Gallagher Command Centre

MIP Plugin Feature 8.30

(Supports Command Centre 8.30 or later CC 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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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' v1.00.133 feature of Gallagher Command Centre (CC).

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 2019 R3.

1.2 Functionality

This feature provides the following functionality:

1. **Share CC events and alarms with Milestone XProtect VMS**

   This feature enables Command Centre events to be sent to, and viewed in, Milestone XProtect VMS. Common events are mapped between the two systems by default, additional events can be configured.

2. **Clear CC 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.

3. **Open CC Doors from Milestone XProtect VMS**

   Milestone operators can open a CC Door from the Milestone video feed. This allows them to visually identify the person before they are granted access. Milestone Operators can also see the status of a CC Door in Milestone XProtect VMS.

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

   You can display a CC 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 CC to Milestone in real-time.

Note: The following functionality is enabled with the separate Gallagher integration, 'Milestone VMS Integration':

- Live video viewing in CC
- Stored video viewing in CC
- Instructions from CC to Milestone
- Milestone events to CC
- Automatic Number Plate Recognition (ANPR) functionality.
- Automatic CC 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 (v8.10).pdf"* provided with the Milestone VMS Integration release.

1.3 Compatibility

This feature introduces the following Gallagher software:

- Gallagher Milestone MIPS Integration v1.00.133

This feature supports the following Gallagher software:

- Gallagher Command Centre vEL8.30.955 (or later CC release)
- Gallagher Controller 6000 vCR8.30.200221a (or later release)

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

- Command Centre Server: Windows Server 2016, Windows 10
- Command Centre Workstation: Windows 10 (64-bit)
- Database: SQL Server 2017

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

1.3.1 Equipment tested

This feature has been tested using the following Milestone software:

- Milestone XProtect Smart Client 2019 R3, Version 13.3a, Build 23
- Milestone XProtect Management Client 2019 R3, Version 13.3a, Build 44

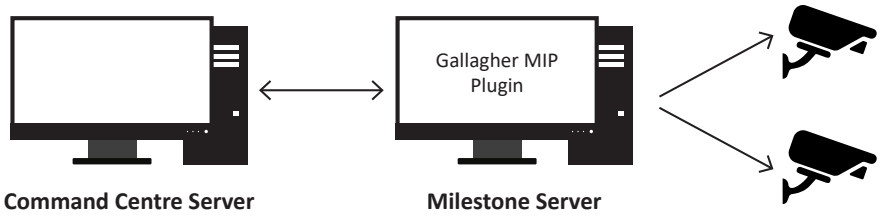
1.3.2 Setup recommendations

The date and time (time zone) used on all devices must be the same (i.e. 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.

1.3.3 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.



2 Command Centre operator privileges

The following Command Centre operator privileges are applicable for this feature:

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

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

3 Installation

To install this feature, perform the following procedure:

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

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

   Note: Additional Milestone server licensing may be required for Command Centre items to integrate with Milestone. Please contact your Milestone representative.
3. On the Command Centre server and all Command Centre workstations, install Command Centre vEL8.30.886 (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 1.00.xx.msi.**
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 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 Online 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 Online Help.

Then, perform steps 4.3 and 4.4 on the **Milestone server**:

4.3 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 tile, 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 CC server into the **Address** field.
5. Enter the API key of your CC server into the ApiKey field. Refer to section 3.2 *"Creating a REST API Client Item"* for assistance.
6. Ensure the **Use Client Certificate** check box is selected.
7. The client certificate thumbprint of your Milestone server will already be in the **Client Certificate Thumbprint** field.

   Copy this Certificate Thumbprint, and paste it into the **Client Certificate Thumbprint** field in the **API Key** tab of your REST Client item properties on your Command Centre server (**[your REST client item]** > **API Key**)
8. Click **Next**.
   The configuration is successfully received from Command Centre. You will be able to see your CC server configuration including your Doors, Units, Servers etc.

   Notes:

   - These CC items 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.

- Whenever you make a change to your CC configuration (e.g. 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.

Mapping Cardholders and PDFs from CC 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 CC 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 CC image PDF in the **Cardholder Image PDF** field.
4. Enter the exact names of (up to) three other CC 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. In the **Cardholders** tab of your access control integration, you can to see the configured PDFs and relevant values when viewing a Cardholder. When a Cardholder's PDF values are changed in CC, you will see the change reflected in Milestone XProtect Management Client immediately.

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.

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 tile, and select **Add new...**
2. Ensure the **Enable** check box is selected.
3. Give the alarm definition a meaningful name (e.g. 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. Selecting **All doors** will match with alarms from all doors. Selecting one of your configured Doors will match with events from that Door 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 CC 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/2020r1/en-US/index.htm

4.4 Milestone XProtect Smart Client

Configure a View in Milestone XProtect Smart Client

To create a View, search for the topic *"Views (configuration)"* in the Milestone Documentation.
Visit: https://doc.milestonesys.com/2020r1/en-US/index.htm

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** tile, into one of the grids in the new View.

   The Access Monitor Settings window displays.

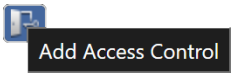
2. Select your desired Door for the grid.

3. Change any other settings as required.

4. Click **OK**.

5. Do you wish to add a Map (similar to a CC Site Plan) to the View?
   If yes, go to step 6.
   If no, go to step 9.

6. To add a Map to the View, search for the topic *"Maps (configuration)"* in the Milestone Documentation.
   Visit: https://doc.milestonesys.com/2020r1/en-US/index.htm

7. To add a Door to the Map, click the 

button from the Tools menu.

8. Find your desired Doors, then click and drag them onto the Map in their appropriate locations.

9. 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 open door override:

In your configured View, click **Unlock** under the Door you want to unlock.
The door icon next to the Door's name will change from red to green.

Or, if you have a Map with a Door set up in the View, right-click on the Door and select **Unlock**.

Notes:

- A 'Request door 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.
- The Milestone Door will unlock for however many seconds you have specified for **Door unlock time** in the Advanced tab of the Door in CC.

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 (e.g. Closed) in Milestone, its associated alarms are subjected to the same action, and the flooded alarm is also processed in CC. 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 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.

7 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, e.g. 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.

8 Considerations

- Similar to Command Centre's Controlled Challenge functionality, Milestone has access request functionality. **We recommend 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 CC Door can then be overridden from Milestone to allow the Cardholder entry. **However**, issues with this functionally include:
    - CC Zone counting is inaccurate because no CC Cardholder Entry events are generated.
    - CC Evacuation Reports are inaccurate because CC loses track of what Zone Cardholders are in.
    - When a Door is overridden to open, an Access Granted event is not generated in CC, and an Access Denied event is still generated.
    - CC Tagboards show inaccurate information.

- Alarm notes are not shared between CC and Milestone systems. When processing an alarm in CC or Milestone, the alarm is processed in CC, but any specified alarm note is not shared with the other system.