Gallagher Command Centre

MIP Plugin Feature v4.0

(Supports Command Centre 8.90.1234 or later Command Centre release)

C12730

Release Note

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Copyright Notice

Contents

1 Introduction

This release note is for the 'MIP Plugin' v4.0.32 feature of Gallagher Command Centre.

1.1 Purpose

The 'Milestone Integration Platform (MIP) Plugin' feature integrates Command Centre with the Milestone Video Management System (VMS). It has been developed using the Milestone SDK 2024 R1.

1.2 Functionality

This feature provides the following functionality:

1. **Share Command Centre events and alarms with Milestone XProtect VMS**

   This feature enables events from mapped Command Centre items to:

   - be sent to and viewed in Milestone XProtect VMS
   - be mapped between the two systems
   - trigger Milestone actions (for example, view associated cameras).

2. **Clear Command Centre alarms with Milestone XProtect VMS**

   Processing or acknowledging an alarm in Milestone does the same in Command Centre. This removes the need to clear an alarm in both Command Centre and Milestone XProtect VMS. Processing an alarm in Command Centre also does the same in Milestone XProtect VMS.

3. **Override Command Centre items from Milestone XProtect VMS**

   Milestone operators can override Command Centre items. For example, a Door can be opened from a Milestone video feed, and Command Centre items can be overridden from a Milestone Map. Milestone Operators may visually identify a person before granting them access from the Milestone video feed. They can also view the status of Command Centre items in Milestone XProtect VMS.

4. **Display Command Centre Cardholder images and PDFs in Milestone XProtect VMS**

   You can display a Command Centre Cardholder image, and up to three non-image PDFs, in Milestone XProtect VMS when an access request is made. Any Cardholder that badges their card at a Gallagher reader has their photo, as well as other information (such as phone number, job title or vehicle registration plate number), displayed on the Milestone video wall in real-time. Cardholder PDFs are updated from Command Centre to Milestone in real-time.

Additional functionality: The following functionality can optionally be enabled with the separate Gallagher integration, 'Milestone VMS Integration':

- Live video viewing in Command Centre
- Stored video viewing in Command Centre
- Instructions from Command Centre to Milestone
- Milestone events to Command Centre
- Automatic Number Plate Recognition (ANPR) functionality.
- Automatic Command Centre camera tile aspect ratio
- 4k resolution footage

For more details about the 'Milestone VMS Integration', refer to the Milestone VMS Integration release note *"Release Note VMS Milestone (v8.30).pdf"* provided with the Milestone VMS Integration release. For a copy of this release note, contact the Gallagher Support Team.

1.3 New in v4.0

The following is added or changed in this version of this feature:

- Supports Milestone XProtect VMS 2024 R1

1.4 Compatibility

This feature introduces the following Gallagher software:

- Gallagher Milestone MIPS Integration v4.0.32

This feature supports the following Gallagher software:

- Gallagher Command Centre vEL8.90.1234 (or later Command Centre release)
- Gallagher Controller 6000 vCR8.80.220810b (or later release)
- Gallagher Milestone VMS Integration v9.10.70 (or later release)

Command Centre and this feature have been tested using the following:

- Command Centre Server: Windows Server 2022
- Command Centre Workstation: Windows 10 (64-bit)
- Database: SQL Server 2019

This feature has *not* been tested in a Command Centre multi-server environment.

This feature fully supports Milestone XProtect Server 2024 R1, 2023 R2, and 2021 R1.

Milestone 2023 R2 and 2021 R1: This feature supports Milestone XProtect Server 2023 R2 and 2021 R1 with one limitation: only one Access Control connection to Command Centre is supported. See section 11 *"Limitation"* for more information. Gallagher did not observe this limitation in 2024 R1.

Third Party Readers: Events, status, and overrides of Command Centre Third Party Readers in Milestone XProtect VMS are supported when using Command Centre vEL9.10 (or later release).

1.4.1 Equipment tested

This feature has been tested using the following Milestone software:

Milestone 2024 R1

- Milestone XProtect Management Server 2024 R1, Version 24.1a, Build 11269
- Milestone XProtect Event Server 2024 R1, Version 24.1a, Build 11269
- Milestone XProtect Smart Client 2024 R1, Version 24.1a, Build 11269
- Milestone Xprotect Management Client 2024 R1, Version 24.1a, Build 11269

Milestone 2023 R2

- Milestone XProtect Management Server 2023 R2, Version 23.2a, Build 32
- Milestone XProtect Event Server 2023 R2, Version 23.2a, Build 30
- Milestone XProtect Smart Client 2023 R2, Version 23.2.41.1, Build 49
- Milestone XProtect Management Client 2023 R2, Version 23.2a, Build 32

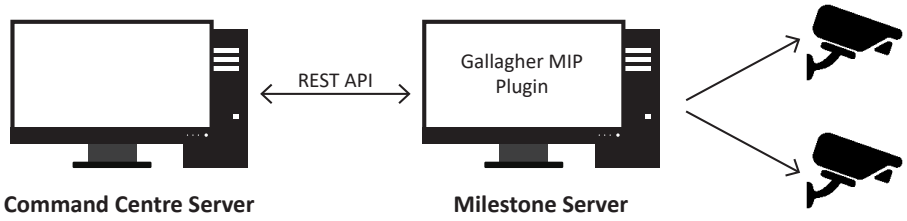
Milestone 2021 R1

- Milestone XProtect Management Server 2021 R1, Version 21.1b, Build 12177
- Milestone XProtect Event Server 2021 R1, Version 21.1b, Build 7871
- Milestone XProtect Smart Client 2021 R1, Version 21.1b (64-bit), Build 7361
- Milestone XProtect Management Client 2021 R1, Version 21.1b, Build 12177

1.5 Deployment architecture

The diagram below demonstrates the **minimum** deployment architecture for this feature.

However, this feature may be used in conjunction with the Milestone VMS Integration, in which case your deployment would also consist of a Middleware PC and any workstations you require.



Note: The port number 8904 should be used for communication between servers.

1.5.1 Setup recommendations

The date and time (time zone) used on all devices must be the same (that is, the date and time on the Command Centre server and all Milestone devices must be the same). If the time zones are not synchronised, an operator may miss viewing an event associated with an alarm.

1.6 Licences required

Command Centre licence

Ensure your licence file (CommandCentre.lic) contains the following entry:

```
[Features]
Milestone=1
```

Milestone licence

Additional Milestone server licensing is required for some Command Centre items to integrate with Milestone. For example, you require an Access Control Module (ACM) Base Licence, and ACM Door Licences for each door that will be connected to a camera. Please contact your Milestone representative for assistance.

2 Command Centre Operator Privileges

The following Command Centre Operator Privileges are applicable for the REST Client Operator used for this feature:

Privilege	is required to...
Edit Alarms	acknowledge and process alarms in Milestone
View Site	configure Milestone
Override	override site items in Milestone
Override - Open Door	open Doors in Milestone
View Cardholders	view Cardholders in Milestone
View Events and Alarms	view Events and Alarms in Milestone

The Operator's Divisions
In Milestone XProtect VMS, you can only view the Command Centre items, and the events of these items, that are in the Division(s) that the REST Client Operator has access to. Give the REST Client operator's Operator Group access only to the Division(s) whose items and their events you want to be viewable in Milestone XProtect VMS.

Configure the Operator Group
Assign the appropriate Operator Privileges and Divisions to the appropriate operators. For instructions on assigning operator privileges, refer to the topic *"Setting up Operator Groups"* in the Configuration Client Help.

3 Installation

To install this feature, perform the following procedure. If a previous version of this integration has been installed and you are upgrading to a newer version, skip section 3 *"Installation"* and refer to section 7 *"Upgrading"* later in this release note.

1. Perform a backup of your Command Centre system.
2. Ensure your licence file contains the following entry:

   ```
   [Features]
   Milestone=1
   ```

   Notes:

   - Additional Milestone server licensing is required for some Command Centre items to integrate with Milestone. For example, you require an Access Control Module (ACM) Base Licence, and ACM Door Licences for each door that will be connected to a camera. Please contact your Milestone representative for assistance.
   - While this feature uses the Gallagher REST API, you do not need a REST API licence.
3. On the Command Centre Server and all Command Centre Workstations, install Command Centre vEL8.90.1234 (or later release) from the Command Centre installation media, if not already installed.
4. On the Milestone server, run the installation executable **Gallagher Milestone MIPS Integration Setup 4.00.xx**.
5. To ensure this feature has installed correctly, select the **Programs and Features** utility from the Windows Control Panel on the Milestone server.

   The program 'Gallagher Milestone MIPS Integration' should be listed as currently installed.

4 Configuration

To configure this utility, perform steps 4.1 and 4.2, and 4.3 on the **Command Centre server**:

4.1 Enabling REST API

To enable REST API, refer to the topic *"Web Services"* in the Gallagher Configuration Client Help.

4.2 Creating a REST API Client Item

To create a REST API Client Item, refer to the topic *"Creating a REST API Client Item"* in the Gallagher Configuration Client Help.

4.3 The REST API Certificate

For the Command Centre and Milestone servers to connect, you will likely need to store your Command Centre Server's REST API Certificate in the Milestone server's Trusted Root Certification Authorities store.

If...	**then...**
your site is using the 'Default Internal Certificate' as the Command Centre Server's REST API Certificate,	store the REST API Default Internal Certificate in the Trusted Root Certification Authorities store on the Milestone server.
your site is using a 'Custom Certificate' as the Command Centre Server's REST API Certificate and the custom certificate is CA-signed,	no further action is required.
your site is using a 'Custom Certificate' as the Command Centre Server's REST API Certificate and the custom certificate is self-signed,	store the Command Centre Server's REST API Certificate or the signing certificate in the Trusted Root Certification Authorities store on the Milestone server.
your site is using an 'External Certificate' as the Command Centre Server's REST API Certificate and the external certificate is CA-signed,	no further action is required.
your site is using an 'External Certificate' as the Command Centre Server's REST API Certificate and the external certificate is self-signed,	store the Command Centre Server's REST API Certificate or the signing certificate in the Trusted Root Certification Authorities store on the Milestone server.

See the following page for help storing the REST API Certificate on the Milestone server.

To view your Command Centre Server's REST API Certificate and install it in the Trusted Root Certification Authorities store on the Milestone server, perform the following procedure:

1. From the Configuration Client menu bar, click **File** > **Server Properties**.
2. Click the **Web Services** tab.
3. Click the **Manage Certificates...** button in the 'Enable REST API' section.

   The Manage REST API Certificate window displays.
4. Click the **View...** button next to the Server Certificate option you are using (for example, if **Default Internal Certificate** is selected, click the **View...** button next to that option).

   The certificate displays with the **General** tab selected by default.
5. Click the **Details** tab.
6. Click the **Copy to File...** button.
7. In the Certificate Export Wizard, click **Next**.
8. Ensure **DER encoded binary X.XXX (.CER)** is selected, and click **Next**.
9. Click the **Browse...** button, enter a **File name** for the certificate (for example, 'REST API Certificate') and **Save** it somewhere (for example, on the Desktop).
10. Click **Next**, then **Finish**.
11. Copy the certificate to the Milestone server machine (for example, via a USB flash drive).
12. On the Milestone server, double-click the REST Client Certificate.
13. The REST Client Certificate opens.
14. Click the **Install Certificate...** button.
15. In the Certificate Import Wizard, select **Local Machine**, then click **Next**.
16. Select **Place all certificates in the following store**, then click the **Browse...** button.
17. Select the **Trusted Root Certification Authorities** folder, then click **OK**.
18. Click **Next**, then **Finish**.

Result: The Command Centre Server's REST API Certificate is installed in the Milestone server's Trusted Root Certification Authorities store.

Note: When using the default certificate:

a. Check the certificate's details, 'Subject Alternative Name', and make sure the IP address listed is the IP address of the Command Centre server.

b. If it is not the Command Centre server IP address, it cannot be changed. You must create a Self Signed certificate. Refer to the topic *"Creating the Client Certificate"* in the Gallagher Configuration Client Help.

   The DNSName must be the IP address of the Command Centre server. For example:

   ```
   New-SelfSignedCertificate -certstorelocation cert:\
   currentuser\my -dnsname 192.168.12.34
   ```

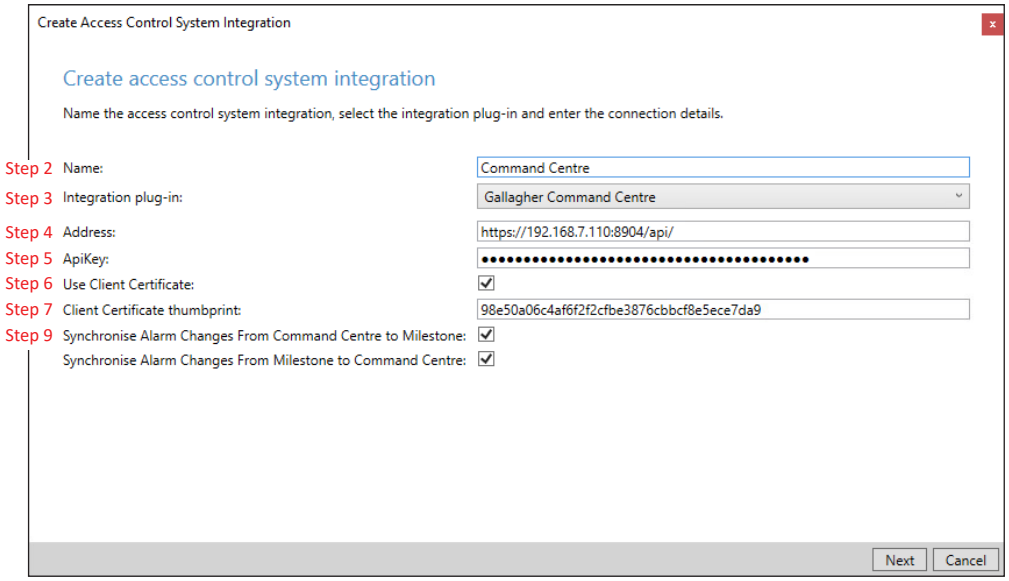
Perform steps 4.4 and 4.5 on the **Milestone server**:

4.4 Milestone XProtect Management Client

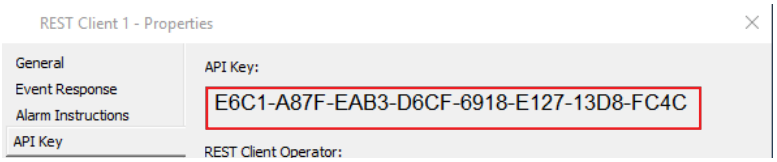
Setting up access control

To set up access control, perform the following procedure in XProtect Management Client:

1. In the XProtect Management Client, right-click on **Access Control** in the left-hand pane, and select **Create new...**



2. Enter a name for the access control system integration into the **Name** field.
3. Select **Gallagher Command Centre** from the **Integration plug-in** drop-down list.
4. Enter the IP address of your Command Centre server into the **Address** field.
5. Enter the API Key of your Command Centre server's REST Client item into the **ApiKey** field. Refer to section 4.2 "*Creating a REST API Client Item*" for help finding the API Key.

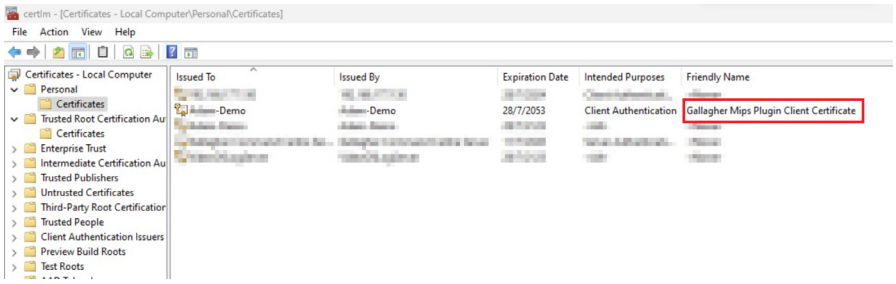


6. Select the **Use Client Certificate** check box.
7. In the **Client Certificate Thumbprint** field, enter the Certificate Thumbprint of the MIP Plugin certificate. This certificate is created automatically when the MIP Plugin is installed on the Milestone server.

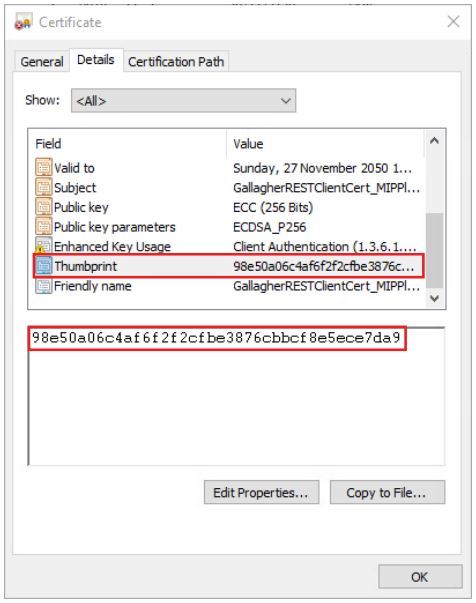
   To find this certificate on the Milestone server:

   a. Press + R on your keyboard, then type **certlm.msc** into the Run window text field, then click **OK**.

   b. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates** and double-click on the Client Certificate that was created by this plugin, (e.g. with Friendly Name 'Gallagher Mips Plugin Client Certificate').



c. Click on the **Details** tab and scroll down to select the **Thumbprint** item.



d. Find the Client Certificate Thumbprint in the grid below.

8. In the **Server Certificate Thumbprint** field, enter the Certificate Thumbprint of the Command Centre server's REST API certificate.

   To find this certificate on the Command Centre server:

   a. In Gallagher Configuration Client, select **File** > **Server Properties** > **Web Services**.

   b. In the 'REST API' section, click the **Manage Certificates...** button.

      The Manage REST API Certificate window displays.

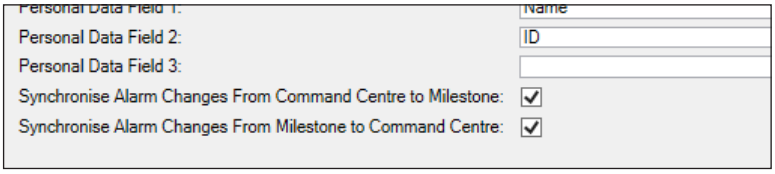
   c. Next to whichever option is selected, click the **View** button.

      The certificate properties window displays.

   d. Click on the **Details** tab and scroll down to select the **Thumbprint** item.

   e. Find the Server Certificate Thumbprint in the grid below.

9. Select the two check boxes **Synchronise Alarm Changes From Command Centre to Milestone** and **Synchronise Alarm Changes from Milestone to Command Centre**.



10. Click **Next**.

    The configuration is successfully received from Command Centre. You will be able to see your Command Centre server configuration, such as your Doors, Units, and Servers.

    Note: If Milestone XProtect fails to connect to Command Centre, check the Command Centre Event Viewer for REST API-related errors.

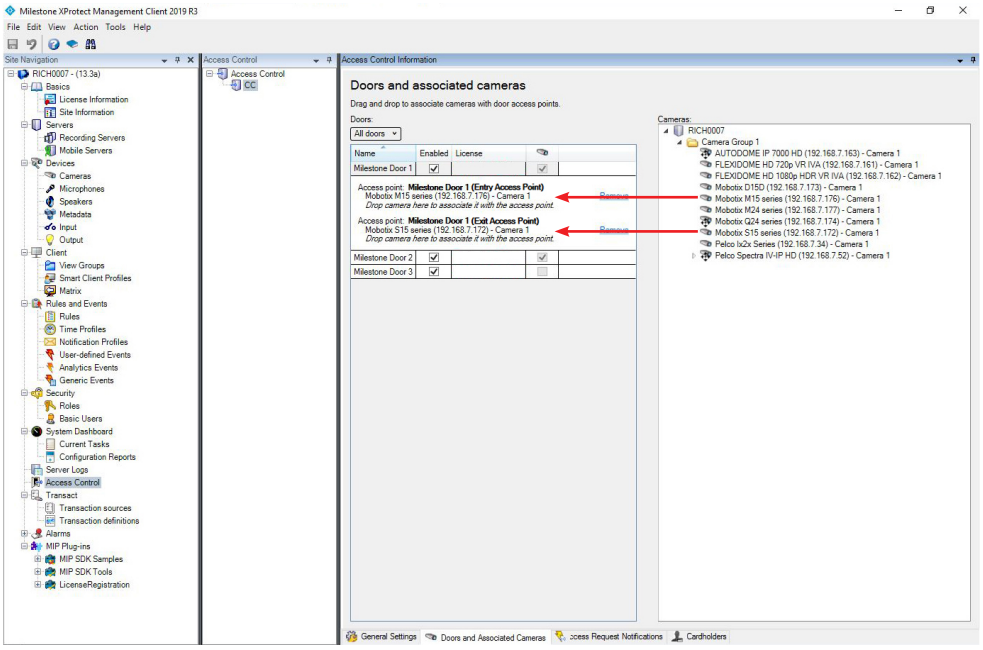
    Notes:

    - The Command Centre items you can see here represent all of the events that Milestone can receive.
    - **Doors** will show all configured Doors that have a controller attached, and that your operator has the divisional privileges to view.
    - **Units** will show all configured controllers that your operator has the divisional privileges to view.
    - To view a Door or Unit that is configured with a parent, an operator also needs the divisional privileges to view the item's parent. For example, an operator must be privileged to view a Door's Controller for the Door to be mapped to Milestone.
    - Whenever you make a change to your Command Centre configuration (for example, add a Door), you should go to General Settings of your Access Control item and click **Refresh Configuration**.
      Your Configuration is then updated on the Milestone server.

Associating Cameras with access points

Your Doors each have 'access points', one for the entry and one for the exit.
To associate cameras with your Doors' access points, perform the following procedure:

1. Click on the **Doors and Associated Cameras** tab of your access control integration.



2. Click and drag a camera from the **Cameras** grid onto an access point (Door exit/entry) to associate the camera with that access point.

3. To save, click the button in the top-left corner of the Management Client window.

Notes:

- More than one camera can be associated with an access point.
- The camera associated with an access point is used in XProtect Smart Client when an access control event related to that access point is triggered.

Mapping Cardholders and PDFs from Command Centre to Milestone

To have Cardholders and configured Personal Data Fields (PDFs) appear in the Cardholders tab of Milestone XProtect Management Client, perform the following procedure:

Before

Before you proceed, ensure you have configured an image type PDF and up to three other non-image type PDFs in Command Centre, and applied these to appropriate Access Groups. Cardholders must have PDF values assigned to them in Command Centre for the values to appear in Milestone XProtect Management Client.

Procedure

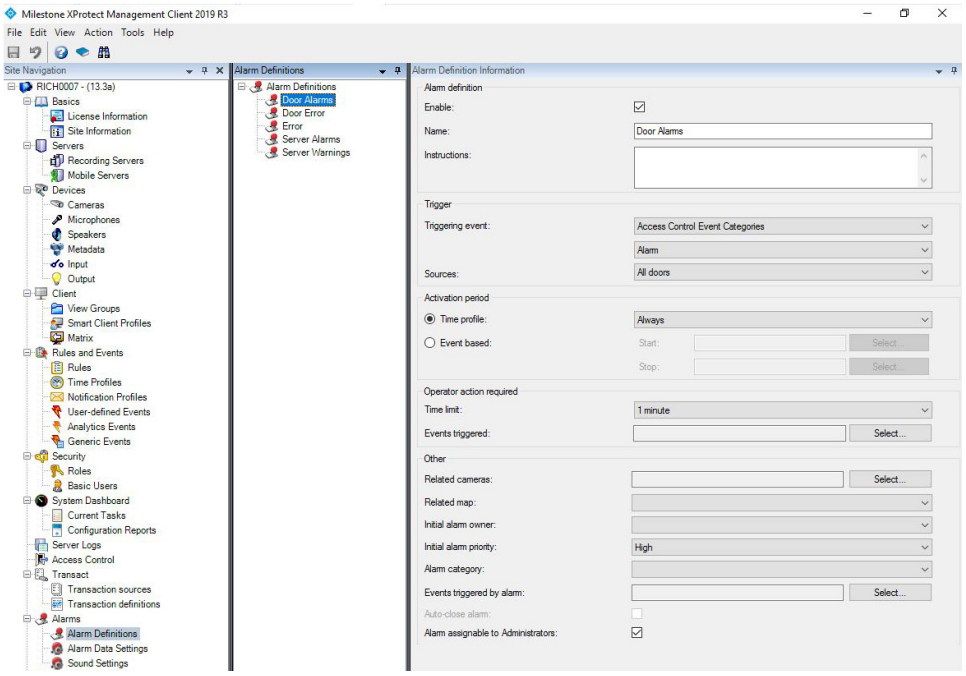
1. Double-click on your newly configured access control integration item (if not already open).
2. Click on the **General Settings** tab.
3. Enter the exact name of your Command Centre image PDF in the **Cardholder Image PDF** field.
4. Enter the exact names of (up to) three other Command Centre non-image PDFs in the **Personal Data Field 1**, **Personal Data Field 2** and **Personal Data Field 3** fields, respectively.
5. To save, click the  button in the top-left corner of the Management Client window.
6. Restart the Milestone XProtect Event Server Service to update all Cardholder PDF values in Milestone.
7. In the **Cardholders** tab of your access control integration, you can see the configured PDFs and relevant values when viewing a Cardholder. When a Cardholder's PDF values are changed in Command Centre, you will see the change reflected in Milestone XProtect Management Client immediately.

Configuring alarm definitions

For Gallagher events and alarms to appear as alarms in Milestone XProtect Smart Client, you must create alarm definitions in Milestone XProtect Management Client. Create as many alarm definitions as required to receive all desired Command Centre events.

To create an alarm definition, perform the following procedure:

1. In XProtect Management Client, right-click on **Alarm Definitions** (under **Alarms**) in the left-hand pane, and select **Add new...**



2. Ensure the **Enable** check box is selected.
3. Give the alarm definition a meaningful name (for example, 'Door Alarms' if you are creating this to define Door alarms).
4. Select **Access Control Event Categories** from the **Triggering event** drop-down list.
5. Select the source of alarm that will match this alarm definition from the **Sources** drop-down list. Select a Door, or click **Other...** and select a Command Centre item.

   Selecting **All doors** will match with alarms from all doors. Selecting one of your configured Doors or Command Centre items will match with alarms from that Door/item only.
6. To save, click the button in the top-left corner of the Management Client window.

   Events that match your configured alarm definition will now appear in the Milestone XProtect Smart Client Alarm Manager. Event synchronisation from Command Centre to Milestone is real-time.

Adding a user to Milestone XProtect Management Client

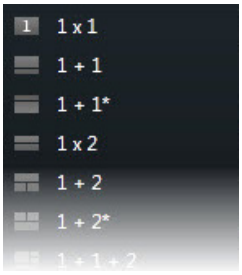
To create roles, users and groups, search for the topic *"Site Navigation: Security"* in the Milestone Documentation. Visit: https://doc.milestonesys.com/2024r1/en-US/index.htm

4.5 Milestone XProtect Smart Client

Create a View in Milestone XProtect Smart Client

To create a View, perform the following procedure:

1. In the right corner, click **Setup** to enter setup mode.
2. In the **Views** pane, select the group you want to add the view to.
3. Click  to create a new view.
4. Select a layout. The layouts are grouped according to their aspect ratio, (i.e. the height/ width relationship of an image), and according to whether they are optimized for regular content or content in portrait mode, (i.e. where the height is greater than the width).

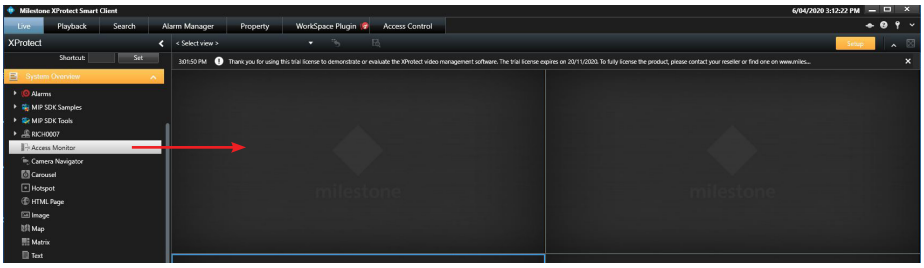


5. Enter a name for the view by overwriting the default **New View** name.
6. Click **Setup** again to exit the setup mode.

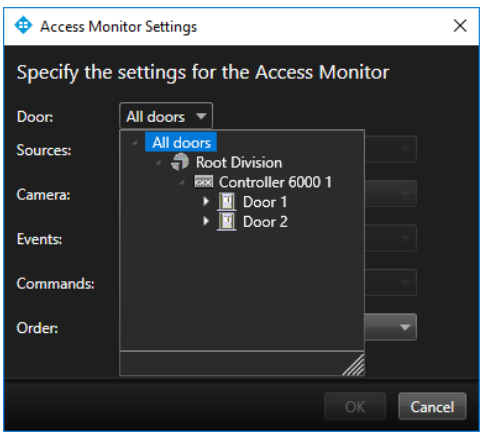
Configure a View in Milestone XProtect Smart Client

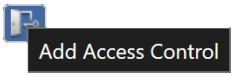
Note: Each Milestone operator must have their own Views configured.

1. Once you have created a View, click and drag **Access Monitor** from the **System Overview** pane into one of the grids in the new View.



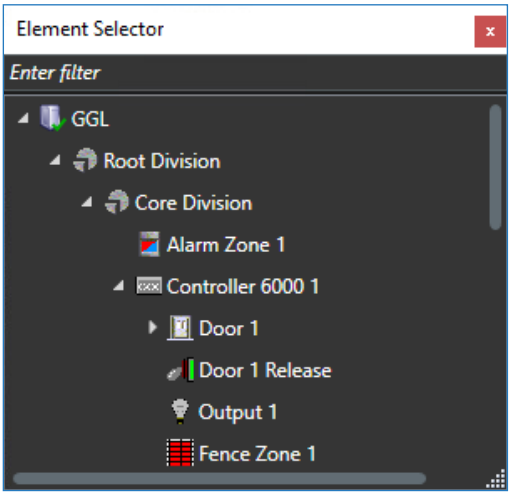
The Access Monitor Settings window displays.



2. Select your desired Door for the grid.
3. Change any other Access Monitor settings as required, then click **OK**.
4. Do you wish to add a Map (similar to a Command Centre Site Plan) to the View?
   If yes, go to Step 5.
   If no, go to Step 8.
5. To add a Map to the View, search for the topic *"Maps (configuration)"* in the Milestone Documentation.
   Visit: https://doc.milestonesys.com/2024r1/en-US/index.htm
6. To add a Command Centre item to the Map, click the 

button from the Tools menu.

   The Element Selector window displays.



7. Find your desired item (for example, a Door), then click and drag it onto the Map in the appropriate location.
8. Click the **Setup** button again to finish setup.

   The View is configured.

   Note: When an event associated with one of the Doors you configured for this View is generated, the associated Cardholder's details will display in the appropriate grid.

5 Using Milestone XProtect Smart Client

5.1 Performing Command Centre overrides in Milestone XProtect Smart Client

In the Milestone XProtect Smart Client, you can perform an override on any item you can override in Command Centre. For example:

In an Access Monitor grid on a View, click **Unlock** under the Door you want to unlock.

Or, if you have a Map with a Command Centre item set up in the View, right-click on the item and select an override.

Notes:

- An override event will be raised in Command Centre by your REST operator.
- The event will be logged in your Milestone XProtect Management Client Audit logs.
- Milestone Doors will unlock for however many seconds you have specified for **Door unlock time** in the Advanced tab of the Door in Command Centre.

5.2 Processing and Acknowledging alarms

Alarms can be viewed in the Milestone XProtect Smart Client Alarm Manager. Alarms are sorted by four alarm states:

- **New** - An unacknowledged alarm in Command Centre
- **In progress** - An acknowledged alarm in Command Centre
- **On hold** - Only relevant to Milestone, will show as acknowledged in Command Centre
- **Closed** - A processed alarm in Command Centre

Acknowledging or processing an event in Command Centre will do the same in Milestone, and vice versa.

To change the state of an alarm in the XProtect Smart Client Alarm Manager, right-click on the alarm and select one of the three options: **Acknowledge**, **Set on hold**, or **Close**.

Notes:

- Changing the state of an alarm to **Acknowledge** will move the alarm to **In progress**.
- Changing the state of an alarm to **Set on hold** will move the alarm to **On hold**.
- Attempts to change the state of an *active* alarm to **Closed** while it is **New** will not work, it will remain in **New**.
- Attempts to change the state of an *active* alarm to **Closed** while it is **In progress** or **On hold** will move it back to **New**.

5.3 Alarm flooding

If a Milestone operator encounters a flooded alarm, it will appear as a large number of identical-looking alarms that 'flood' their alarm viewer. These similar alarms behave as 'flooded' alarms. The earliest occurring alarm in a set of flooded alarms acts as the main flooded alarm. Actions made on the main flooded alarm affect its associated alarms.

If an action is made on this main flooded alarm (for example, Closed) in Milestone, its associated alarms are subjected to the same action, and the flooded alarm is also processed in Command Centre. If an action is performed on the flooded alarm in Command Centre, the equivalent action will also be performed on the main flooded alarm and its associated alarms in Milestone.

If the main flooded alarm is still active in Milestone, it behaves identically to a normal active alarm when actions are made on it (see section 5.2 "*Processing and Acknowledging alarms*"), however, the associated alarms of the active main flooded alarm are not affected.

If an action is made on an associated alarm (not the main flooded alarm), only that associated alarm will be affected, and no future actions made on the main flooded alarm will affect that associated alarm. However, doing this may cause unexpected behaviour, and is unadvised.

6 Error messages

The following is an error message that may display within Milestone XProtect Management Client.

Message	Description
Unable to receive configuration from the access control system. Error message: Error fetching configuration from Command Centre. See the MIP logs for more information.	**When creating an access control system:** This is caused by an incorrect value in your access control setup, for example, an incorrect API key or IP address. Make sure the specified connection details are correct. **When updating an access control system:** This is caused by your REST operator not having the correct privileges, or by a communications issue.

7 Upgrading

You may wish to upgrade just your MIP Plugin version, or both your MIP Plugin and Command Centre versions. The MIP Plugin v4.0 requires Command Centre vEL8.90.1234 or later release.

7.1 Upgrading Command Centre

If your installed Command Centre version is lower than vEL8.90.1234, or you would like to upgrade to a later Command Centre release, perform the following procedure. Otherwise, go to section 7.2 *"Uninstalling the MIPS Integration"*.

1. Perform a backup of your Command Centre system.
2. Exit Command Centre and stop the Command Centre Services.
3. Upgrade Command Centre to your desired version (vEL8.90.1234 or later release). Refer to the document *"3E0068 Release Note Gallagher Command Centre vELx.xx.xxxx (Upgrade Procedures).pdf"* located on the Gallagher installation media.
4. Restart the Command Centre Services.

7.2 Uninstalling the MIPS Integration

1. On the Milestone server, stop the MilestoneEventServerService.
2. Use the Windows **Programs and Features** utility to remove the program 'Gallagher Milestone MIPS Integration'.

7.3 Installing the MIPS Integration

1. On the Milestone server, run the installation executable **Gallagher Milestone MIPS Integration Setup 4.00.xx**.
2. To ensure this feature has installed correctly, select the **Programs and Features** utility from the Windows Control Panel on the Milestone server.

   The program 'Gallagher Milestone MIPS Integration' should be listed as installed.
3. Restart the MilestoneEventServerService.
4. In Milestone XProtect Management Client, go to General Settings of your Access Control item and click **Refresh Configuration**.

7.4 Uninstalling the MIPS Extension

The MIP Plugin v3.0 and later versions do not use the MIPS Extension.

1. Exit Command Centre and stop the Command Centre Services.
2. On the Command Centre Server, use the Windows **Programs and Features** utility to remove the program 'Gallagher Milestone MIPS Extension' (if installed).
3. Restart the Command Centre Services.

7.5 Adding the Server Certificate Thumbprint in Milestone XProtect

The MIP Plugin v4.0 adds a requirement for the Command Centre Server's REST API Certificate thumbprint to be added to the Access Control settings in Milestone XProtect Management Client. Connection between the two systems will fail until this is added.

1. In the XProtect Management Client, select **Access Control** from the left-hand pane, then select the Command Centre Access Control item.

   Note: Command Centre Access Control items will have 'Gallagher Command Centre' in the 'Integration plug-in' field on their 'General Settings' tab.

2. In the **Server Certificate Thumbprint** field, enter the Certificate Thumbprint of the Command Centre server's REST API certificate.

   To find this certificate on the Command Centre server:

   a. In Gallagher Configuration Client, select **File** > **Server Properties** > **Web Services**.

   b. In the 'REST API' section, click the **Manage Certificates...** button.

      The Manage REST API Certificate window displays.

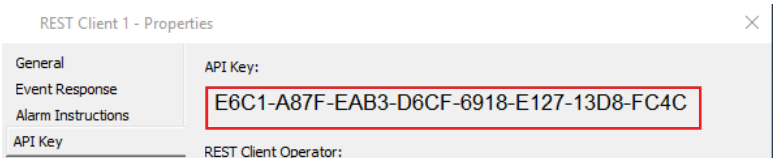
   c. Next to whichever option is selected, click the **View** button.

      The certificate properties window displays.

   d. Click on the **Details** tab and scroll down to select the **Thumbprint** item.

   e. Find the Server Certificate Thumbprint in the grid below.

3. Since you modified the settings, you may need to re-enter the API Key of your Command Centre server's REST Client item into the **ApiKey** field. Refer to section 4.2 "*Creating a REST API Client Item*" for help finding the API Key.



8 Uninstallation

To permanently uninstall this feature, use the Windows **Programs and Features** utility to remove the program 'Gallagher Milestone MIPS Integration' from the Milestone server.

9 Considerations

- Similar to Command Centre's Controlled Challenge functionality, Milestone has access request functionality. **Gallagher recommends that Milestone access request is not used**. 'Access request' means events can be mapped from Command Centre to appear in Milestone as access request events. The associated Command Centre Door can then be overridden from Milestone to allow the Cardholder entry. **However**, issues with this functionally include:
    - Command Centre Zone counting is inaccurate because no Command Centre Cardholder Entry events are generated.
    - Command Centre Evacuation Reports are inaccurate because Command Centre loses track of what Zone Cardholders are in.
    - When a Door is overridden to open, an Access Granted event is not generated in Command Centre, and an Access Denied event is still generated.
    - Command Centre Tagboards show inaccurate information.
- Alarm notes are not shared between Command Centre and Milestone systems. When processing an alarm in Command Centre or Milestone, the alarm is processed in Command Centre, but any specified alarm note is not shared with the other system.
- The MIP Plugin supports viewing the status of Doors, Access Zones, Fence Zones, Alarm Zones, Outputs, Inputs, and Macros in Milestone.
- Only the 'Normal' and 'Offline' Intercom statuses are reflected in Milestone:
  - 'Call ringing', 'Call connected', 'On hold', etc. appear as 'Normal',
  - 'The intercom endpoint is offline' appears as 'Normal',
  - 'The intercom system server is offline' appears as 'Offline', and
  - all other error states appear as 'Offline'.
- The MIP Plugin v4.0 adds a requirement for the Command Centre Server's REST API Certificate thumbprint to be added to the Access Control settings in Milestone XProtect Management Client. Connection between the two systems will fail until this is added. You may get an error stating 'Unable to receive configuration from the access control system' when modifying the Access Control settings in XProtect Management Client. To fix this, refer to section 7.5 *"Adding the Server Certificate Thumbprint in Milestone XProtect"*.

10 Limitation

- Gallagher found that Milestone 2021 R1 and 2023 R2 only support one Command Centre Server Access Control item (i.e. they do not support multiple Command Centre Servers). If multiple Access Control items are configured for Command Centre Servers in Milestone 2021 R1 or later release, all but one are removed upon restarting the Milestone event service.

  Gallagher did *not* observe this limitation in Milestone 2024 R1. If you require Milestone Access Control items for multiple Command Centre Servers, ensure you use Milestone 2024 R1.

11 Requesting more items or events to be added

Items
The Command Centre items you can view in Milestone are defined in the file 'CommandCentreTypeMappings' located in `C:\Program Files\Milestone\MIPPlugins\Gallagher Milestone MIPS Integration`
If you require additional item types to be added, contact the Gallagher Support Team.

Icons
The icons for the Command Centre items you can view in Milestone are defined in the file 'CommandCentreIconMappings' located in `C:\Program Files\Milestone\MIPPlugins\Gallagher Milestone MIPS Integration`
If you require additional icons to be added, contact the Gallagher Support Team.

Events
The Command Centre events you can view in Milestone are defined in the file 'CommandCentreEventMappings' located in `C:\Program Files\Milestone\MIPPlugins\Gallagher Milestone MIPS Integration`
If you require additional event types to be added, contact the Gallagher Support Team.