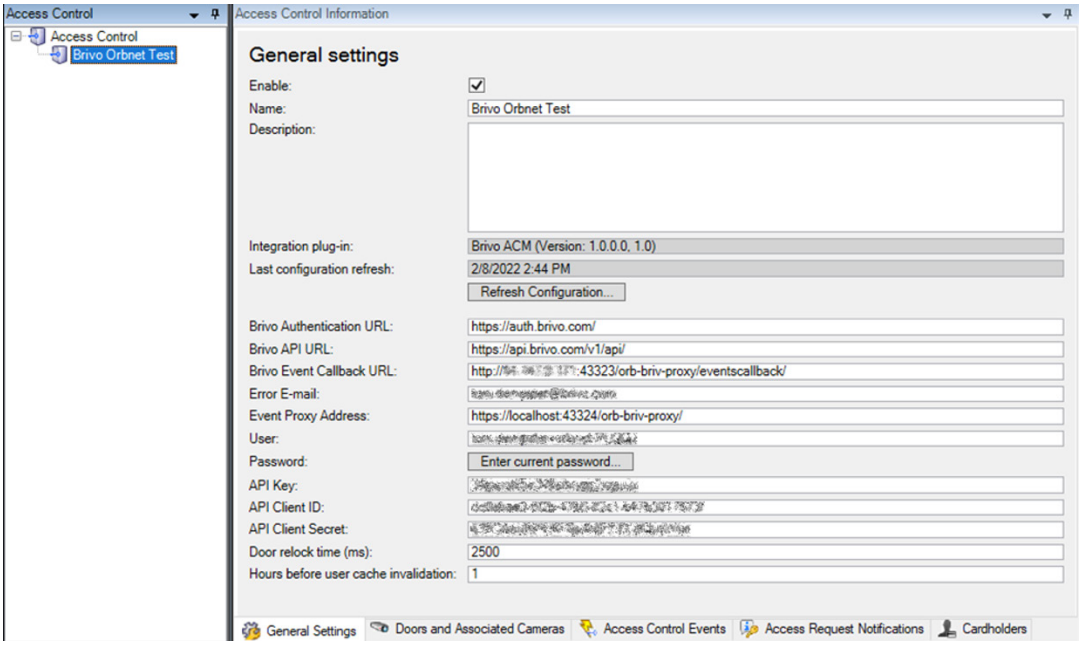
The initial configuration is now complete. Additional setting can be changed via the **Milestone Management Client**.



Access Control Information/Other Settings

This integration provides the below configuration tabs.

General Settings



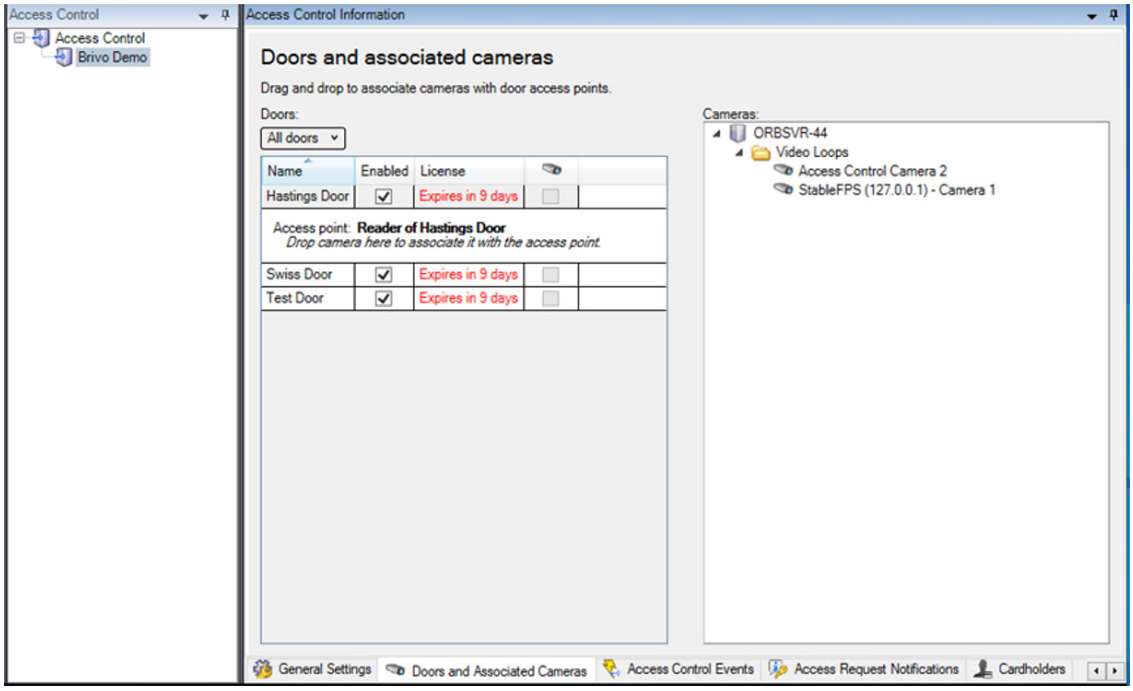
Refresh Configuration: When a new door is added or removed from the Brivo Access system, use refresh configuration to update the doors within Milestone.

Enter current password: If the account password is changed, use this button to update. Also use to input the password before refreshing the configuration if troubleshooting a connection issue.

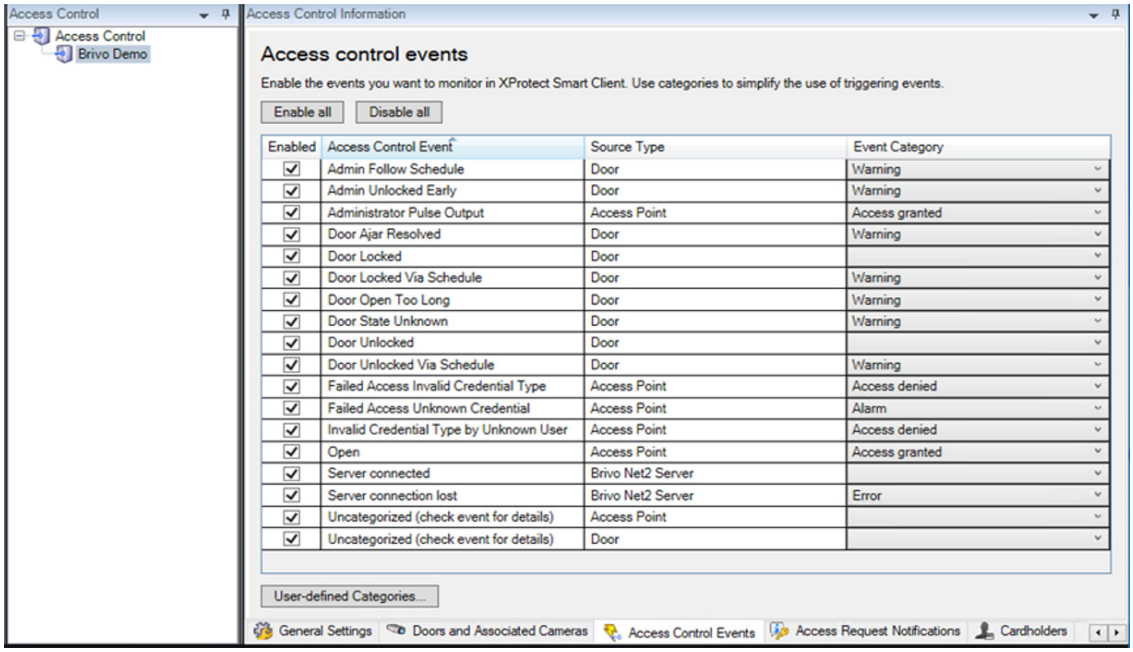
Door relock time (ms): When open door commands are sent from Milestone, this is the time used before relocking the door. **Default (2500ms)**.

Hours before user cache invalidation: This is the time frame used for updating user information in Milestone (E.g. names, pictures). If a user information change is made in Brivo, this could take up to the time specified to show in the Milestone events. Default (1h), Minimum 1h, Maximum 24h.

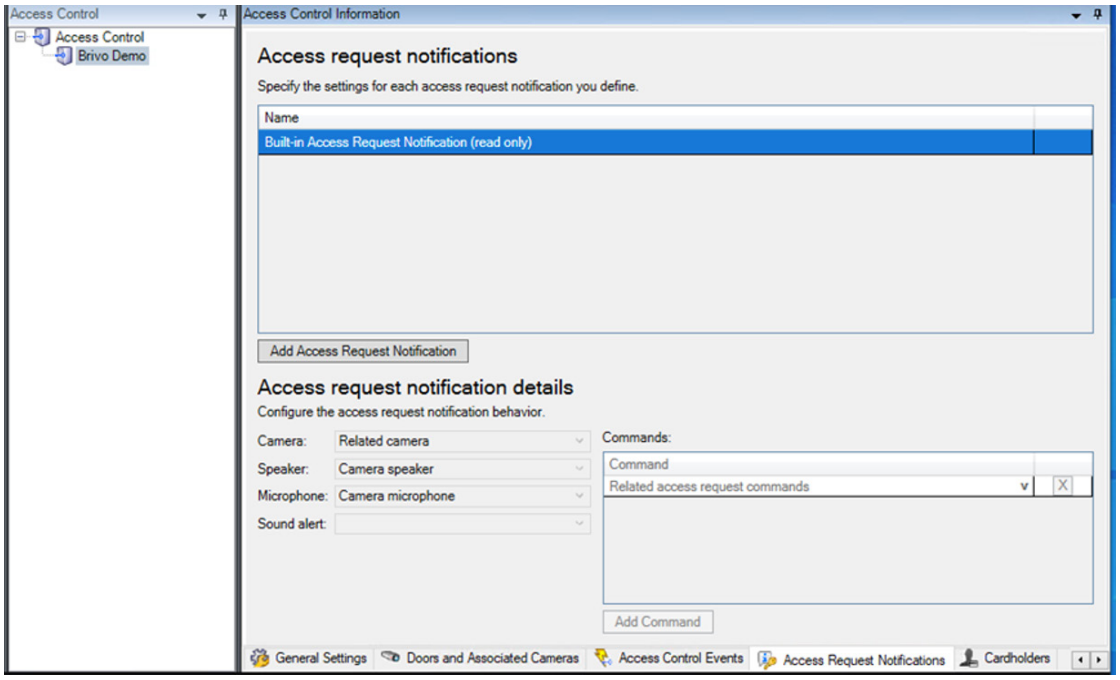
Doors and Associated Cameras



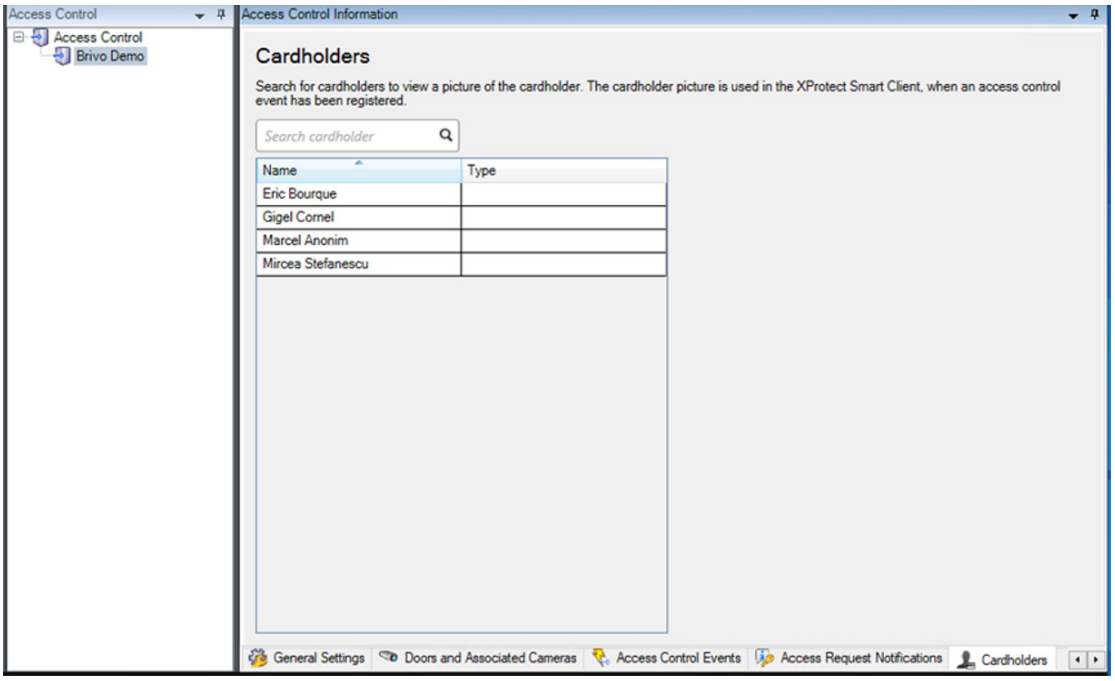
Access Control Events



Access Request Notifications (Not currently supported in Brivo Access)



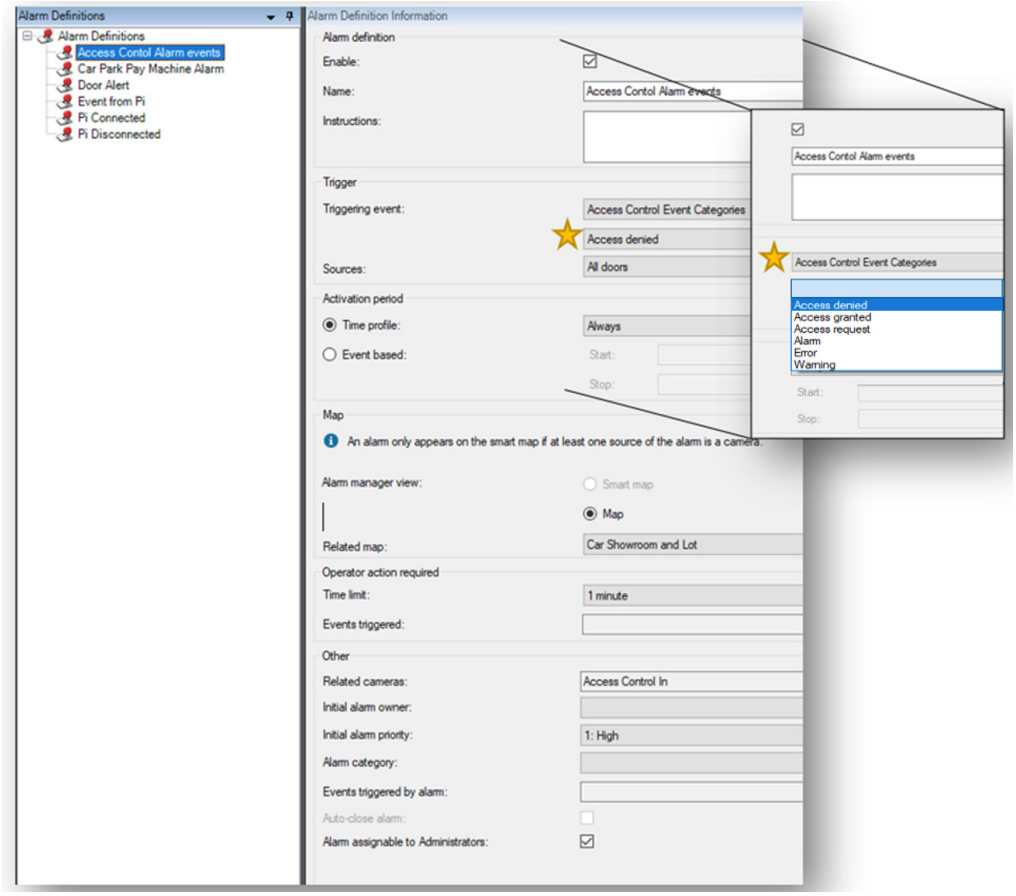
Cardholders



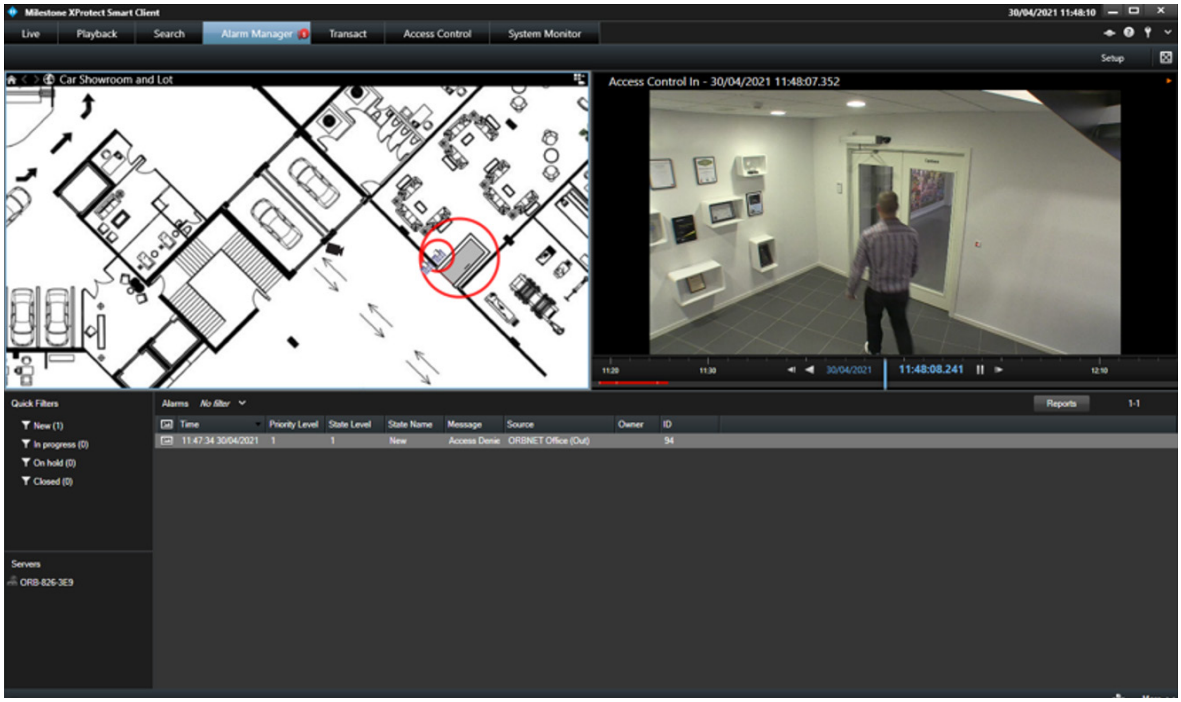
Alarm Definitions

In the Milestone Management, alarms can be created from Access Control Events.

The below alarm shows an easy method to create an access denied event on all doors in the system, and then have that event auto display an alarm in the Milestone Smart Client showing a specified map view.



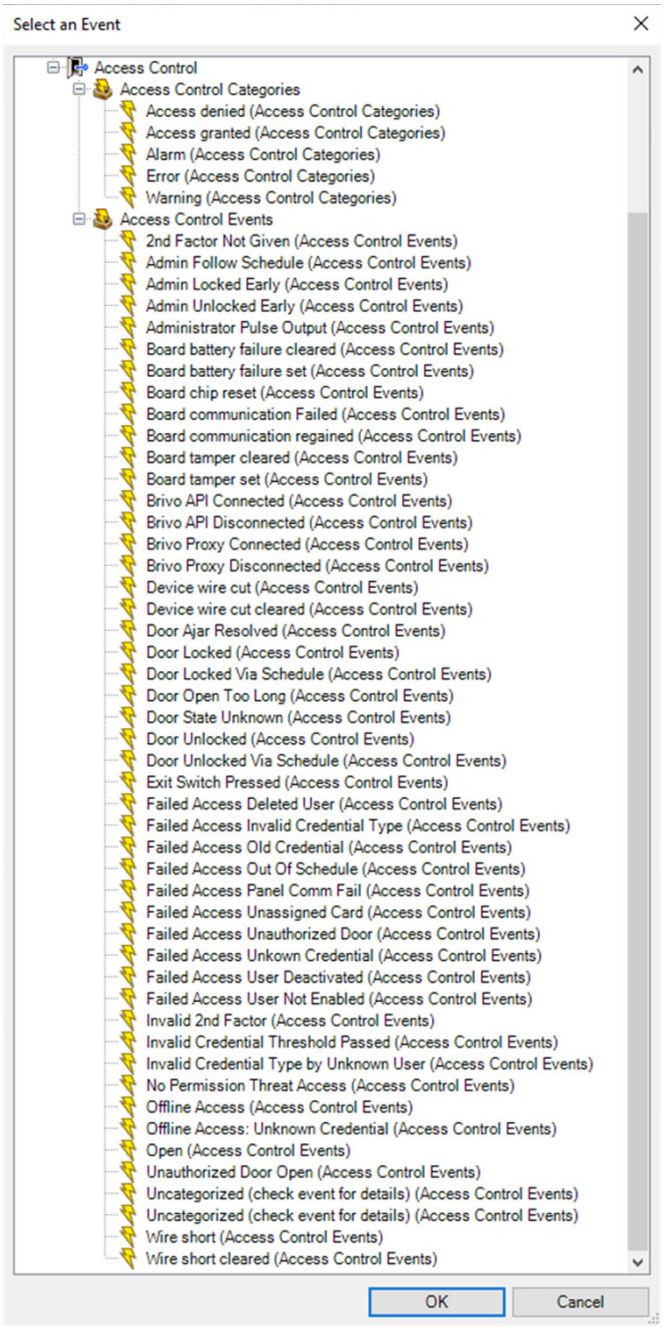
Below shows the **Alarm** being triggered within the Smart Client. This will display a red flashing ring around the door that has triggered the event.



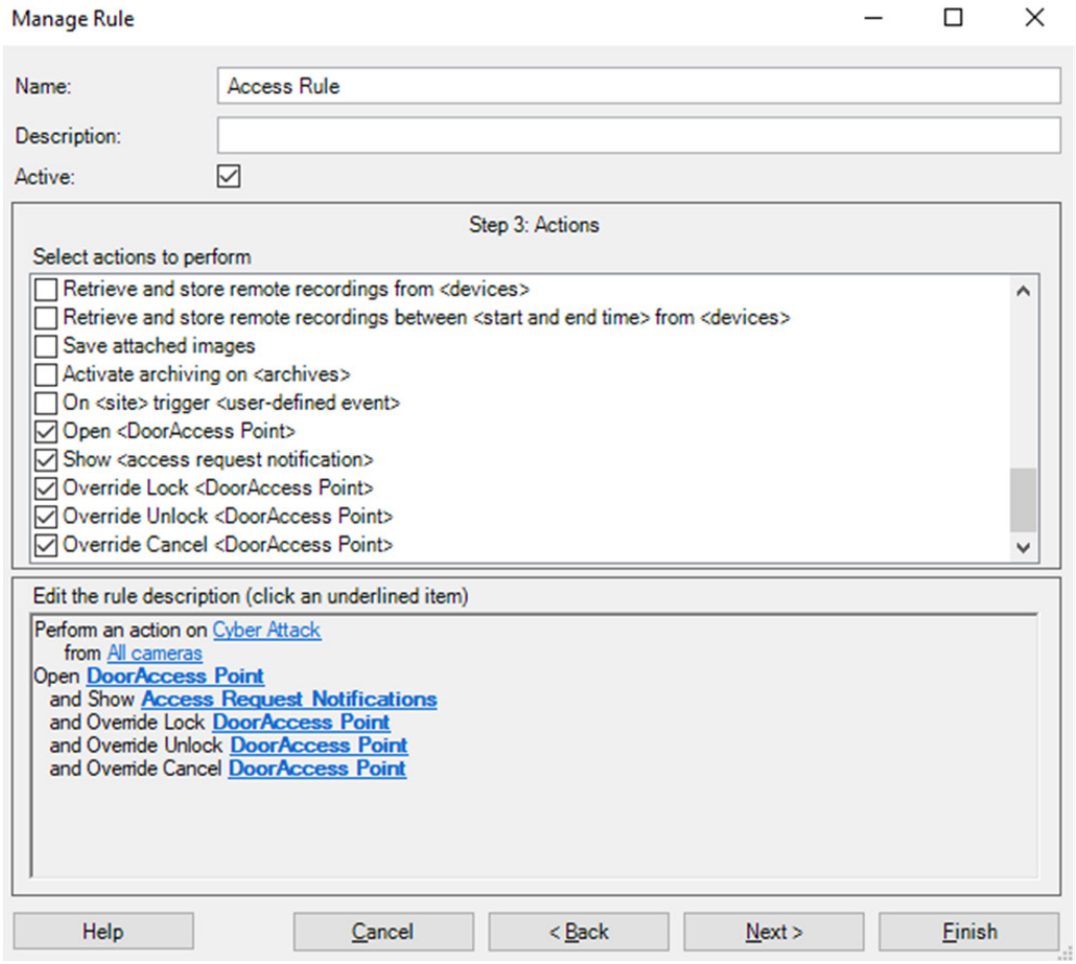
Rules and Events

To access the Access Control events in Milestone, select the **Rules and Events > Rules** section in the Management Client and then right click in the center column to add a new rule.

- Perform an action on **Event**



With Milestone **Rules and Events**, it is possible to enable an event from the Access Control System to trigger an additional event or action in XProtect. The rule below is a simple example of how to record a specific camera when an **Access Denied** event is received.

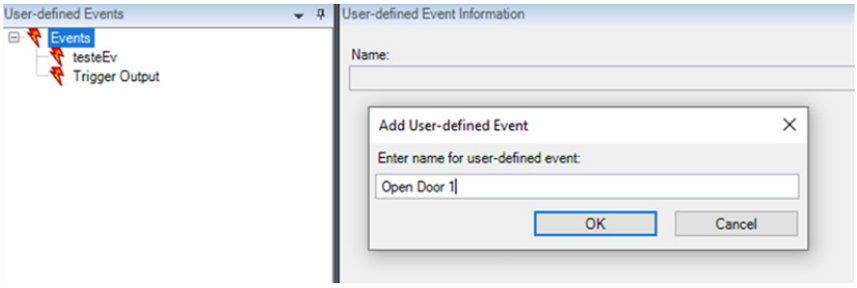


User-defined Events

Often overlooked, the **User-defined Event** allows easy access to the control of an out-bound action from Milestone and the Smart Client. The initial setup of the User-defined event is as a placeholder for a Rule.

Under **Rules and Events** select **User-defined Events**, right click and **Add User-defined Event**.

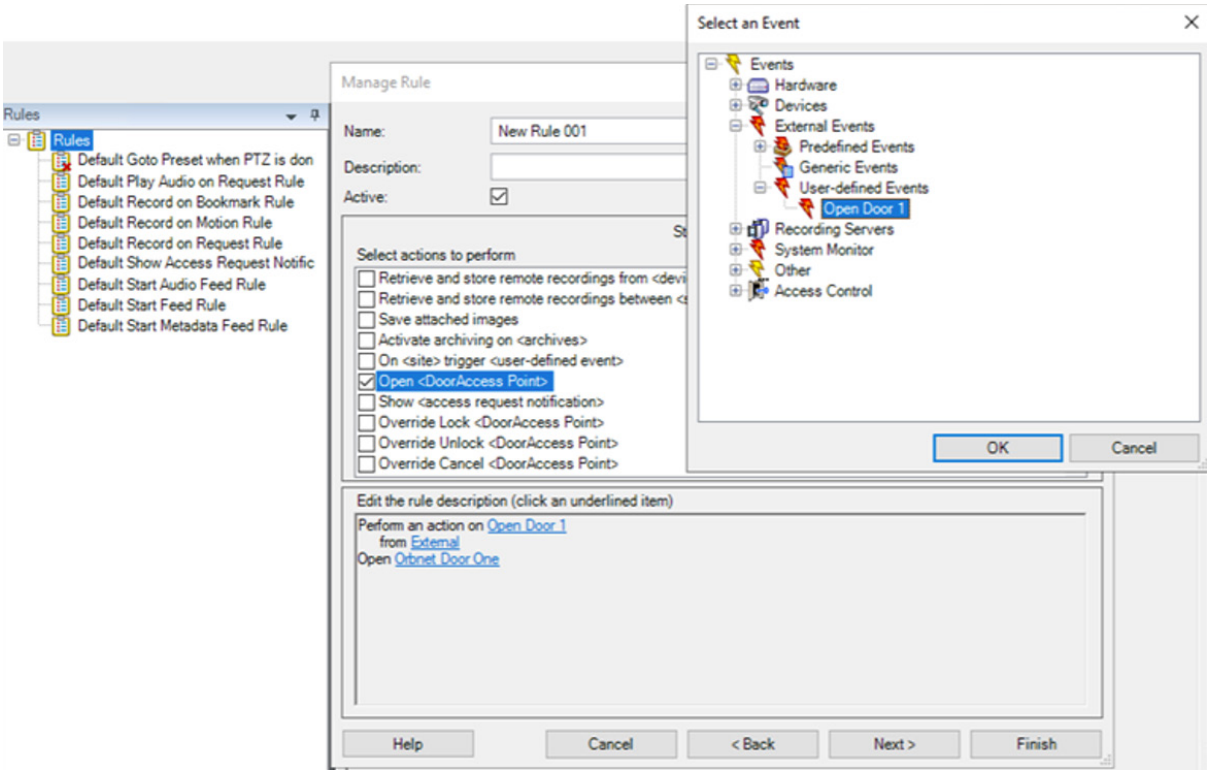
This provides just a name field. Fill this with a name relevant to the action you intend to add. Remember that this is the name of the event shown in the Smart Client.



Back in **Rules**, create a new rule and select the **User-defined Event** that was created.

Perform an action on **Event**

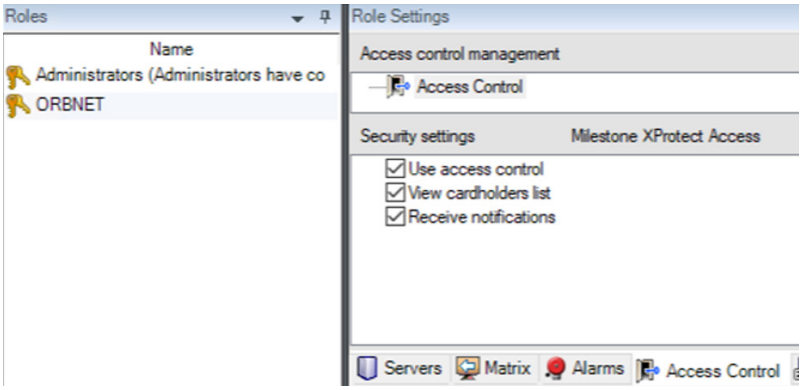
- **Events > External Events > User-defined Events**
- Click **Next** and select the relevant action to be performed on the Brivo panel by selecting the checkbox(es).



User access for Smart Client

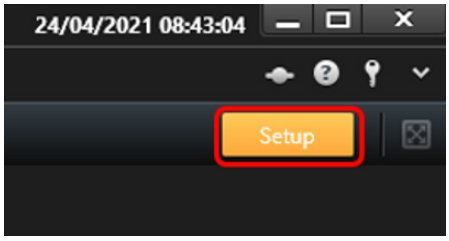
There are many options for the display and management of Access Control data in the Milestone Smart Client. The ORBNET Systems for Brivo integration seeks to enable many of these.

To begin, log into the Smart Client with a user who is a member of a role with Access Control Settings enabled in the Milestone Management Client.



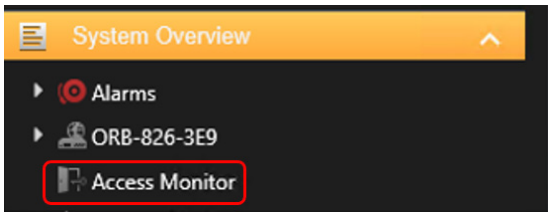
Smart Client Features and Setup

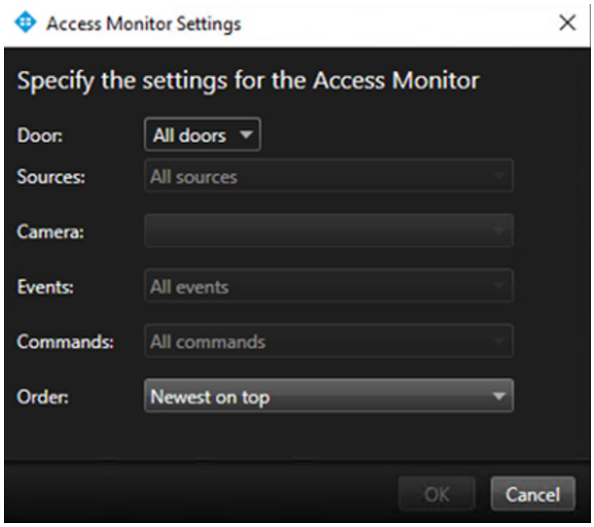
Once logged into the Smart Client, enter **Setup** mode via the right-hand site menu. This allows access to the setup of the features that follow. The menu bars will show in orange to indicate setup is enabled.

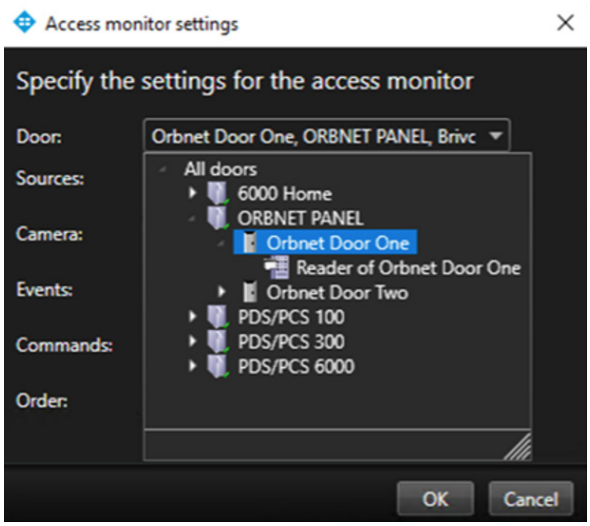


Access Monitor

Drag the **Access Monitor** into the window tile and select the source door. Now choose the events to be received from a specific door. It is recommended to select a door for the **Access Monitor** instead of the reader as it will provide more events.

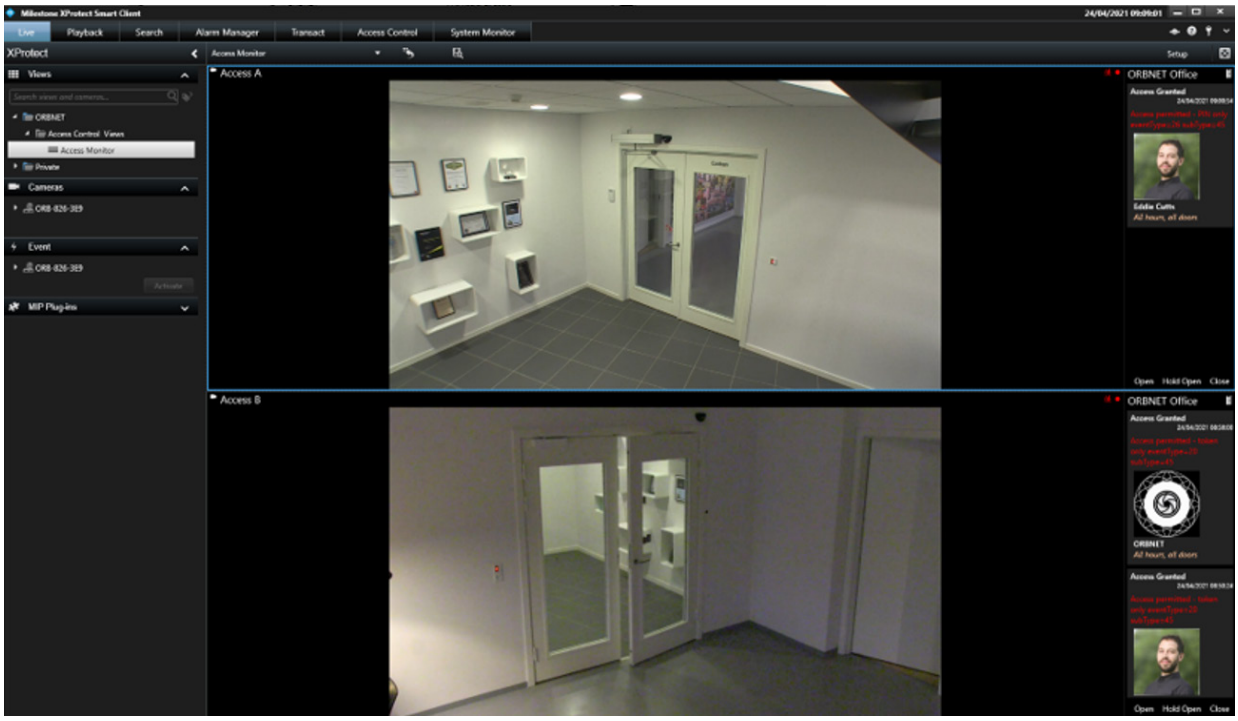






The below example is of a door with one reader. Here there is door / 2 readers and 2 cameras. The same door is associated with both windows in the Smart Client and individual readers per door.

View shown in Smart Client where the related or select camera feed is shown with door events shown to the right of the tile. When an event is clicked, you will be taken back to playback within the tile showing the time the event occurred.



Smart Client Maps

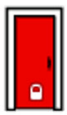
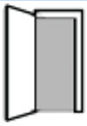
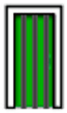
All the Brivo components can be added to a map created within the Milestone Smart Client.

Icons for the **Doors** and **Readers** can be added to the Milestone Maps. Note that in the screenshot below the reader icon will change color depending on the credential result.

Doors will show Red when locked, an Open door when unlocked. For the override states these show with bars on the door to indicate a fixed state of Locked (Red) or Unlocked Green). Readers will flash green or red depending on the badge presented and be in the normal state otherwise.

When a device is offline or there is a connection issue the device icon with a cross will be shown.

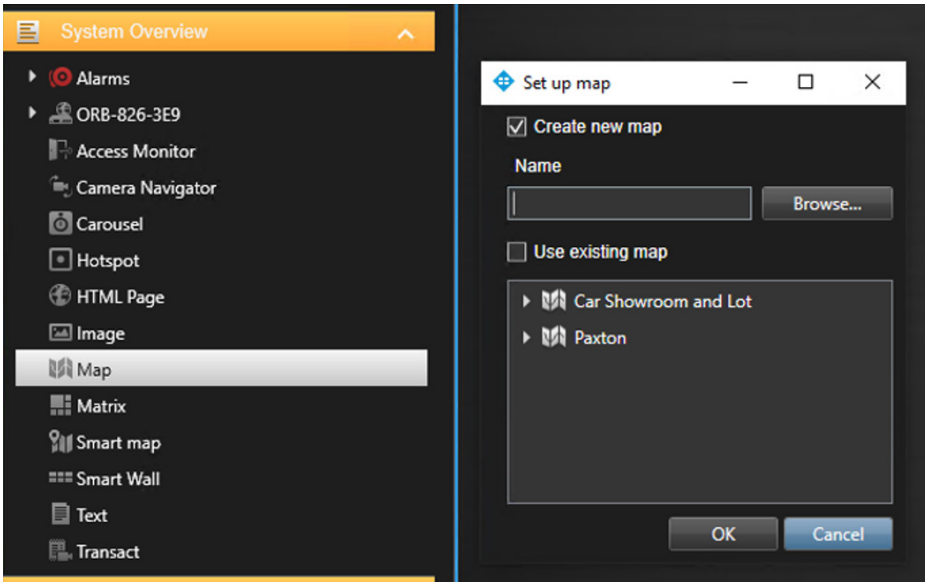
Door States

Locked	Unlocked	Override Lock	Override Unlock	Offline
				

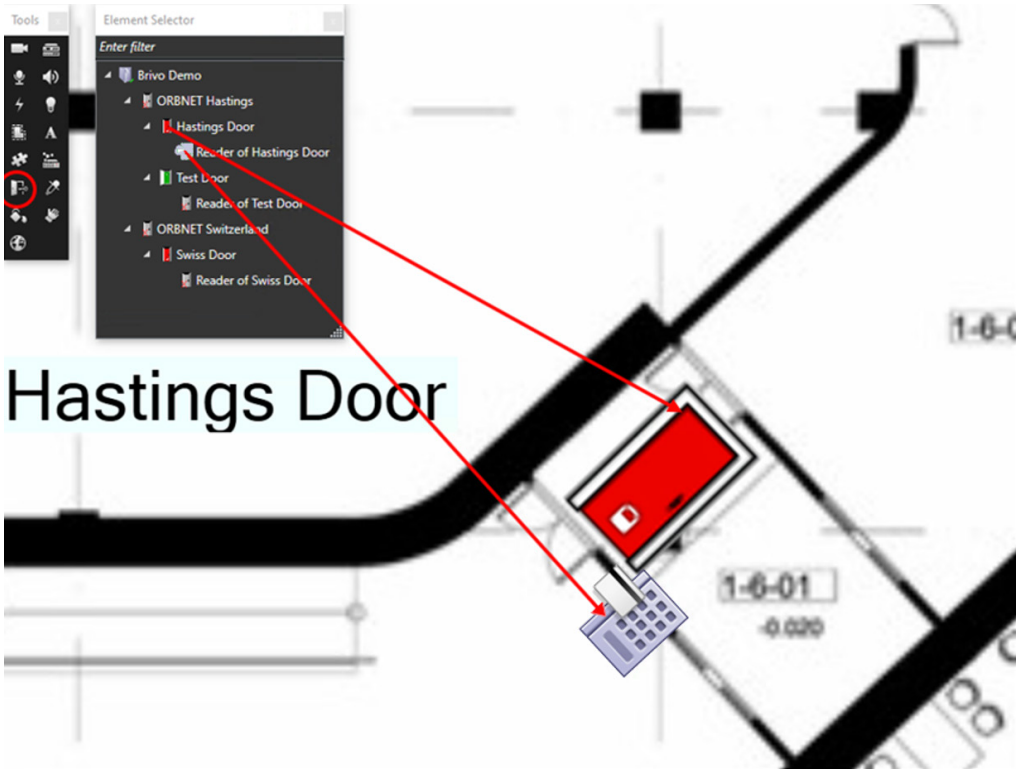
Reader States

Normal	Access Granted	Access Denied	Offline	
				

Under **Setup** mode, create a new view layout (Recommended 1x1), and drag the Map component into the blank tile. Select a floor plan image representing your site layout.



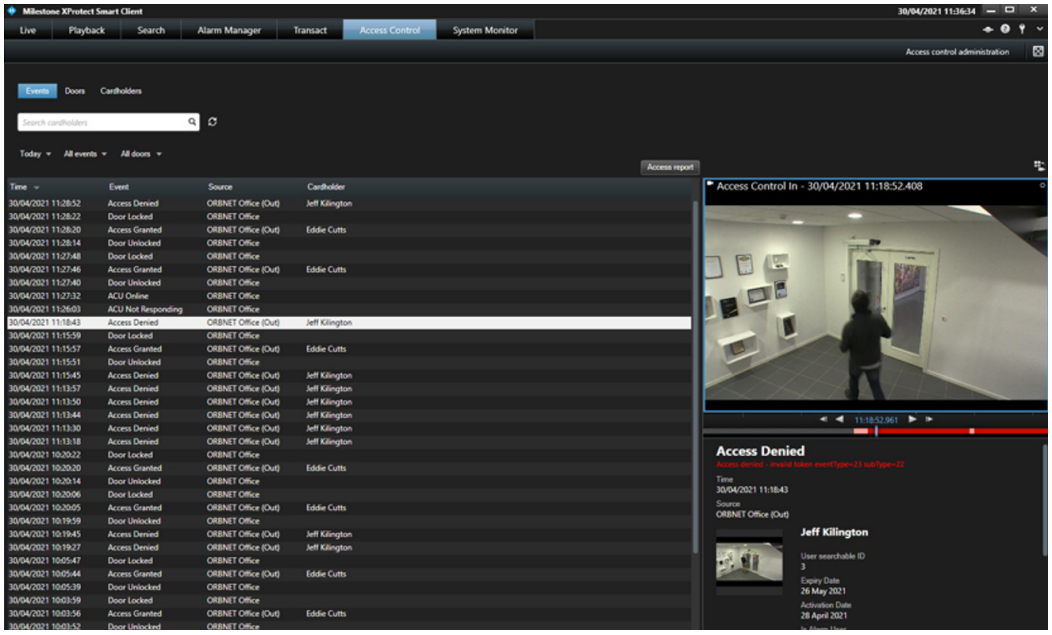
From the **Tools** menu, select **Access Control**. From the drop-down list, you will now see Brivo devices that have been enabled within Milestone.



Access Control Tab

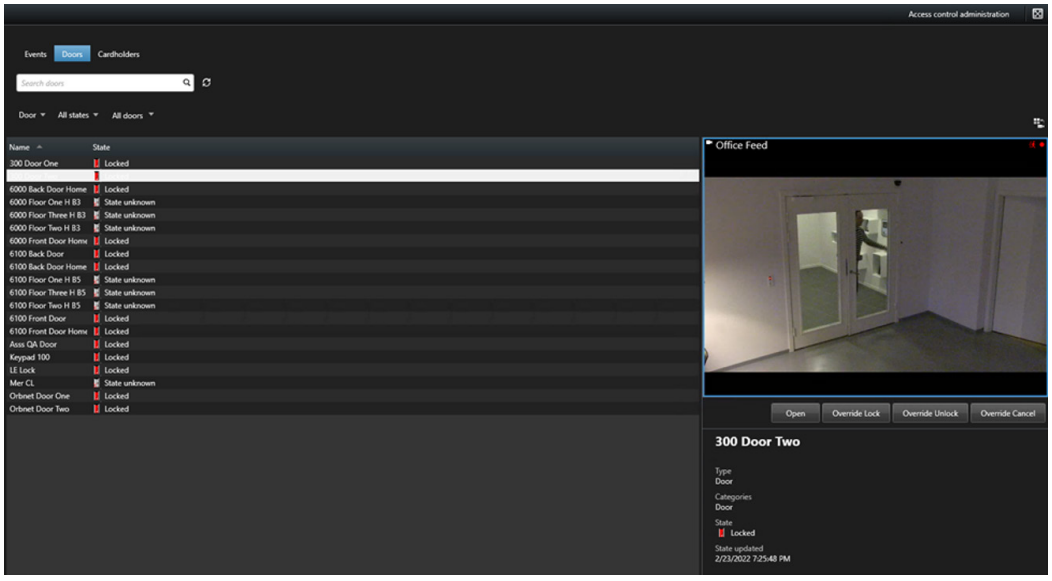
The **Access Control Tab** in the Milestone Smart Client can be used as the central monitoring interface for the access control system. Events can be searched by Event type, specific doors and or cardholders. There is also an option to have the list update live.

Once an event is selected, as shown in the below screenshot – additional information is shown from the door, cardholder, or event type.

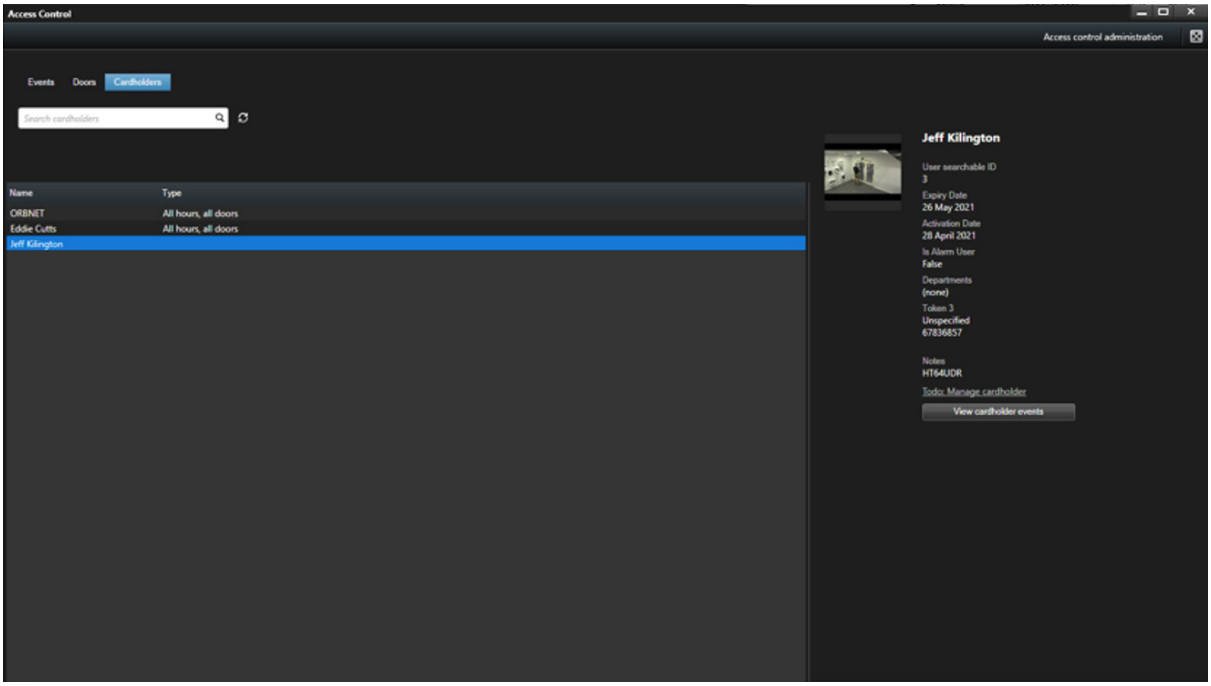


The **Doors** tab shows the list of doors in the system allowing control of the door from Milestone.

The controls shown are **Open**, **Override Lock**, **Override Unlock**, and **Override Cancel**.



The **Cardholders** tab allows the test search of users and the single click search of all events for a specific user. It is then possible to create a report complete with a screenshot thumbnail for every event for the cardholder.

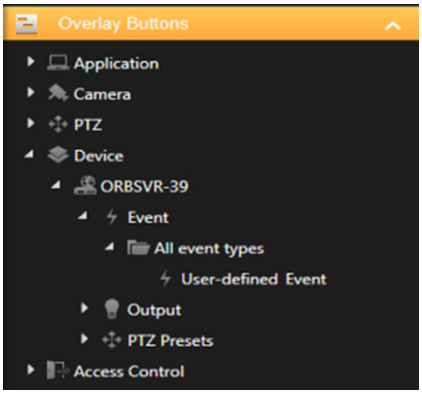


User-defined Event

From a layout that is already created, find **Overlay Buttons > Device > {Server-Name} > Events > All Event Types > {User Created User-Defined Event}**.

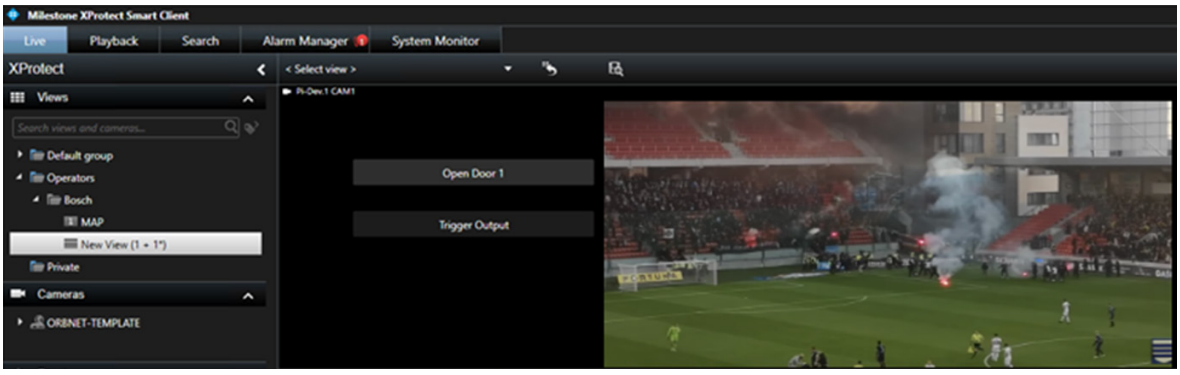
NOTE: See **User-Defined Events** section under Milestone Rules and Alarms in this document for more information.

Drag and drop this onto a tile, this will show as a push button over the camera tile.



When out of setup in Live mode, you will see the **Overlay Button** only when the mouse is hovered over the camera tile. These can only be used in a camera tile.

As shown below, **Open Door 1** and **Trigger Output**.



Troubleshooting

Event Server Installation

If Milestone was installed via a custom installation, the Event service may not have been included as it is not always required.

From the server/machine with the Milestone Management service follow to http://localhost/installation/admin/

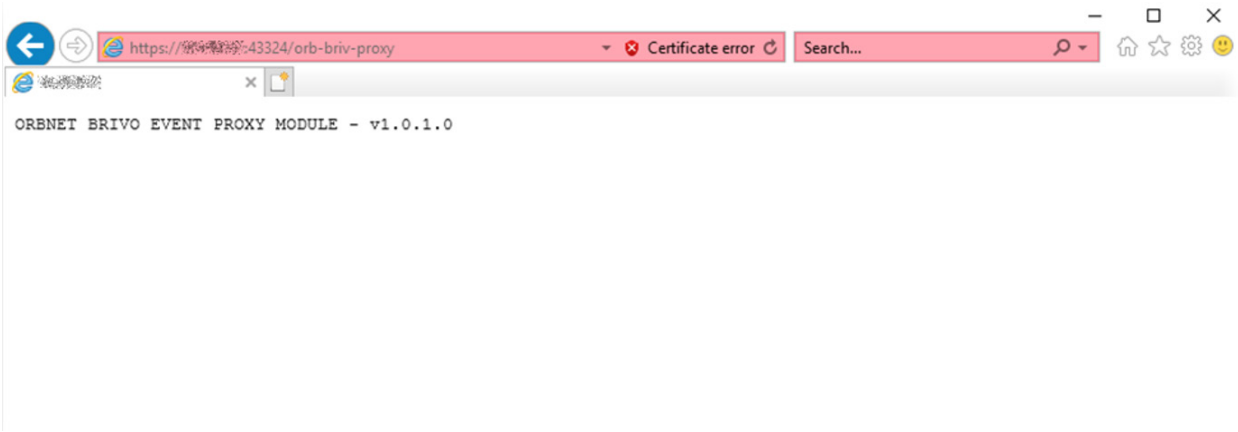
This will provide a Milestone installation page where you will be about to run the installer for the Event Server. This must be installed so the ORBNET plugin can communicate with Milestone.

Unable to receive configuration from the access control system

If Milestone is unable to communicate with brivo please check your access to the below site. A firewall rule will need to be implemented to allow this connection.

https://<ipOrHostname>:<port>/orb-briv-proxy/eventscallback/

Use your external IP and the Port used for this service and remove **eventscallback/** from the end of this URL. You should be able to access the below webpage with your external IP and port **43323** [default internal port].



Changing Default Proxy Port

To update the default port a manual change is needed in the config file. Stop the Proxy service first, before changing and saving this. Ensure this is updated in the Milestone Management Application general settings for the brivo connection.

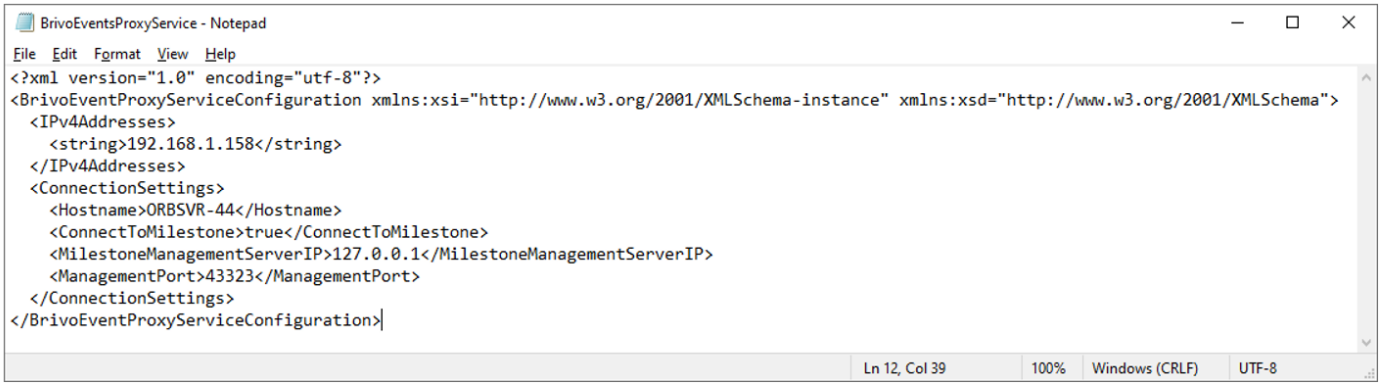
For Service Accounts;

C:\Users\<user>\AppData\Local\Brivo Events Proxy\Brivo Events Proxy

For Network Service Accounts;

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Brivo Events Proxy\Brivo Events Proxy

BrivoEventsProxyService.xml



Revision List

Date	Version	Author	Description
March 10, 2022	1.0		Initial Draft