MOTOROLA SOLUTIONS

Safety & Security Ecosystem

Orchestrate Deployment Guide

APRIL 2025

MN007835A01-Y

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end users in EU and UK countries should contact their local equipment supplier representative or service center for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions. To enable faster response time to customer issues, Motorola Solutions provides support from multiple countries around the world.

Service agreement customers should be sure to call the CMSO in all situations listed under Customer Responsibilities in their agreement, such as:

- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN007835A01-R	The following sections were added: • Avigilon Decision Management System–Orchestrate Integration on page 65 • Rave Panic Setup on page 101 The following sections were updated: • Safety and Security Ecosystem Introduction on page 11 • Orchestrate Activation Process on page 13 • Avigilon Unity Cloud Services Setup on page 14 • Troubleshooting on page 106	January 2024
MN007835A01-T	The manual was reorganized: • Removed chapter on Unity Video Alarms Cloud Connector • Consolidated chapter for MOTOTRBO and WAVE PTX • Maintenance considerations moved to specific product chapters The following sections were added: • Capacity Max Voice and Radio Command Gateway on page 78 • Configuring Capacity Max Voice and Radio Command Gateway on page 87 • Rave Alert Setup on page 102 The following sections were updated: • CommandCentral Unit Management on page 73 • MNIS IPSC Configuration Parameters on page 84 • Ally Integration on page 70 • Orchestrate Rules Configuration on page 103	May 2024
MN007835A01-U	The following sections were added: • Email Integration on page 71 • Adding Device Range for MOTOTRBO Radios in a Carrier System Model on page 76 • Adding Talkgroup Range for MOTOTRBO Radios in a Carrier System Model on page 77 • MOTOTRBO Software Version Requirements on page 88 • ASTRO Integration and Configuration on page 95	July 2024

Version	Description	Date
	The following sections were updated: • Safety and Security Ecosystem Introduction on page 11 • Configuring Avigilon Unity Cloud Services Central Station on page 15 • CommandCentral Unit Management on page 73 • Adding WAVE PTX Devices Through Auto Create Unit on page 91 • WAVE PTX Maintenance Considerations on page 94	
MN007835A01-V	Avigilon Decision Management System Prerequisites on page 65 was added. The following sections were updated: • Configuring Orchestrate for Avigilon Decision Management System on page 66 • Configuring Avigilon Decision Management System on page 67 • Ally Integration on page 70	October 2024
MN007835A01-W	The following sections were added: • Changing Your Provider Account on page 18 • Deleting the Unity Cloud Services Site from Orchestrate on page 21 • Configuring Unity Access: Server Version 7_6 and Later on page 23 • Configuring Unity Access: Server Version 7_5 and Earlier on page 25 The following sections were updated: • Avigilon Unity Cloud Services Setup on page 14 • Avigilon Unity Access Setup on page 22 • Unity Access Events as Triggers on page 29	January 2025
MN007835A01-Y	The following sections were updated: • Configuring Emergency Location in Unit Management on page 76 • MNIS Capacity Max Configuration Parameters on page 86	April 2025

Contents

About this Manual

This manual is developed as a support tool for Motorola Solutions employees and channel partners. The chapters within this manual present information on deploying the solution.

Related Information

Go to https://learning.motorolasolutions.com/ to view the current course offerings and technology paths.

For associated information, refer to the following documents:

Related Information	Purpose
Orchestrate Activation Process	Documents process, requirements and responsibilities between customer, channel partner and Motorola.
Avigilon Alarm Gateway and VidProxy Installation and Configuration Guide	Describes ACM and ACC integration.
Avigilon Control Center Alarms Cloud Connector Installation	Describes the installation and configuration process for Cloud Connector.
Motorola Edge Node Installation Guide	This guide is intended for dealers, application providers, and MSI Sales and Solution Integration teams.
Ally Avigilon Orchestrate Integration Setup Instructions	Describes Channel Partner requirements for deploying Ally.
Orchestrate User Guide	Describes creating custom workflows between Avigilon Alarms and MOTOTRBO radios or Ally.
Orchestrate System Planner	Provides information concerning the impact of the solution on pre-sales system planning considerations.
CommandCentral Admin 2.0 Online Help	Provides information on how to use CommandCentral Admin.
Motorola Gateway to LMR Network (MGLN) System Planner	Provides information on the Motorola Edge Node and MGLN mapping solution. It is intended for dealers, application providers, and MSI Sales and Solution Integration teams.
Capacity Max Installation and Configuration Manual	Provides information on MOTOTRBO Capacity Max system installation and configuration procedures.
Orchestrate Activation Checklist	This document describes steps required to configure other products with Orchestrate.
MOTOTRBO to Orchestrate Deployment Guide	This manual is developed as a support tool for Motorola Solutions employees and channel partners. The chapters within this manual present information on deploying MOTOTRBO with the Orchestrate solution.

Chapter 1

Safety and Security Ecosystem Introduction

Safety and Security Ecosystem is Motorola Solutions' modular ecosystem that unifies voice, data, video and analytics on one connected platform.

Orchestrate is a cloud based solution that supports Safety and Security Ecosystem. It provides a customer friendly user interface to create custom workflows. A workflow consists of Triggers which result in one or more Actions. An Orchestrate trigger is an analytic event, an access control event that is configured as an Alarm in the Avigilon Unity Video, an emergency declaration from a MOTOTRBO device or a WAVE PTX device. The Avigilon Unity Access event is configured as an external software event in the Avigilon Unity Video.

The Safety and Security Ecosystem with Orchestrate consists of the following elements:

Triggers

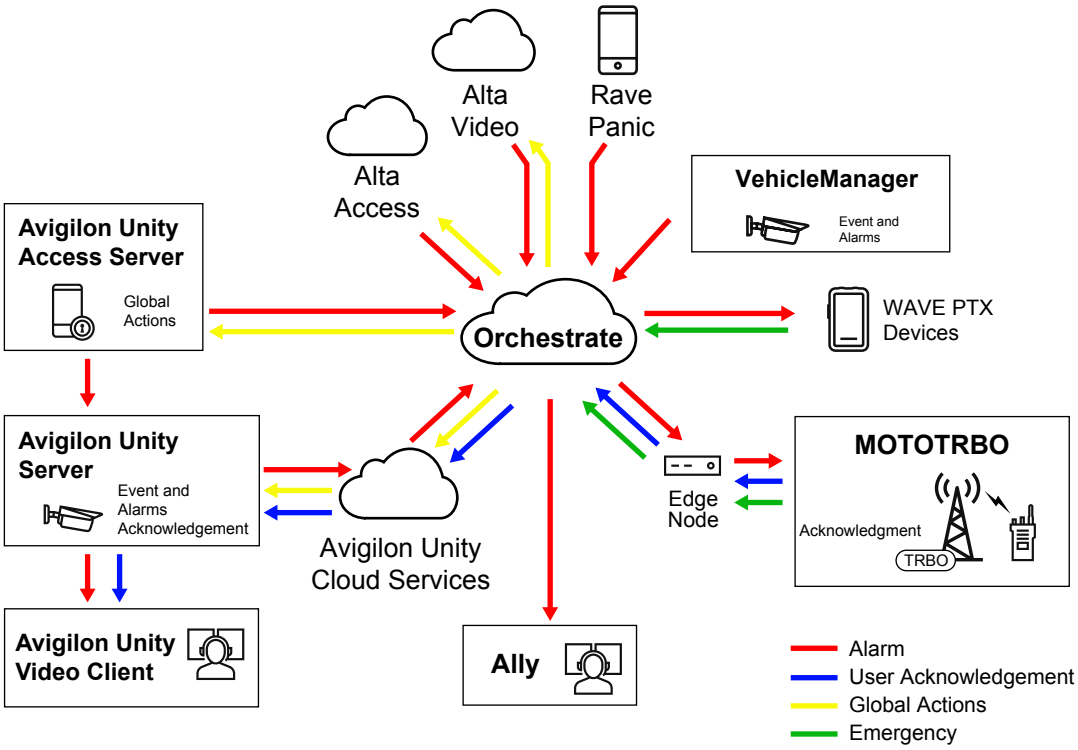
- Avigilon Unity Video Analytics Alarm from Avigilon Unity Video
- Avigilon Unity Video Analytics Alarm from Avigilon Unity Video via Avigilon Unity Cloud Services
- Avigilon Unity Access Events directly from Avigilon Unity Access
- Avigilon Unity Access Events through Avigilon Unity Video

  An Avigilon Unity Video with Avigilon Unity Video/Access integration is required to support Avigilon Unity Access in an Orchestrate deployment.
- Emergency Declaration from a MOTOTRBO radio
- Emergency Declaration from a WAVE PTX device
- Target Alert Service (TAS) LPR Alert from VehicleManager Enterprise
- TAS LPR Alert from VehicleManager Enterprise
- Alta Access Events directly from Alta Access
- Alta Video Events directly from Alta Video
- Rave Panic Alarms

Actions

- Alarm through text message to MOTOTRBO
  - Individual radios
  - Talk Group radios
- Alarm through individual text messages to WAVE PTX devices with text messaging capability
- Alarm to Ally Dispatch window
- Global Action / Action Group for Avigilon Unity Access
- Avigilon Unity Video Alarms triggered by Avigilon Unity Cloud Services Action
- Action for Alta Access
- Action for Alta Video
- Email to CommandCentral Admin users

Figure 1: System Diagram with Message Flow



The customer must provide internet connectivity to Avigilon Unity Cloud Services to facilitate remote support activities to Motorola Solutions. Support activities include connection to Avigilon Unity Cloud Services, and remote assistance when required.

For more information on MOTOTRBO systems, Avigilon systems, WAVE PTX, or Ally, see their respective documentation and training.

NOTE: For convenience, **Avigilon Unity Video** and **Avigilon Unity Access** are further referred to as **Unity (Video)** and **Unity Access**.

Chapter 2

Orchestrate Activation Process

To request an Orchestrate account, submit the following form:

https://docs.google.com/forms/d/e/1FAIpQLSf347lAijL7rFobq74a2YJ_q1TP6JEQ8fKqTO_6bMSG7tvnMw/viewform

NOTE:
This form is for users that do **not** have a Unity Cloud Services account. If you have a Unity Cloud Services account, do not fill out this form – instead, in Unity Cloud Service go to the **Organization Management** and request an Orchestrate account.

Chapter 3

Avigilon Unity Cloud Services Setup

Customers with Avigilon Video and Avigilon Unity Cloud Services can establish a connection with Orchestrate by following a self-registration process.

Self-registration Process in Unity Cloud Services

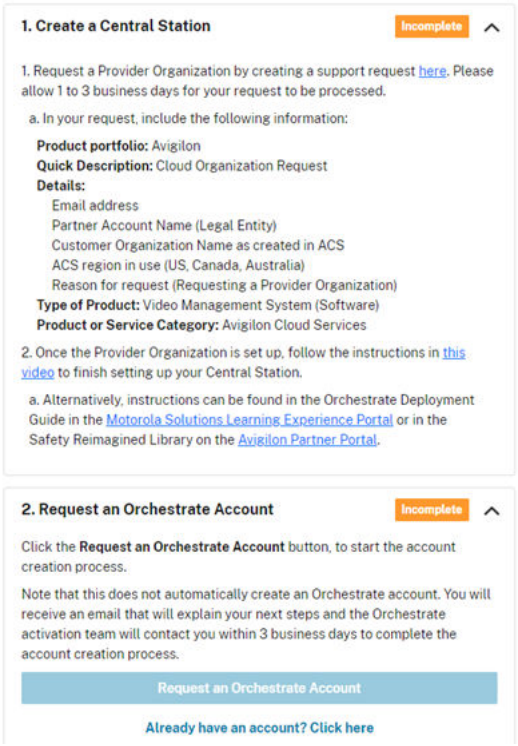
Users must log on to Avigilon Unity Cloud customer organization as **Admin**, then navigate to **Organization Management** → **Orchestrate**.

Integration Requirements

The following conditions must be fulfilled for a successful integration between Avigilon Unity Cloud Services and Orchestrate:

1. You must create a Central Station.
2. You must be signed up for Orchestrate, which means requesting and activating your Orchestrate account.

Figure 2: Unity Cloud–Orchestrate Integration Steps



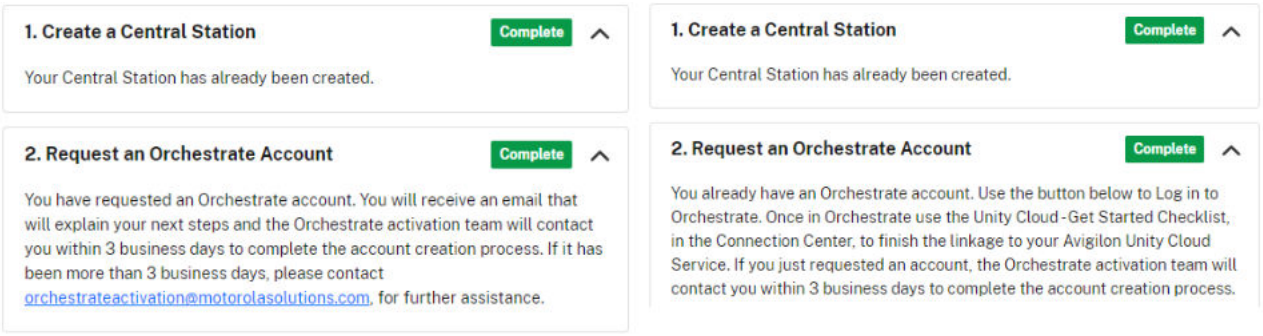
If you already performed any of the required steps, the respective sections are marked as **Complete**.

To finalize the integration, follow the instructions on screen and complete all procedures, until all sections are marked as **Complete**.

When you request an Orchestrate Account to be created, you receive an email explaining the next steps, and the Orchestrate Activation team contacts you within three business days to complete the account creation process.

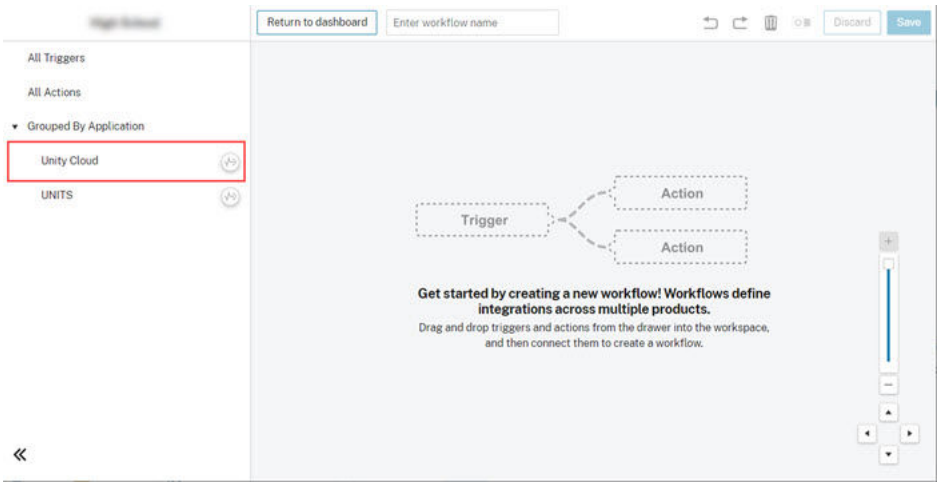
After succesful account creation, you can log on to Orchestrate and finish the linkage to Unity Cloud. The following figure demonstrates the progression of configuration steps.

Figure 3: Completed Unity Cloud Integration Steps: Account Requested vs. Account Created



If your integration is correct, you should see your Unity Cloud Services triggers available in the Orchestrate workflow creation page.

Figure 4: Unity Cloud Triggers in Orchestrate



Alternative Scenario: Self Registration with Orchestrate account already created

Complete the Central Station creation procedure first, then choose the **Already have an account? Click Here** option. You are then navigated to the Orchestrate logon page.

NOTE: If you selected this option accidentally and you do not have an Orchestrate account, refresh the Avigilon tab. The buttons will then reset.

Next, complete the connection, and all steps are recognized as **Complete**.

3.1 Configuring Avigilon Unity Cloud Services Central Station

Prerequisites:

Customers or Channel Partners may register for a Unity Cloud Services account by going to cloud.avigilon.com. This is a self registration process.

1. Select the appropriate region from **USA**, **Canada**, or **Australia**.
2. Follow the on-screen instructions to register the organization name and administrator email address.

The administrator (Customer or Channel Partner) will receive an email with registration information, and then follow the email instructions to continue the registration process, which includes the creation of the account and password.

As part of the ordering process, Motorola Solutions (Avigilon) will provision the Customer or the Channel Partner as a Service Provider organization in Unity Cloud Services.

To request for a Service Provider organization to be created, follow the steps in the *ACS User Guide*, or fill in the following request form.

When the organizations are provisioned by the Customer/Channel Partner and Motorola Solutions, you can proceed to site addition and Orchestrate connection.

Procedure:

Adding Unity Video sites to Unity Cloud Services

1. Log on to Unity Cloud Services as the Customer organization administrator.
2. From the left-hand side navigation bar, select **Organization Management**.
3. In the top-right corner of the screen, click **Add Site**.
4. Fill out the form as appropriate for the Unity Video site.
5. Submit the form.

   The Activation Code appears.
6. Go to the Unity server and navigate to Unity Video setup.
7. Under **Site Setup**, select **Avigilon Cloud Services**.
8. Enter the Activation Code received in step 5 and click **Connect**.

   The Unity Video site is now connected to Unity Cloud Services. For more information, see *ACS User Guide*.

   The next step in the process is to assign permission to access the site to the Service Provider, who will handle the integration with Orchestrate.

   The process requires the customer to be assigned the Orchestrate Service Package. The customer must also grant the Service Provider access to the site. The final steps include the Service provider acknowledging the service request from the customer and provisioning of the integration with Orchestrate.

Obtaining the Orchestrate Service Package

9. Log on to Unity Cloud Services as the Service Provider organization administrator.

   If the administrator is the same as the Customer organization, navigate to the Service Provider organization by selecting **Switch Organization** in the top-right corner, next to the **Login ID**.
10. From the left-hand navigation bar, select **Organization Management**.
11. Select **Customers**.
12. Copy the nine character Customer Invite Code.

    This code can then be provided to the Customer organization administrator to provide access rights to specific Unity Cloud Services sites. In rare cases where the Unity Video Connect package is provided by the Dealer/Provider instead of Avigilon, only the Unity Video Connect Service Package is required.

Assigning access to the site for the Service Provider

13. Log on to Unity Cloud Services as the Customer organization administrator.

    If the administrator is the same as the Service Provider organization, navigate to the Customer organization by selecting **Switch Organization** in the top-right corner, next to the **Login ID**.
14. From the left-hand navigation bar, select **Organization Management**.

15. Under **Sites**, select and click on the Site for which you want to grant access.
16. Select **Service Packages** tab and click **Add Service Packages**.
17. Enter the nine character Customer Invite Code.

    The service provider receives a service request stating that you have requested monitoring of this site through the service package provided.

To acknowledge the Service Request from the Customer, click on the link from the email notification, or navigate directly to Unity Cloud Services and perform the following steps:

18. Log on to Unity Cloud Services as the Service Provider organization administrator.

    If the administrator is the same as the Customer organization, navigate to the Service Provider organization by selecting **Switch Organization** in the top-right corner, next to the **Login ID**.
19. From the left-hand navigation bar, select **Organization Management**.
20. Select the **Customers** tab.
21. Accept any of the pending requests in the tab by clicking **Accept**.

Provisioning the Integration with Orchestrate for the customer

22. Log on to Unity Cloud Services as the Service Provider organization administrator.

    If the administrator is the same as the Customer organization, navigate to the Service Provider organization by selecting **Switch Organization** in the top-right corner, next to the **Login ID**.
23. From the left-hand navigation bar, select **Organization Management**.
24. Select **Monitoring** → **Central Stations**.
25. Click **Add Central Station**.
26. In **Integration Type**, select **Orchestrate**.
27. Select the appropriate **Customer Organization Name**.

    A service account user is automatically created. Typically, there is no need to change the username or password.
28. Click **Save**.
29. Return to the **Central Stations** tab and enable the connection by moving the **Connection** slider.
30. Go to the **Site Configurations** tab.
31. Locate the Customer organization and Site.
32. Assign the **Central Station** to the Site and click **Save**.

    The configuration in Unity Cloud Services is complete. For more information, see *ACS User Guide*.

Postrequisites:

Service Provider/Customer can proceed with the configuration in Orchestrate. To activate the service in Orchestrate, perform the following steps:

1. Log on to Orchestrate Agency as the administrator user.
2. From the left-hand side navigation, select **Connection Center**.
3. Select **Unity Cloud**.
4. Click **Configure**.
5. Follow the instructions on the page.

When required, use the **Customer organization's Administrator** login.

NOTE: If a Provider/Dealer Administrator is setting up for the customer, ensure that the Administrator is also explicitly added to the Customer Organization as an administrator.

6. Upon login, select the **Customer Organization**.
7. Enter the Service Activation Code – it is the same nine character code used for Unity Cloud service packages.

   Either the **ACC Connect** or the **Remote Monitoring** Packages may be used for Orchestrate Connection.
8. Click **Connect**.

   Orchestrate finalizes the connection with Unity Cloud Services.

When that configuration is finished, the setup to connect Unity Video to Orchestrate through Unity Cloud Services is completed. Unity Video Alarms will now show up as Triggers within Orchestrate for the Agency registered.

3.2 Changing Your Provider Account

Procedure:

1. Delete your current Central Station by performing the following actions:
   a. In the Orchestrate **Connection Center**, in the Unity Cloud **Configure** page, disconnect the Unity Cloud Services.
   b. Wait until all the capabilities (that is Unity Cloud Triggers and Actions) are deleted in the workflow page.
   c. In the previous provider account, unassign the Orchestrate central station from the sites.
   d. Delete the Orchestrate Central Station.
   e. Delete the provider account from the sites in the Unity Cloud organization.
2. Proceed with the new provider.

3.3 Avigilon Unity Cloud Services Network Requirements

Unity Cloud Services require the Unity server to have Internet access, and to be able to reach the Unity Cloud Services platform (regional based).

Port Requirements

Unity Cloud Services require the following ports to be open to the Public Internet:

- Port 443 – TCP through SSL or HTTPS (Unity Cloud Services WebUI, Device Connection)
- Port 1025-65535 – TCP through STUN (Video streaming)
- Port 3478 or 443 – UDP or TCP through TURN (Video Streaming)

Bandwidth Requirements

For use with Orchestrate, the bandwidth requirement will be minimal, as the data transmitted are IoT Event messages, which are highly efficient. If a video stream is requested as part of normal Unity Cloud Services use, bandwidth will change depending on the camera stream. For example, a 3MP camera running at six fps requires 1–3 Mbps (depending on video quality).

3.4
Avigilon Unity Cloud Services: Multi Unity Server Site Configuration

Unity Cloud Services manage Unity Video as Sites. Clustered Unity servers are managed as a Site in Unity Cloud Services. Unity Cloud Services do not have the ability to manage individual servers within that site.

3.5
Migrating from Unity Video Cloud Connector to Unity Cloud Services Connector

NOTE: Unity Video Cloud Connector must be off at all times when a Unity Cloud Services Connector is in use.

To migrate from a Unity Video Cloud Connector to a Unity Cloud Services Connector, perform the following steps:

Procedure:

1. Shutdown the Unity Video Cloud Connector (confirm shutdown from the Virtual Machine).
2. Connect Unity Video site to Unity Cloud Services through a Customer Organization (if not completed already).
3. Set up a Service Provider Organization for the Customer Organization (if not completed already).
4. Follow the steps to set up and activate Unity Cloud Services connection to Orchestrate.

   When the setup is complete and Alarms are ingested into Orchestrate, the **Unity Cloud** folder displays (at the same level as Unity Video).
5. Pause all Unity Video workflows.
6. Migrate the Unity Video workflows by creating **new** workflows based on Unity Cloud Services alarms as triggers.
7. Confirm that Unity Cloud Services workflow is working and proceed with removal (or pausing) of Unity Video workflows.

3.6
Configuring Unity Cloud Services Actions

Unity Cloud Services Actions can be configured to trigger a Unity Video Alarm. When the Unity Video Alarm is triggered, the user can view the triggered alarm within the Unity Client. For alarm configuration guidelines, refer to the Unity Video documentation. For Unity Cloud Services Actions, it is recommended to use an External Software Event alarm.

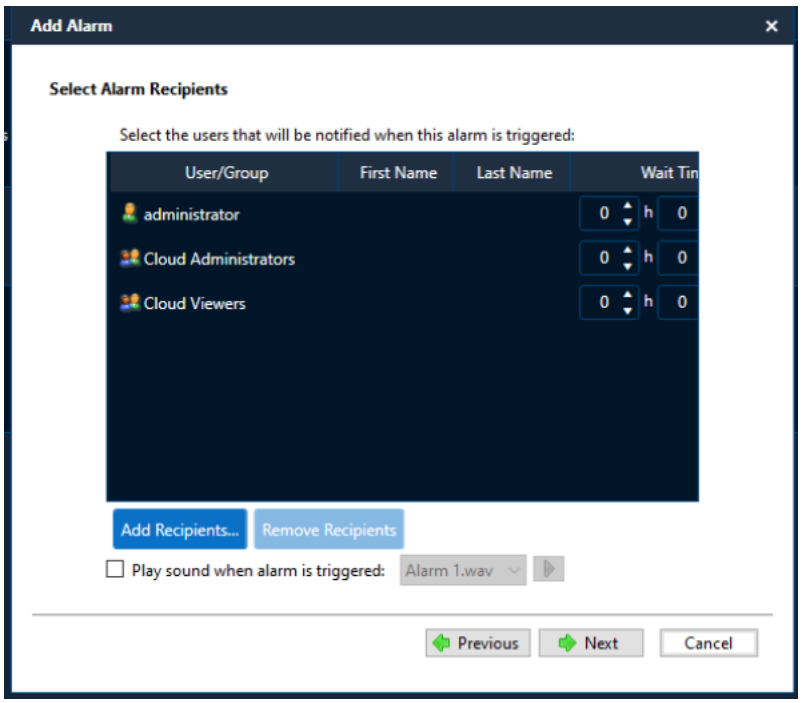
NOTE:
Unity Cloud Services actions can only be triggered by Unity Video alarms through Unity Cloud Services or Unity Access events. Unity Video alarms through the Unity Video Cloud Connector are not supported.

Unity Cloud Services actions are marked as completed when the command is executed on Unity Video. If Unity Video encounters any failure on raising the alarm, the failure is **not** signaled back to Orchestrate.

Multiple Action requests to the same Unity servers may experience timeout because the load will place stress on the Unity server.

Unity Video alarms must be configured with the Unity Cloud Services associated **Alarm Recipients** to allow the Alarm to be raised through Unity Cloud Services. For alarms designated as Unity Cloud Services Actions, ensure that the **Cloud Administrators** is one of the alarm recipients.

Figure 5: Selecting Alarm Recipients



To configure Unity Video Alarms as Unity Cloud Services Actions in Orchestrate, perform the following steps:

Procedure:

1. Log on to the Orchestrate Agency as the administrator user.
2. From the left-hand side navigation, select **Connection Center**.
3. Select **Unity Cloud**.
4. Click **Configure**.
5. Follow the instructions on the page.

   When required, use the **Customer organization's Administrator** login.

   NOTE: If a Provider/Dealer Administrator is setting up for the customer, ensure that the Administrator is also explicitly added to the Customer Organization as an administrator.
6. Upon logon, select the **Customer Organization**.
7. Select the **Alarm** tab.
8. Select the alarm desired as an action and move it to the Action list on the right side by clicking the right-facing arrow.
9. To finalize the alarm list, click **Save**.

   NOTE: When an alarm is chosen as an Action, it is no longer available as a Trigger. Orchestrate will reflect this change after a refresh window of approximately 5–10 minutes.

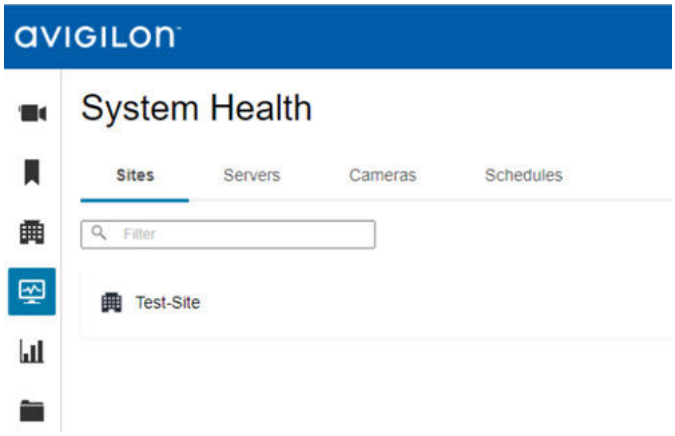
3.7

Unity Video/Unity Cloud Services Troubleshooting

Unity Cloud Services connection with Unity Video can be verified by using the Health Monitoring feature available in Unity Cloud Services.

Navigate to **System Health** and verify the status of the servers and cameras.

Figure 6: Avigilon System Health Tab



Next, you may also check the status of cameras by selecting **View tab** to live stream at least one of the cameras.

If you are still encountering issues, proceed to the Unity client and retrieve a System Bug Report. The system bug report can be accessed in the following way:

1. Log on to the Unity server.
2. In the top-right corner of the Unity Client select **Settings**.
3. Navigate to **System Bug Report**.
4. Select a download location and wait for the download to complete.

Send the file to the appropriate Motorola Solutions support team for resolution.

3.8

Deleting the Unity Cloud Services Site from Orchestrate

IMPORTANT: Performing the following steps in a wrong order may result in Orchestrate disruption.

Procedure:

1. In the Orchestrate **Connection Center**, in the Unity Cloud **Configure** page, disconnect the Unity Cloud Services.
2. Wait until all the capabilities (that is Unity Cloud Triggers and Actions) are deleted in the workflow page.
3. In Unity Video or the Unity client, disconnect the Unity Cloud Services site.
4. Remove the site from Unity Cloud Services.
5. Reconnect the Unity Cloud Services with Orchestrate again.

Chapter 4

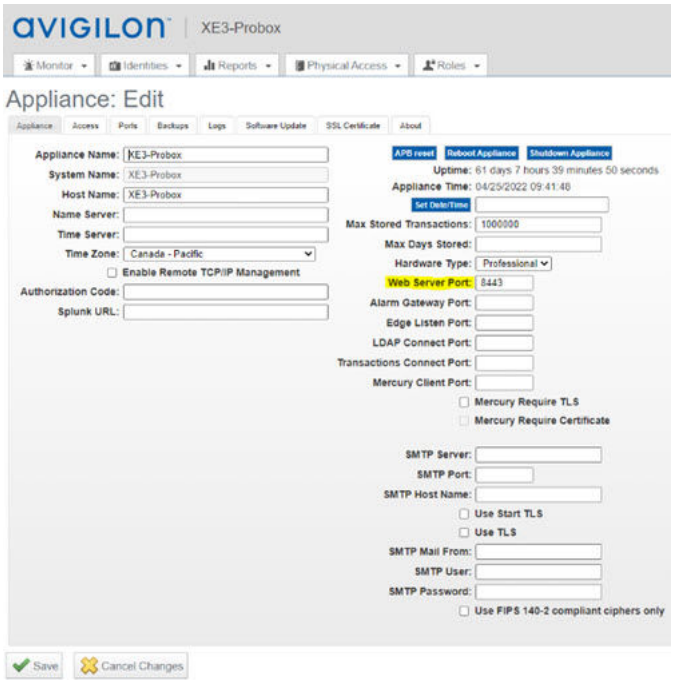
Avigilon Unity Access Setup

Unity Access support for triggers through Events/Alarms is done through either a direct connection with the Unity Access servers or through Unity Video/Unity Access Unification. The following setup steps are for the configuration of Unity Access as actions through Unity Access Global Actions. The steps to configure Unity Access for global action also enable the direct trigger support.

As part of the onboarding, Motorola Solutions provisions the Customer Agency with the required configuration to use the Orchestrate Configuration UI and Unity Access Connector. When the provisioning is completed, the Channel Partner or Customer may directly configure Unity Access for Orchestrate within the Unity Access and Orchestrate Configuration UI.

In Unity Access, navigate to the **Appliance** settings page. Configure the **Web Server Port** to the desired port value and note to use this port for all eventual network mapping configurations. The Web Server Port is used by the REST API interface.

Figure 7: Avigilon Appliance Page



In Orchestrate, your actions depend on your Unity Access server version.

For server version 7.6 and later, refer to Configuring Unity Access: Server Version 7_6 and Later on page 23.

For server version 7.5 and earlier, refer to Configuring Unity Access: Server Version 7_5 and Earlier on page 25.

For information on how to upgrade your server, refer to Unity Access documentation. For further assistance, contact the Orchestrate support team.

IMPORTANT:
The identity used to connect Unity Access to Orchestrate must be a specific Orchestrate user.

To avoid interruption of service, all password changes performed in the Unity Access server must be also replicated in Orchestrate in less than 10 minutes.

Every 10 minutes Orchestrate tries to reestablish the connection to Unity Access. When Orchestrate tries to connect with the wrong password multiple times, Unity Access interprets such connection attempts as a threat, and locks the account.

In such case, users can ask the agency admin to unlock their accounts and reset their passwords.

If the agency admin is not available, a new Orchestrate user account can be created.

4.1
Configuring Unity Access: Server Version 7_6 and Later

When using Unity Access server version 7.6 and later, you are using the new Unity Access connector.

IMPORTANT: All customer servers must be connected by using the same connector.

Procedure:

1. In Orchestrate, from the left-hand side navigation, select **Connection Center**.

   The Connection Center supports multiple products.
2. Select **Unity Access**, then click **Configure**.
3. At the top of the screen, select **Server version 7.6 or above**.
4. Select the **Servers** tab.
5. Select **Add Server**,

   Other available options include the **Delete** button which allows users to delete a configured Unity Access server, or the **Edit** button which allows users to edit existing configurations. The **Refresh** button allows you to manually trigger a refresh of the list at any time.
6. In the **Add Server** dialog box, configure the Unity Access server connection.

Figure 8: Add Server Dialog Box

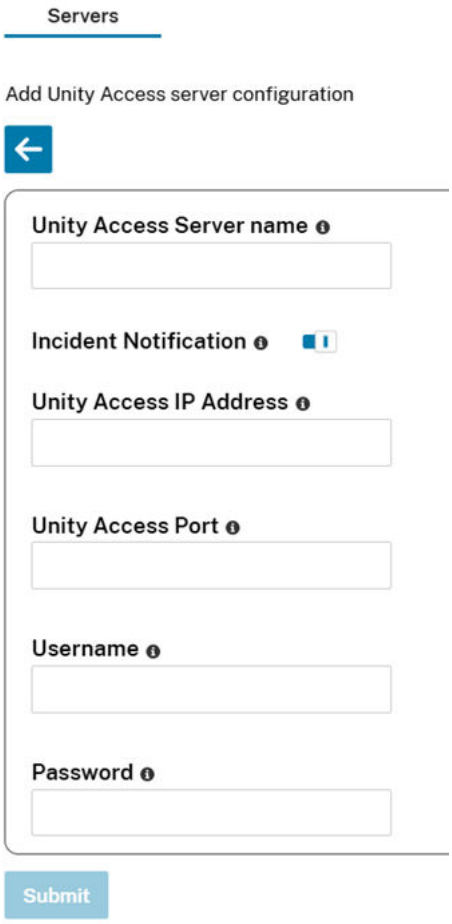


Table 1: Add Server Fields Description

Field Name	Description
Unity Access Server name	Name given to identify the Unity Access server. The context of the name is only relevant in Orchestrate and will be unique.
Incident Notification	Use this toggle to enable/disable Incident notifications.
Unity Access IP Address	The external facing IP address. This IP address should be the WAN facing IP provided by the Internet Service Provider for which the Unity Access server is connected to.
Unity Access Port	The REST interface TCP port. Depending on the network configuration, this port may be the same as the one configured in the Unity Access UI (if no port mapping is configured). If port mapping is configured (due to security/firewall), consult your network service pro-

Field Name	Description
	vider. The configured port should be the port that is externally available to the Internet.
Username	REST API user name.
Password	REST API user password.

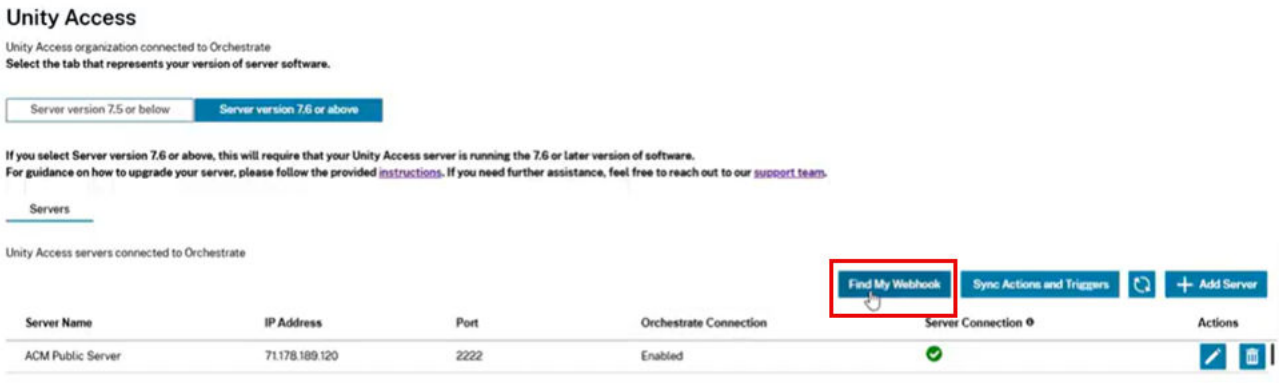
7. When the configuration is complete, store the values and complete the configuration by clicking **Submit**.

   Webhook Information dialog box displays.

8. Copy the **Webhook URL** for further configuration in Unity Access.
9. In Unity Access, in **Global Actions**, create a **Webhook** type Action and click it.
10. In **API URL**, paste the **Webhook URL** value copied from Orchestrate.

    If you do not have the values copied, you can retrieve it in Orchestrate in the Unity Access configuration screen by selecting **Find My Webhook**.

    Figure 9: Finding Unity Access Webhook



   The **Username** and **Password** values are also available there.

11. In **User Name**, paste the **Username** value copied from Orchestrate.
12. In **Password**, paste the **Password** value copied from Orchestrate, then click **Save**.

    For more information, refer to the ACS User Guide.

4.2 Configuring Unity Access: Server Version 7_5 and Earlier

When using Unity Access server version 7.5 and earlier, you are using the legacy Unity Access connector.

IMPORTANT: All customer servers must be connected by using the same connector.

Procedure:

1. In Orchestrate, from the left-hand side navigation, select **Connection Center**.

   The Connection Center supports multiple products.

2. Select **Unity Access**, then click **Configure**.
3. At the top of the screen, select **Server version 7.5 or below**.
4. Select the **Servers** tab.
5. Select **Add Server**,

   Other available options include the **Delete** button which allows users to delete a configured Unity Access server, or the **Edit** button which allows users to edit existing configurations. The **Refresh** button allows you to manually trigger a refresh of the list at any time.
6. In the **Add Server** dialog box, configure the Unity Access server connection.

Figure 10: Add Server Dialog Box

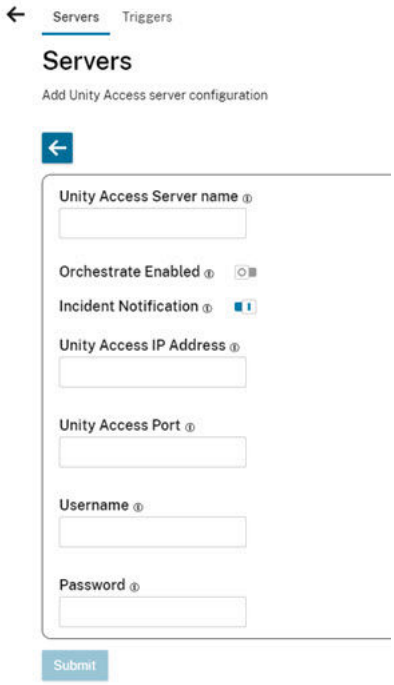


Table 2: Add Server Fields Description

Field Name	Description
Unity Access Server name	Name given to identify the Unity Access server. The context of the name is only relevant in Orchestrate and will be unique.
Orchestrate Enabled	By default, this is always **ON** for creation. When Editing, the user may turn this **OFF** to disable the discovery of Global Actions to Orchestrate. This configuration will **not** remove the Actions from Orchestrate.
Incident Notification	Use this toggle to enable/disable Incident notifications.
Unity Access IP Address	The external facing IP address.

Field Name	Description
	This IP address should be the WAN facing IP provided by the Internet Service Provider for which the Unity Access server is connected to.
Unity Access Port	The REST interface TCP port. Depending on the network configuration, this port may be the same as the one configured in the Unity Access UI (if no port mapping is configured). If port mapping is configured (due to security/firewall), consult your network service provider. The configured port should be the port that is externally available to the Internet.
Username	REST API user name.
Password	REST API user password.

7. When the configuration is complete, store the values and complete the configuration by clicking **Submit**.

   NOTE: There may be up to a five minutes delay before the Unity Access Global Actions are discovered into Orchestrate.

   For more information, refer to the ACS User Guide.

4.3 Unity Access Network Requirements

Unity Access connection to Orchestrate requires an Internet connection through an HTTPS port with a public facing IP address. Unity Access network configuration can be done by the Unity Access UI.

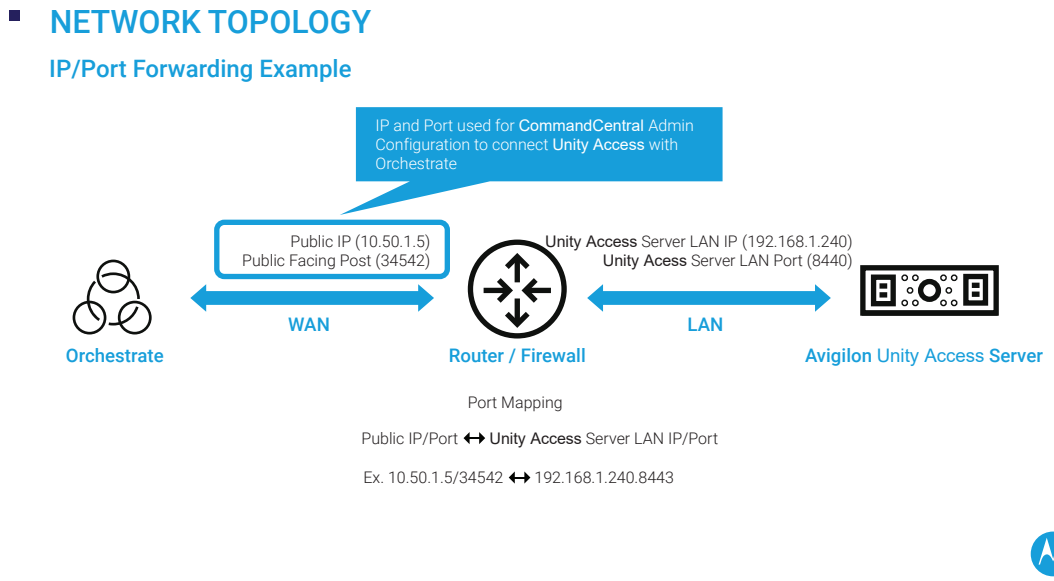
In some network scenarios, the Unity Access site may be behind firewalls or reverse NAT configurations. As a result, partners or customers may be required to put special routes or punch holes in the firewall for the Unity Access server to reach the Internet.

(Optional) Setup Information Using FQDN Filtering

Domain Allow List:

- US names:
  - http://orchestrate-acm.commandcentral.com
  - http://egress.ent.commandcentral.com
- CA names:
  - http://orchestrate-acm.commandcentral.ca
  - http://egress.ent.commandcentral.ca

Figure 11: Port Forwarding Example



4.4 Unity Access: Multi Server Configuration

Multiple Unity Access servers are supported for a single Customer Agency. This may be configured in the Connection Center in the **Unity Access** → **Configure** → **Servers** tab.

NOTE: Unity Access servers configured in Failover or Replication modes are not supported.

For more information, see *Orchestrate System Planner*.

4.5 Global Actions and Global Action Group

Global Actions are configured within Unity Access and they may be linked to a variety of action types, such as Door Grants, Panel Macros, and others. When a Unity Access server is connected to Orchestrate, any additional Global Actions are discovered into Orchestrate within a five minutes window. Global Actions may be removed from Unity Access, which subsequently triggers a removal from Orchestrate.

In addition, there is a special type of Global Action called Action Group, which is a collection of other Global Actions. Individual actions within the Global Actions are not discovered.

Unity Access Global Actions processing depends on the Unity Access server performance. To ensure stable deployment, limit the total number of actions in Unity Access to 50, and the number of concurrent Global Action triggering to five.

NOTE: Unity Access actions can only be triggered by Unity Video alarms through Unity Cloud Services. Unity Video alarms through the Unity Video Cloud Connector are not supported.

4.6
Unity Access Events as Triggers

NOTE: This section is only applicable for customers with Unity Access version 7.5 and earlier.

Unity Access Events can also be configured as triggers in Orchestrate. The list of Event Types supported is the same as the list supported for Unity Video/Unity Access Unification. The functionality enables customers who may not have Unity Video to take advantage of Unity Access Event triggering in Orchestrate.

No additional configuration is required for this feature (if you are already configured for Unity Access action).

4.6.1
Creating Unity Access Triggers

Procedure:

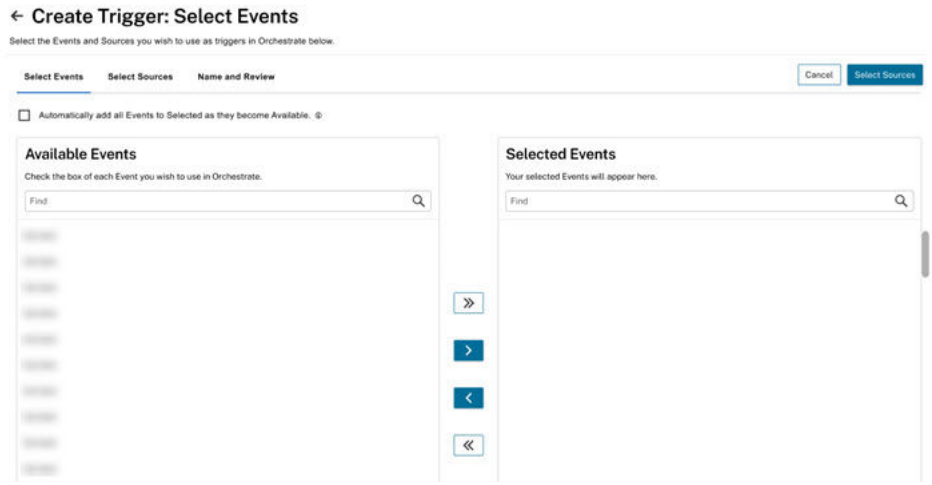
1. Log on to the Orchestrate Agency as the administrator user.
2. From the left-hand side navigation, select **Connection Center**.
3. Select **Unity Access**.
4. Click **Configure**.
5. Select **Triggers**.

   Figure 12: Unity Access Triggers Page

6. In the top-right corner of the page, select **Create Trigger**.

   Create Trigger page appears. In this page you can configure Events and Sources for your trigger, then verify and save it for your agency.

Figure 13: Trigger Creation: Selecting Events



NOTE: The **Automatically add all Events...** check box is unselected by default. If the check box is selected, all Events added in the future are automatically added to the currently edited trigger, so that you do not have to make manual updates.

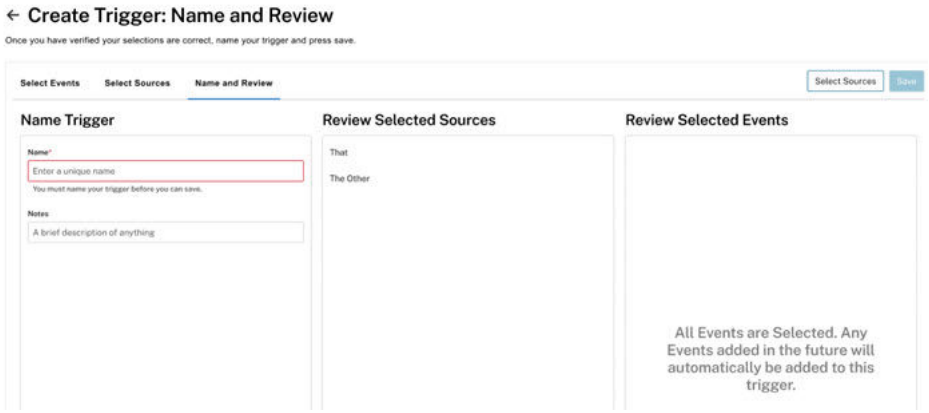
7. From the **Event List**, select the desired events and click the right-facing arrow to add them to the trigger.
8. If you want to remove any of the added events from the trigger, under **Selected Events** select the desired items and click the left-facing arrow.
9. In the top-right corner of the page, click **Select Sources**.

   The **Select Sources** page appears.

   NOTE: The **Automatically add all Sources...** check box is unselected by default. If the check box is selected, all Sources added in the future are automatically added to the currently edited trigger, so that you do not have to make manual updates.
10. From the **Sources List**, select the desired sources and click the right-facing arrow to add them to the trigger.
11. If you want to remove any of the added sources from the trigger, under **Selected Sources** select the desired items and click the left-facing arrow.
12. In the top-right corner of the page, click **Name and Review**.
13. In the **Name and Review** page, fill in the **Name** of the trigger (required) and **Notes** about the trigger (optional).

    In case of any naming errors, an error message displays under the **Name** field.
14. Review the added Events and Sources.

Figure 14: Trigger Creation: Name and Review



If you want to make any changes to the list of added Events and Sources, you must navigate to respective sections by selecting tabs, or by using the button in the top-right corner.

15. In the top-right corner, click **Save**.

    If the trigger creation is succesful, a green toast message appears at the top of the page.

4.6.2

Managing Unity Access Triggers

Procedure:

1. To edit an existing trigger, in the **Triggers** page, next to the desired trigger click **Edit**.

   The **Create Trigger** page appears. Edit your trigger as described in Creating Unity Access Triggers on page 29, then save your updates.

2. To delete an existing trigger, in the **Triggers** page, next to the desired trigger click **Delete**, then confirm when prompted.

   IMPORTANT: This action cannot be undone.

3. To copy an existing trigger, in the **Triggers** page, next to the desired trigger click **Copy**.

   You are navigated to the **Name and Review** page of the trigger. The name of the trigger is appended with `Copy`. You can rename the copied trigger according to your needs, and edit the notes, events, and sources assignments. When ready, save your copied trigger.

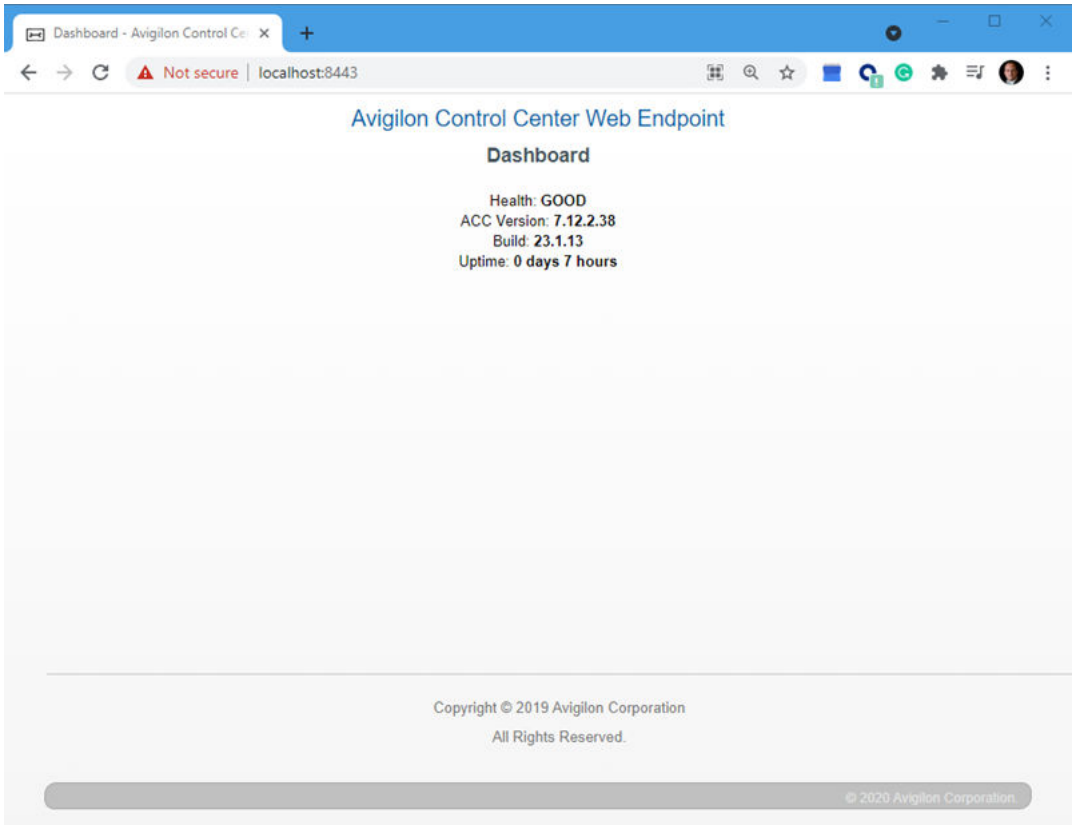
Chapter 5

Unity Video and Unity Access Unification

5.1 Unity Video Web End Point (WEP) Service

In order to get Alarms to flow through the Cloud Connector to the Cloud, the Unity Video's WEP Service must be installed and running. When the WEP Service is running, it can be verified by using a web browser and navigating to `http://<Unity Video Server IP>:8443/` and ensuring that the following is displayed.

Figure 15: WEP Service Enabled



5.2 Unity Video Licenses

For Alarms to be configured, the Unity Video must contain at least one Unity Video 7 Enterprise license. Some video analytics require additional licenses.

5.3 Unification

If access control is part of the deployment, then the Unity Access appliance can be connected to the Unity server, such that Unity Access events flow to Orchestrate through the Unity server. This integration between the Unity Access appliance and the Unity server is done through Unification.

Unity Access appliance (v5.10.10) and Unity server (v7.6) Unification supports the following events:

- ACCESS_CONTROL_DOOR_ACCESS_DENIED
- ACCESS_CONTROL_DOOR_ACCESS_GRANTED
- ACCESS_CONTROL_DOOR_FORCED
- ACCESS_CONTROL_DURESS
- ACCESS_CONTROL_REX
- ACCESS_CONTROL_DOOR_HELD_OPEN
- ACCESS_CONTROL_DOOR_OPENED
- ACCESS_CONTROL_DOOR_CLOSED
- ACCESS_CONTROL_CONNECTED
- ACCESS_CONTROL_DISCONNECTED
- ACCESS_CONTROL_DOOR_FORCED_NORMAL
- ACCESS_CONTROL_DOOR_HELD_OPEN_NORMAL
- ACCESS_CONTROL_CERT_VALIDATION_FAILED
- ACCESS_CONTROL_NEW_CERT_TRUSTED
- ACCESS_CONTROL_EVENT_SERVICE_OFFLINE
- ACCESS_CONTROL_EVENT_SERVICE_RESTORED
- ACCESS_CONTROL_INPUT_ACTIVATED
- ACCESS_CONTROL_INPUT_DEACTIVATED
- ACCESS_CONTROL_INPUT_IN_ERROR
- ACCESS_CONTROL_INPUT_NOT_IN_ERROR
- ACCESS_CONTROL_UNSUPPORTED_FEATURE

To enable the Unification, perform the steps in Connecting the ACM Appliance to an ACC Site.

5.4 Unity Video Heartbeat Alarm

Deployments may have infrequent Unity Video Alarms, and they may not have personal monitoring video in a control center setting. For these types of deployments, it is recommended to incorporate a Unity Video Heartbeat into the solution to help detect system failures, so that they can be addressed in a timely manner.

When loaded on a Unity Server, the AlarmTriggerApp supports the ability to trigger a Unity Video Alarm based on a software event. This in combination with a scheduled Windows Task produces a periodic Heartbeat Alarm to Orchestrate. In Orchestrate a view of the last received Unity Video Alarm time is visible in the side tray. This can be used to verify Unity Video Alarms are being sent and accepted in the cloud. Additionally, the Orchestrate product threshold for Unity Video or Unity Cloud Services can be set to two or three times the heartbeat rate. The failure to receive any Unity Video Alarm during the threshold period triggers an email to the email address associated with the customer.

5.4.1 Enabling the Unity Video Heartbeat Alarm

Procedure:

1. Obtain the Orchestrate Alarm Trigger Application from Motorola My View.

   It is located under MOTOTRBO Data and System Tools.

2. Copy the Orchestrate Alarm Trigger Application onto the Unity Server and extract the contents to a folder on the system.

   In the following steps, the following filepath is assumed: `C:\AlarmTriggerApp`

3. Configure the Heartbeat Alarm on the Unity Server.

   NOTE:
   This step consists of three substeps:

   a. Creating a low-privileged user account that the AlarmTriggerApp will use to trigger the alarm.

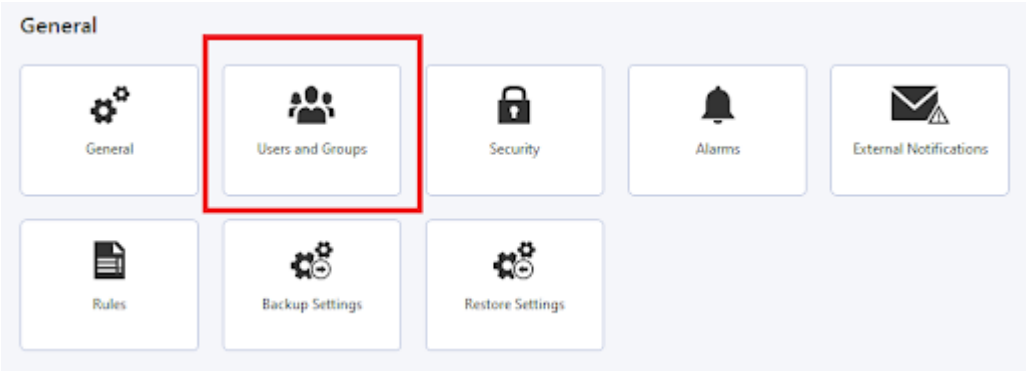
      The AlarmTriggerApp requires a user account and a password to make API calls to the system. For security reasons, it is best practice to create a user with the minimum privileges necessary to trigger the alarm.

   b. Configurating an alarm.

   c. Configurating the rule to trigger the alarm.

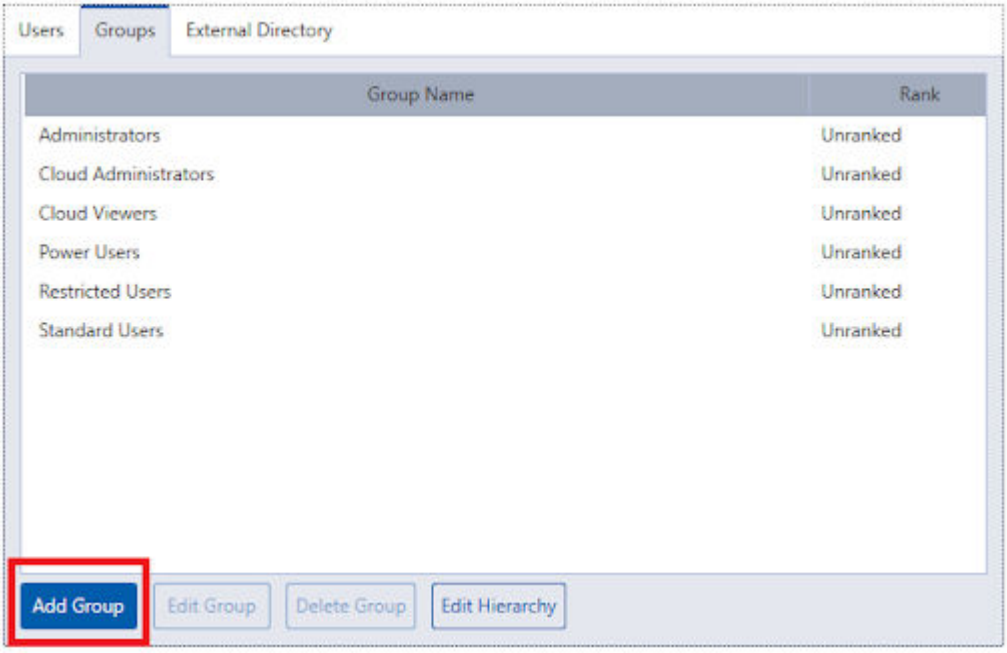
   a. **Create A Low Privileged User Account**: Under **Site Setup** → **General**, go to **Users and Groups** settings

   Figure 16: General Settings



In the **Groups** tab, select **Add Group**.

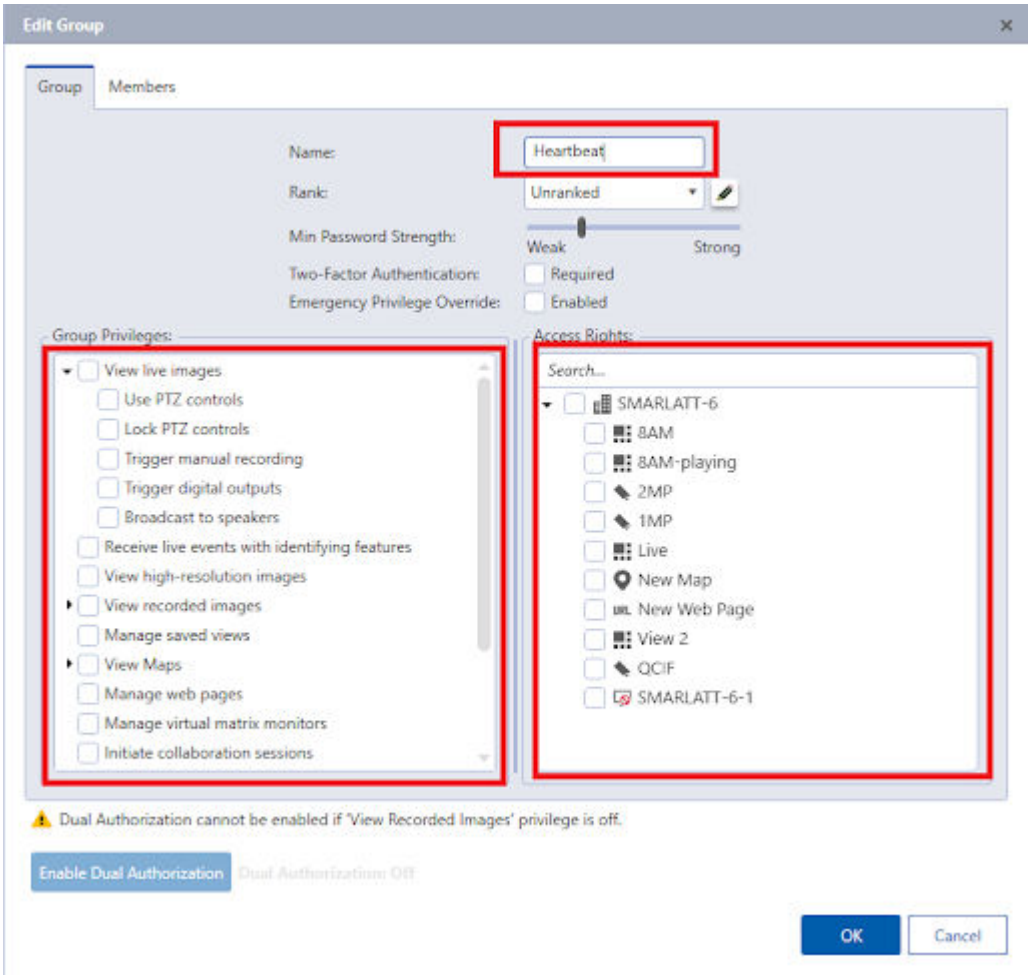
Figure 17: Groups Tab



Copy permissions from any group.

Name the group **Heartbeat**, and uncheck all **Group Privileges** and **Access Rights**.

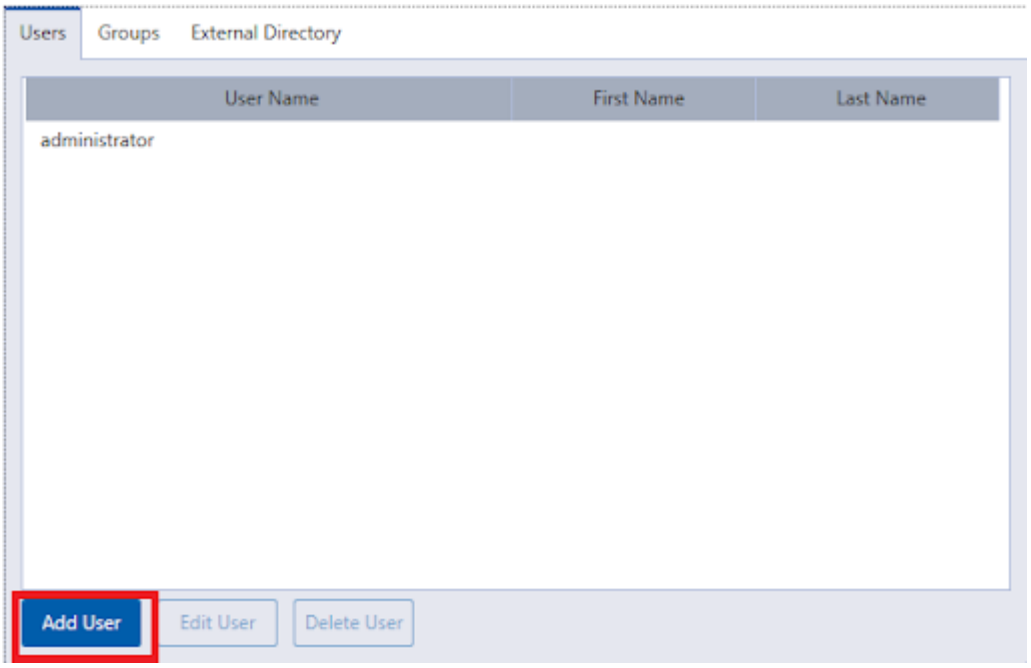
Figure 18: Heartbeat Group Parameters



Add the group by clicking **OK**.

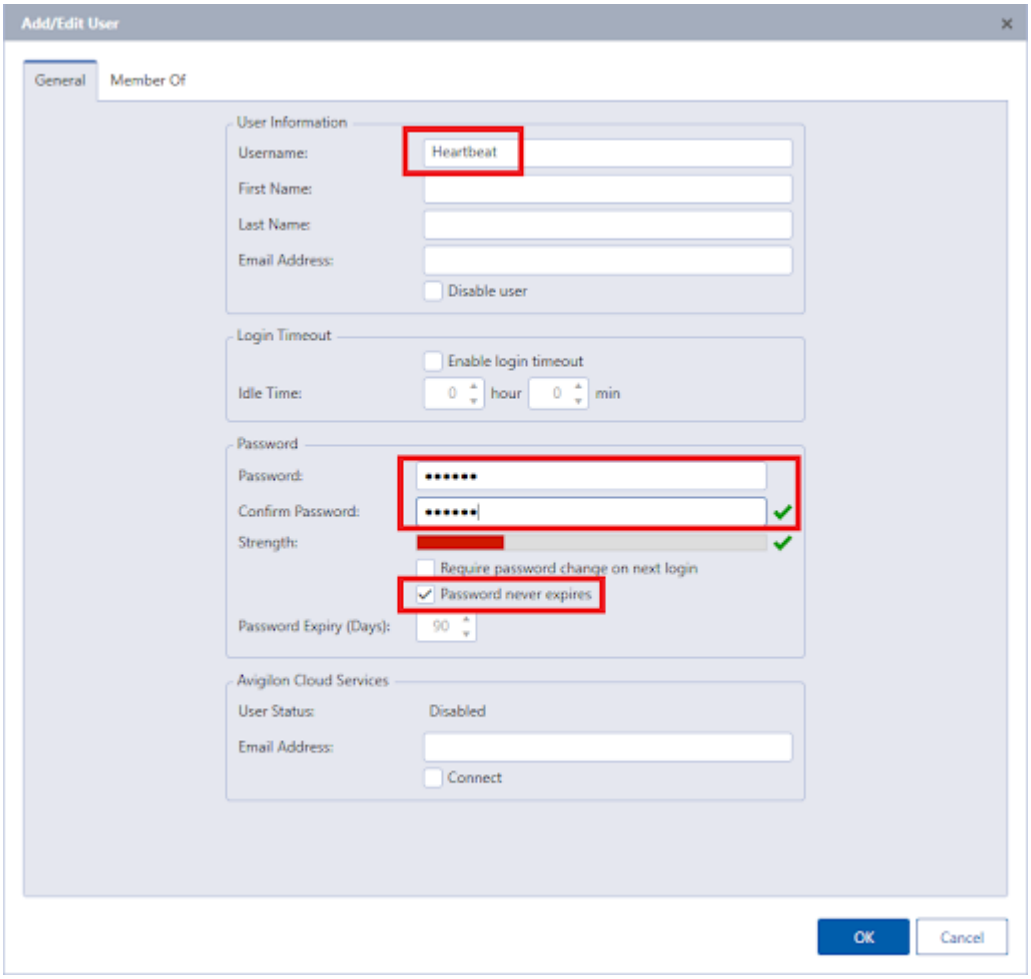
Next, go to the **Users** tab and select **Add User**.

Figure 19: Users Tab



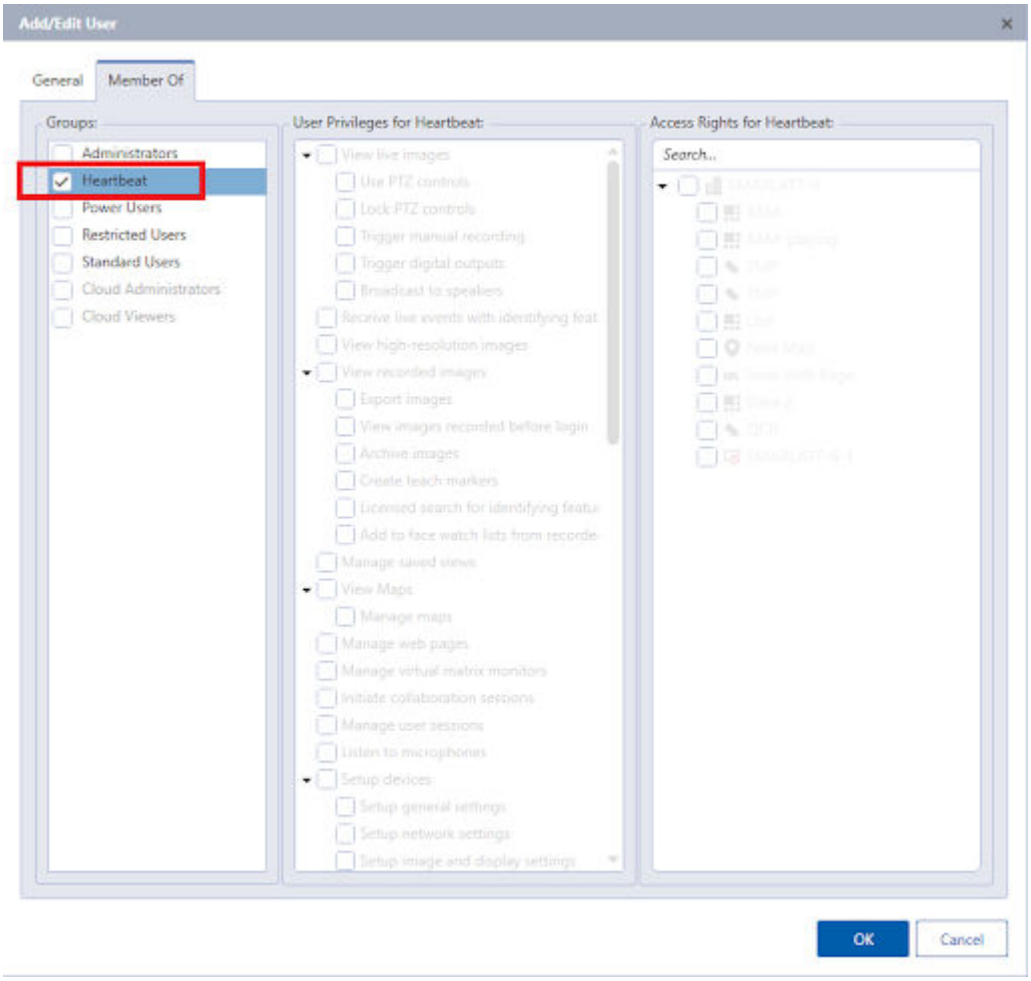
Name the user **Heartbeat**, set the password that will be used by the heartbeat app, and set the password to **Password never expires**.

Figure 20: Heartbeat User Parameters



Go to the **Member Of** tab and select the **Heartbeat** group.

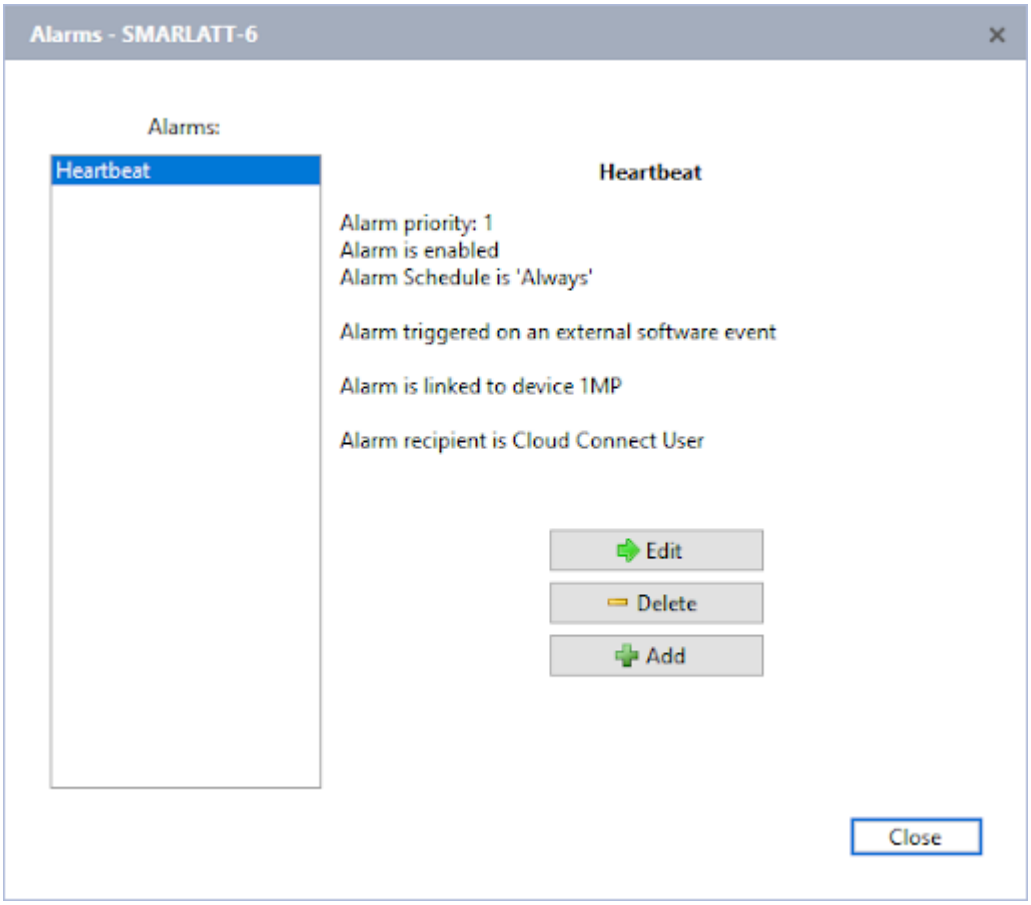
Figure 21: Adding User to a Group



To add the new user account, click **OK**.

b. **Configure the Alarm**: Under **Site Setup** → **General**, open the alarms configuration page and add an alarm called `Heartbeat` with the following configuration:

Figure 22: Heartbeat Alarm Configuration

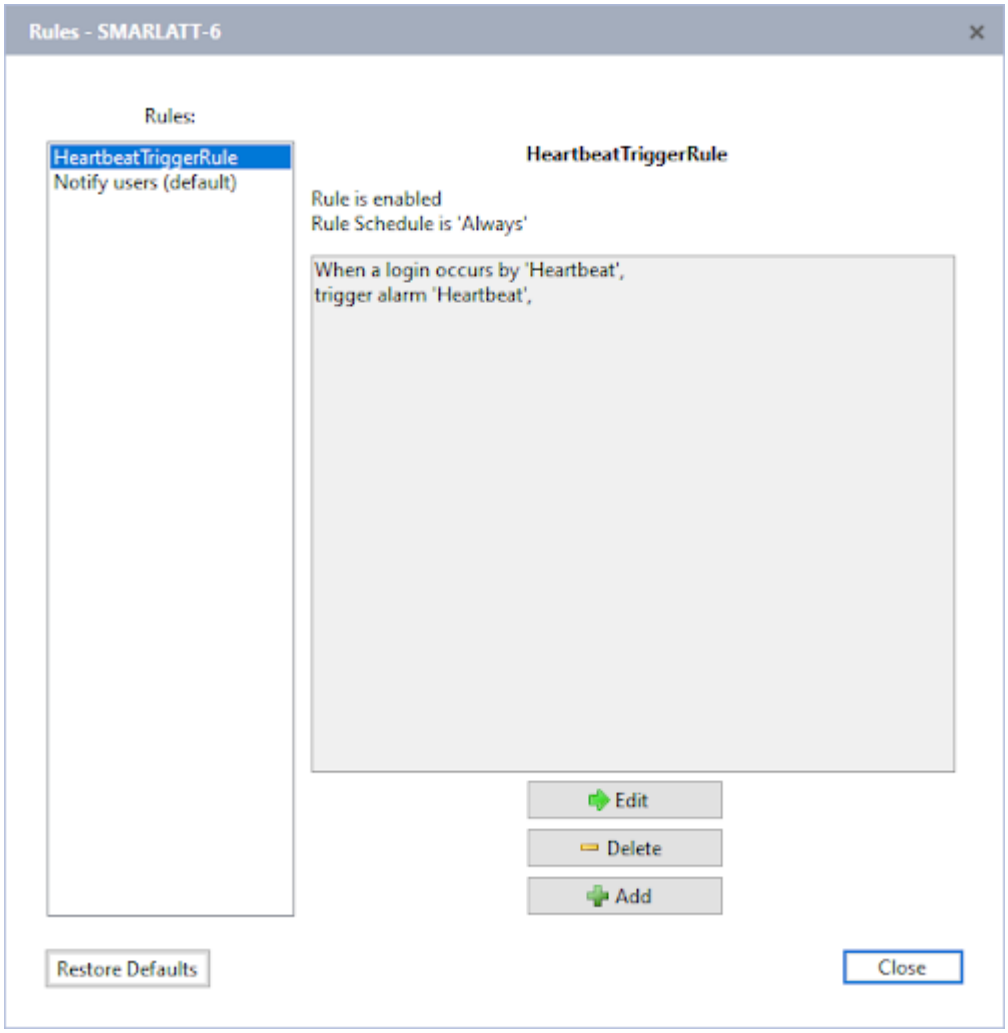


Important Parameters:

- Alarm Schedule is **Always**,
- Alarm is triggered on an external software event,
- Alarm recipient is Cloud Connector User (OrchestrateConnection),
- The linked device is irrelevant.

c. **Configure the rule to trigger the Alarm**: Under **Site Setup** → **General**, open the rules setup dialog box and add a new rule with the following configuration:

Figure 23: Rules Dialog Box



The trigger event is a login by user: **Heartbeat**

The rule-action is to trigger the alarm: **Heartbeat**

The rule should be **enabled** and scheduled to **Always** run.

4. Determine the desired heartbeat interval.

   The recommended value is 60 minutes for a Unity Video site with only one Unity Server.

5. To create a repetitive trigger, configure Windows Task Scheduler to the task at the desired heartbeat interval.

   By default, ACCTriggerApp produces a single trigger, and then exits.

   Step example:

   A configuration for a heartbeat Alarm every one hour:

Figure 24: AlarmHeartbeat Properties – General

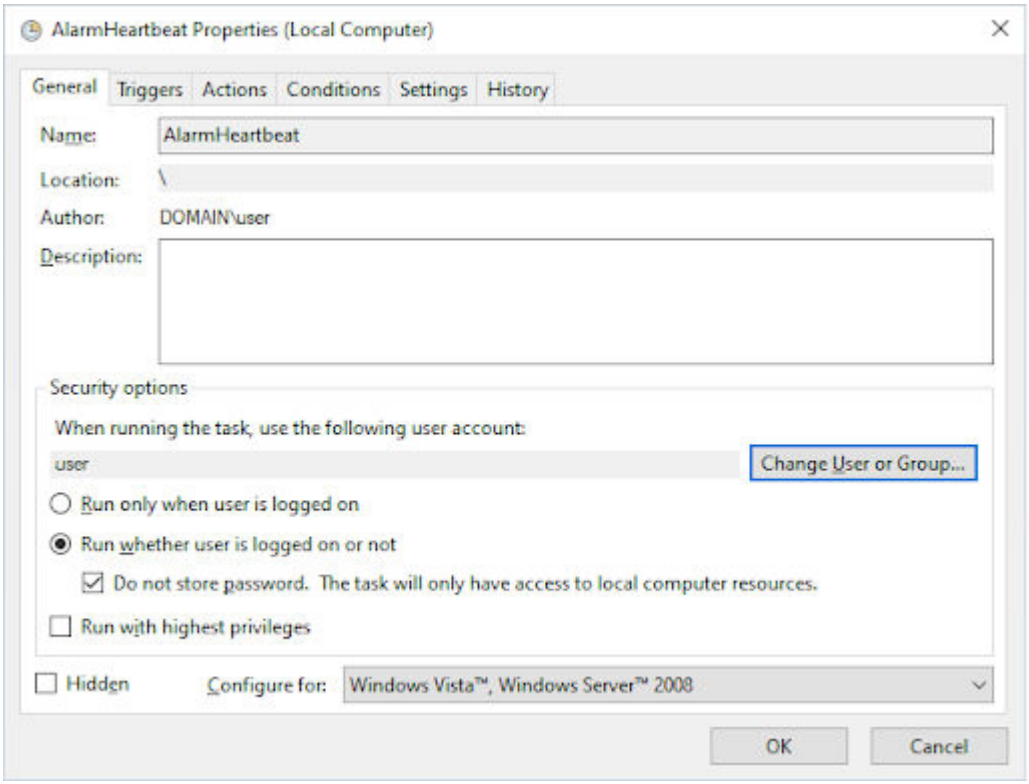
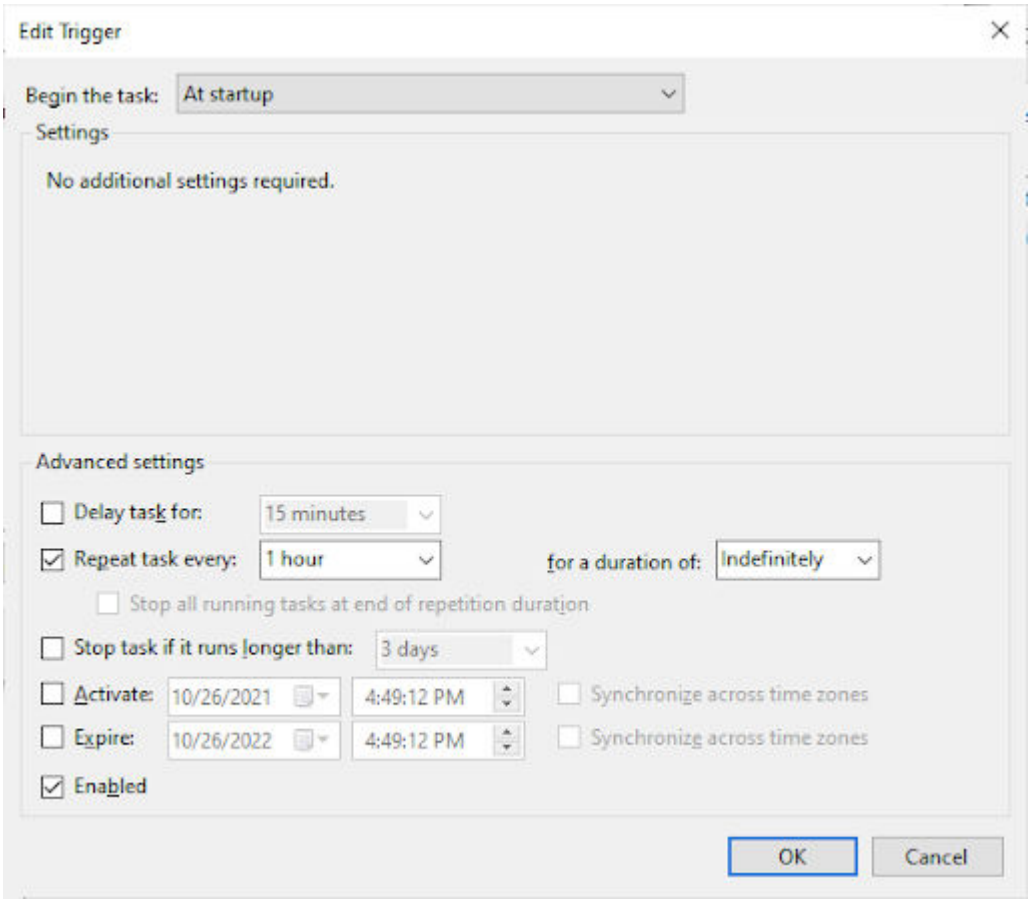
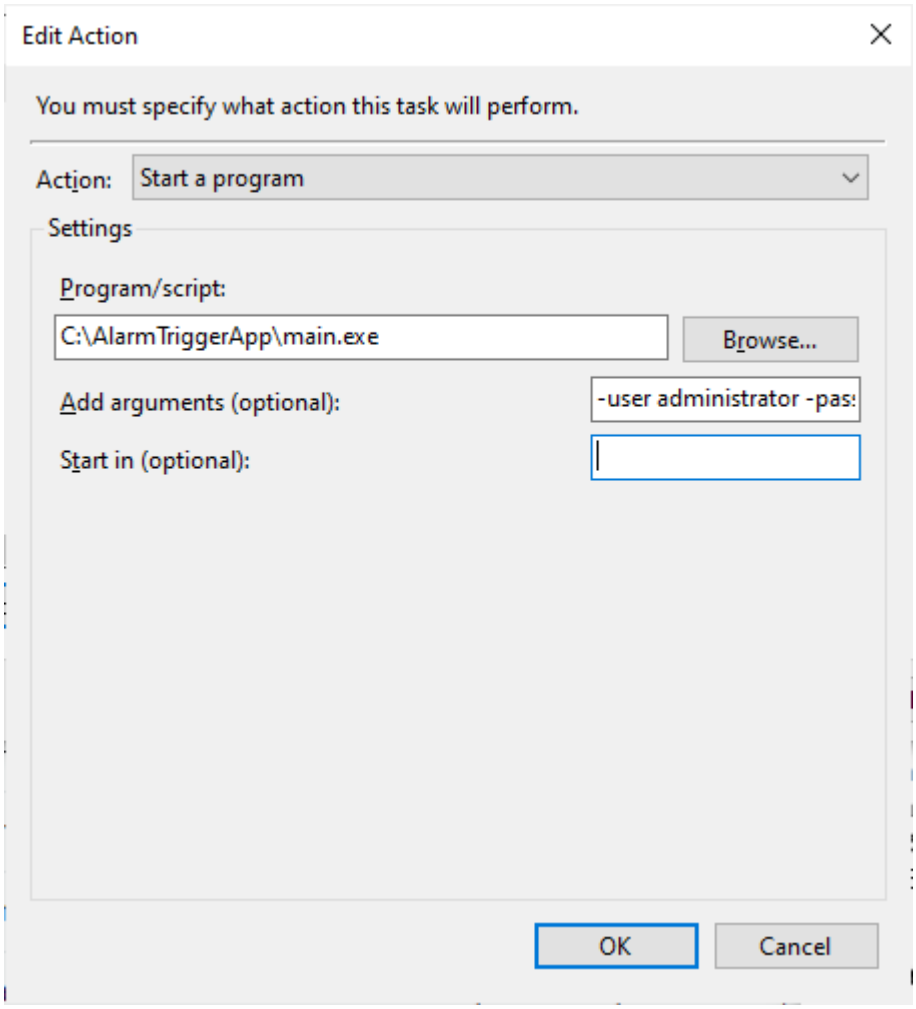


Figure 25: Editing Triggers



NOTE: This task is set to trigger at startup. The user should manually run it the first time to initiate it or to reboot the machine. Also, you should view in Orchestrate if the last received Unity Video Alarm occurred at the time of manual initiation or reboot. A refresh of the Orchestrate page may be necessary.

Figure 26: Editing Actions



Add arguments: `-user Heartbeat -password` *`<heartbeatuserpassword>`*

If running the alarm trigger app on a different machine (not recommended for production), use `-host` argument to specify the hostname or IP of the target machine running the web-endpoint service.

Example:

```
-user Heartbear -password <heartbeatuserpassword> -host
        192.168.10.10
```

Figure 27: AlarmHeartbeat Properties – Conditions

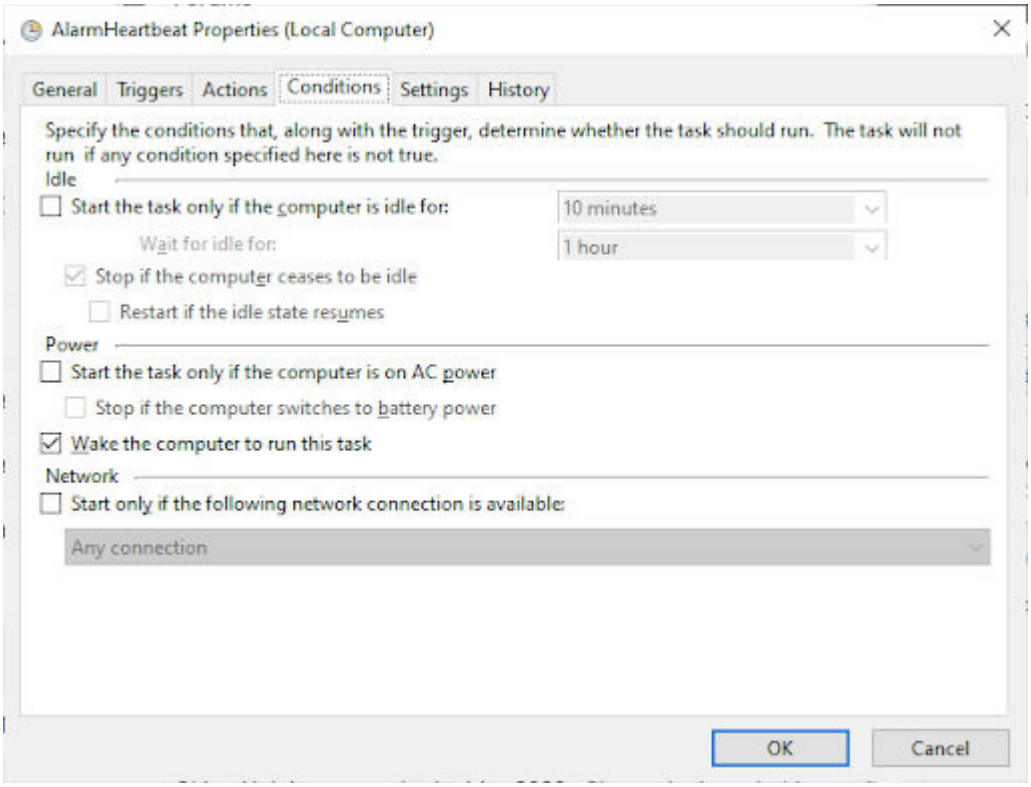
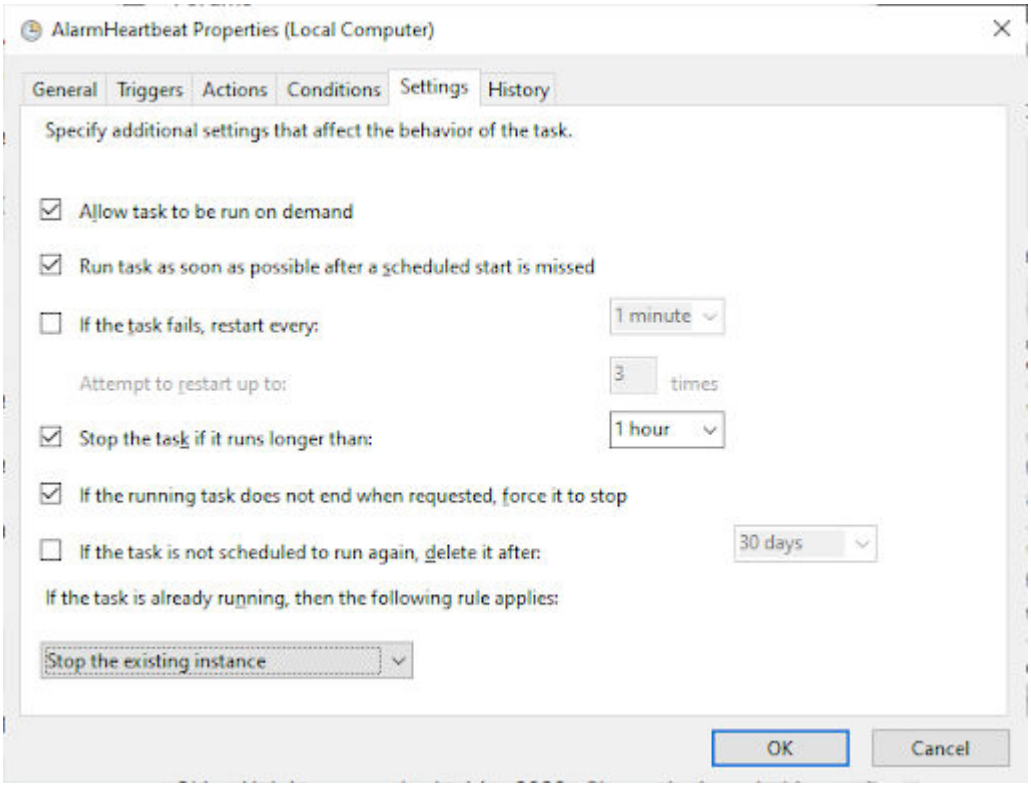


Figure 28: AlarmHeartbeat Properties – Settings



5.5
Unity Video Maintenance Considerations

Over time it is possible that new devices are added to the deployment.

The following are some maintenance considerations.

Adding cameras that can trigger an Alarm

After creating an Alarm in Unity Video for the new camera, the Alarm becomes available in Orchestrate as a Trigger. This can take up to five minutes.

Adding access control connections that can trigger an Alarm

After creating an Alarm in Unity Video for the new access control connection, the Alarm becomes available in Orchestrate as a Trigger. This can take up to five minutes.

NOTE: Orchestrate places Unity Access Alarms under the Unity Video, as they flow through the Unity Video to Orchestrate.

Deleting Alarms from Unity Video

After deleting the Alarm and Rule in Unity Video, the Trigger is removed from the list of Unity Video Triggers within 10 minutes.

If the Trigger is deployed in a workflow that is not part of a group, the Action is flagged and the user has the option to delete or replace the Action.

If the Trigger is deployed in a workflow that is part of a group, the Action is removed from the group with no indication.

5.6
Unity Video/Unity Access Alarm Configuration

Unity Video and Unity Access events must be mapped to Alarms if they are meant to be used in Orchestrate workflows. Additionally, a rule must be configured for the Alarm as well.

NOTE: For Alarms to be fed to the Cloud Connector, web endpoint service must be enabled.

For information on configuring a Unity Video Alarm from a Unity Video Event, see the “Alarms” section in the Avigilon Control Center™ Client User Guide.

For information on configuring a Unity Video Alarm from a Unity Access Event, see the “Adding ACC System Alarms” section in the *Avigilon Alarm Gateway and VidProxy Installation and Configuration Guide*.

For information on configuring a Rule for a Unity Video Alarm, see the “Adding a Rule” section in the Avigilon Control Center™ Client User Guide.

NOTE: To ensure that the business rules mapping in Orchestrate is clear, it is recommended that alarm names follow a meaningful naming convention. The names should include the location codes (for example: **Build 7**, **Door B**, or **Front Entry**), or alarm types (for example: **Watch List**, **Loitering**, **Tampering**, or **Perimeter Alert**). With consistent references, mapping the alarms to business rules is easier and more understandable.

Alarm Configuration Best Practices

The voice and text alarms sent to endpoint radios are based on the Unity Video alarm name. To get the most out of your system, consider the following:

- Radio users will receive all Unity Video alarms with the integration user as an alarm recipient. Only assign alarms to the integration user if a radio user needs to respond.
- Create an alarm for each alarm trigger sent to radio users.
- Use short, descriptive alarm names that follow the format: “Event type, Location”
  - Commas and periods create a pause in voice alarms.
  - Be aware of the text message character limit for your endpoint radios.
  - Avoid using the camera name in the alarm name, as this information may not help the radio user.
- Set the Unity Video alarm schedule to match when radio users should receive alarms.
- After a while, you may find that:
  - Radio users only need the location or a code word in the alarm name.
  - Some alarms occur at the same time each day due to the site's regular operation and can be ignored.
  - New alarms should be sent to radio users.
- For Alarms to be accessible to Unity Cloud Services, in the Unity Client under the Alarm configuration, ensure that the Cloud Administrator and Cloud Viewer have permissions to the alarm.
- Revisit your alarm strategy regularly to see if the alarm name, trigger, and schedule are still appropriate.
- For Alarms used with Unity Cloud Services, until the support of Alarm acknowledgement is available, administrators may want to configure the alarm to Auto-Acknowledge.
- Unity Video does not forward all alarm types to Unity Cloud Services due to the possibility of overloading in the event of a misconfigured alarm. Refer the following table to see which of the basic alarm triggers are supported, unverified, and unsupported:

Table 3: Alarm Support Levels

Alarm (Trigger Source Types)	Support Level
Motion Detection	Not Supported
Video Analytics Event	Supported
Digital Input Activation	Unverified
License Plate Watch List Match	Supported
POS Transaction Exception	Unverified
Device Error	Unverified
System Error	Unverified
External Software Event	Supported
Face Watch List Match	Supported

- Unity Video also supports Alarm Trigger by Rules Events. Not all rule events will be forwarded to Unity Cloud Services due to the possibility of overloading in the event of a misconfigured rule. Refer to the following table to see which of the rule events are supported, unverified, and unsupported:

Table 4: Alarm Trigger by Rules Events

Support Level	Rule Events	
Supported	Device Events	Video analytics event started
		Video analytics event ended

Support Level	Rule Events	
	Access Control Events	Door access granted
Not Supported	Device Events	Motion Detection **IMPORTANT:** If a Motion Detect Alarm is configured in the Unity Video, that Alarm will become a trigger option in Orchestrate. If this trigger is added to a workflow, the workflow will never be successful.
Unverified	All other rules events not outlined above have not been verified, but they may be supported by Unity Video and Unity Cloud Services.	

Chapter 6

Avigilon Alta Access–Orchestrate Setup

The Alta Access–Orchestrate integration provides a cloud layer to create workflows between many Motorola Solutions products.

Figure 29: Alta Access as a Trigger Overview

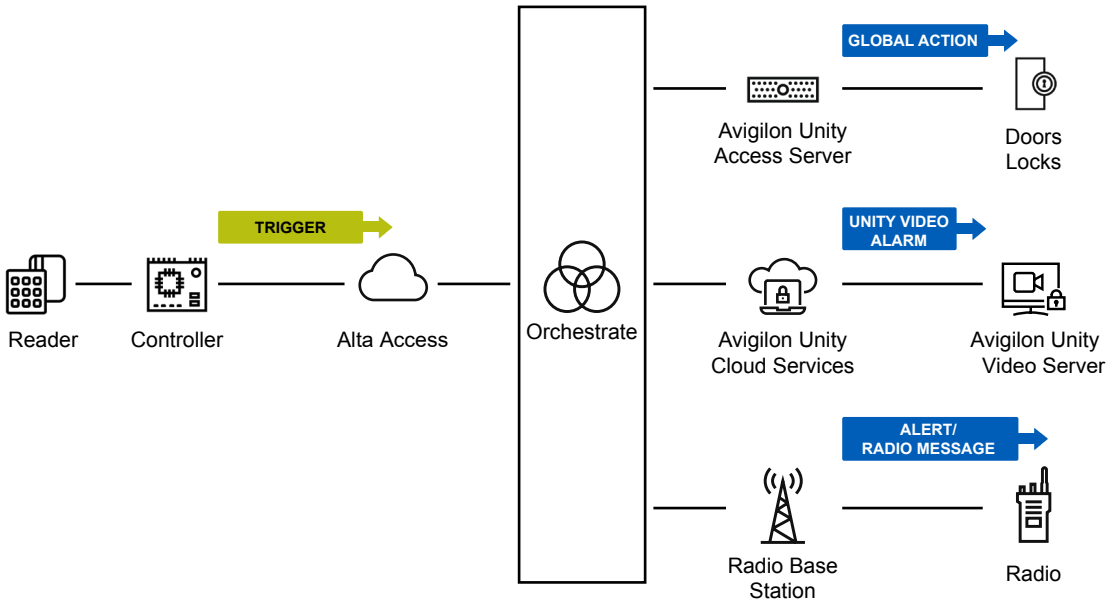
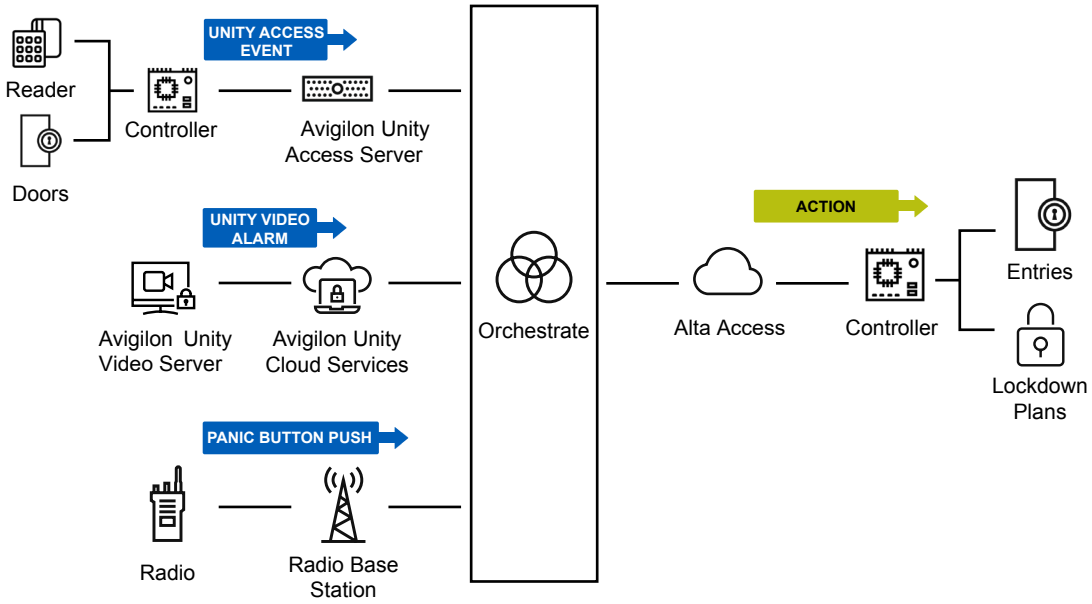


Figure 30: Alta Access as an Action Overview



Actions and Events

Orchestrate supports bi-directional integration with Alta Access providing action capabilities, such as unlocking doors or triggering a lockdown, in response to Orchestrate triggered workflows.

The following Alta Access events can also be consumed and configured in Orchestrate workflows to create powerful workflows among a variety of downstream products.

6.1
Alta Access Actions and Events

Alta Access Basic Plan / Enterprise / Premium Available Actions

```
Unlock Entry
Change Entry State
Trigger Lockdown Plan
Revert Lockdown Plan
```

Alta Access Basic Plan / Enterprise / Premium Available Triggers

```
Contact Sensor State Changed
Generic Input State Changed
REX State Changed
Tamper Detector State Changed
```

Alta Access Enterprise / Premium Available Triggers

```
Entry Ajar Ended
Entry Ajar Started
Entry Anti-Passback Breach
```

```
Entry Unlock Authenticated
Entry Unlock Authentication Failed
Entry Unlock Authorized
Entry Unlock Authorization Failed
Entry Forced Open
Entry Unlocked
Entry Unlock Failed
Reader Fault State Changed
Relay Fault State Changed
Lockdown Plan Revert Authorized
Lockdown Plan Trigger Authorized
Lockdown Plan Reverted
Lockdown Plan Triggered
```

6.2 Setting Up Alta Access–Orchestrate Integration

Procedure:

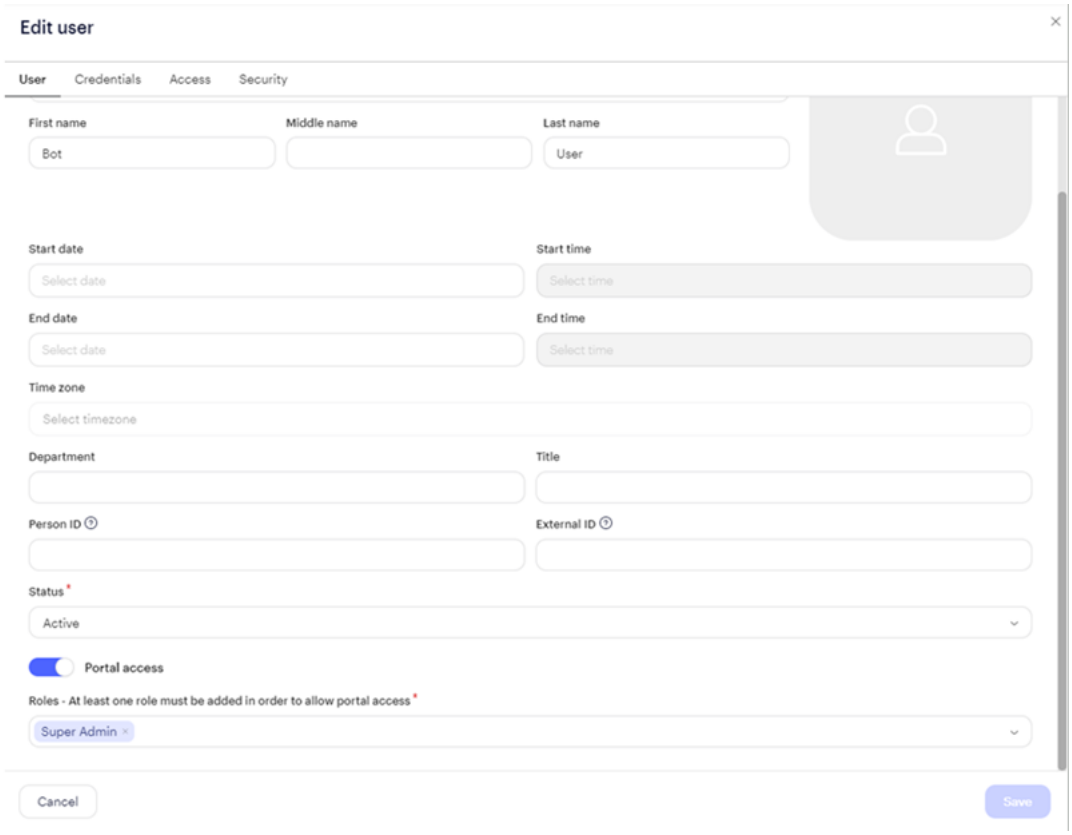
1. Create a Bot user on your Alta Access organization and configure it to access all required entries and lockdown plans by performing Create an Avigilon Alta "bot".

   Make note of the credentials used for the Bot user.

   NOTE: If you want to add the same bot user to multiple ORGs, then you will share the specific email and namespace associated with your bot user's identity. For more information, see https://support.openpath.com/what-is-a-namespace-HkPOX6bFO.

2. Enable Portal Access for the the bot user account by clicking the toggle, then adding the Super Admin role.

Figure 31: Alta Access – Editing User



NOTE: If the end user prefers to create a custom Role with a limited scope, then navigate to **Users** → **Role**, and grant **READ** and **WRITE** permissions to Rules (Configuration), Entry States (Sites), and Lockdown Plans (Sites), and **READ** only permissions to Reports.

3. Optional: To maintain and assign the needed access, create a Group for your bot user.
4. In the **Edit User** window go to **Access** and ensure that **Remote Unlock** is `Enabled` for the Bot user.
5. In the **Edit User** window go to **Credentials**, and create a CloudKey that is assigned to your Bot user. Make note of the name of the CloudKey.

   For instructions on how to perform this step programmatically through API, see https://openpath.readme.io/docs/programmatically-generate-cloud-key-credentials.
6. Obtain and note the Organization Id (OrgId) for your organization in Alta Access.

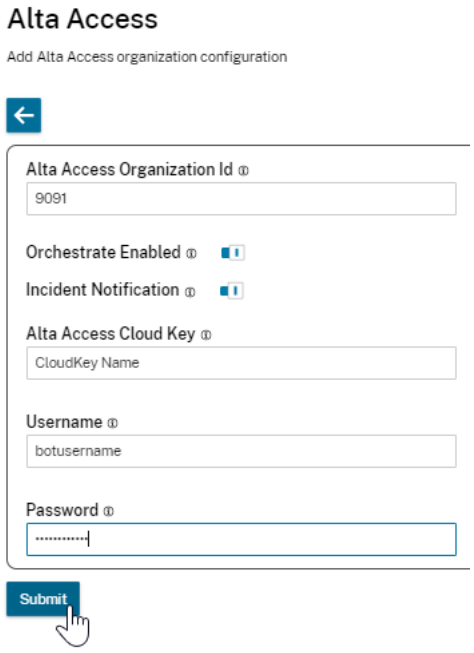
   The OrgId is needed when configuring Alta Access in the **Orchestrate Config** application. To quickly find your OrgId and other resource ids, use the web portal and check the URL – it includes `.../o/<#>/...`

   Example: `https://control.openpath.com/o/302/dashboards/activityDashboard`

   <#> value is the OrgId – in the example, it is 302.
7. Log on to Orchestrate under the desired agency for creating the integration.
8. From the left-hand side navigation, select **Connection Center**.
9. Select **Alta Access**.
10. Click **Configure**.
11. Select **Add Organization**.

12. Fill in the corresponding entries and Submit the form to verify the connection.

Figure 32: Adding Alta Access Organization ID



NOTE: The **Username** is the email address associated with the bot user. The **Alta Access Cloud Key** is the NAME of the CloudKey.

When the connection is successful, actions should shortly appear in Orchestrate. Any configured trigger Rules for Orchestrate will also display.

13. When Configuring Alta Access Rules as triggers for Orchestrate, set the webhook **HTTP Method** to **POST**.

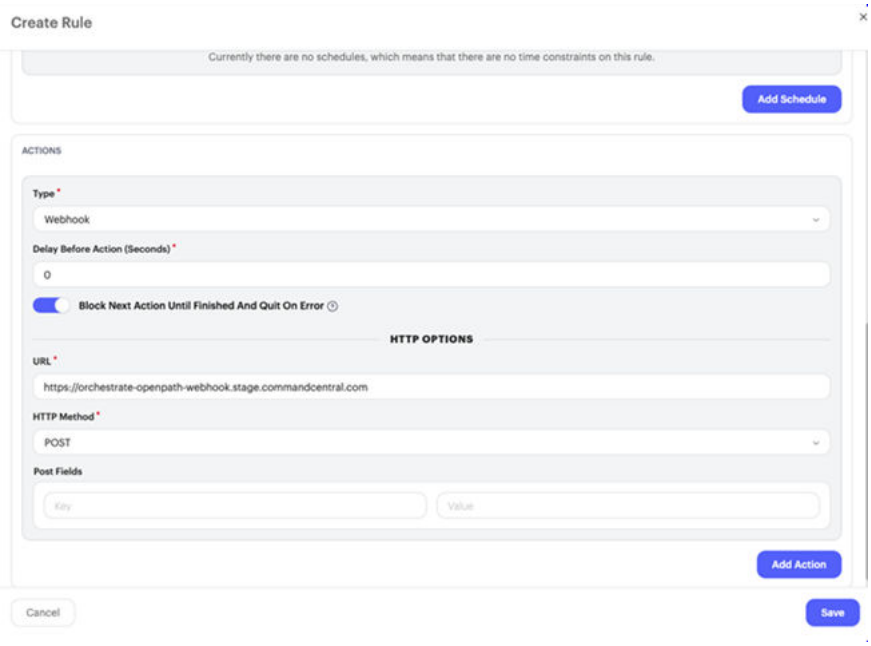
You can find the correct Webhook **URL** in the **Orchestrate Config** application under **Alta Access**.

You should leave all **Post Fields** empty – they will be filled automatically in a few minutes.

NOTE:
The on premises ACU will be sending the webhook request directly to Orchestrate. Ensure that this traffic is not blocked by your firewall.

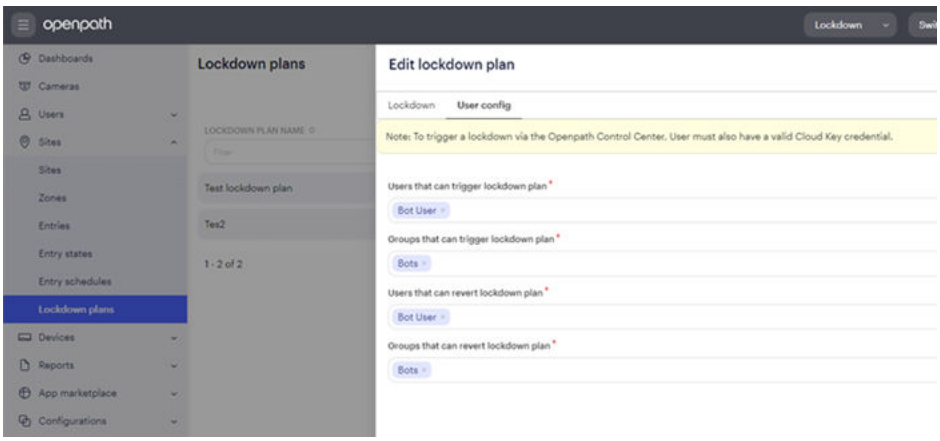
For more information on Alta Access network requirements, refer to https://support.openpath.com/what-are-the-network-requirements-for-openpath-controllers-HyC_t7jUO.

Figure 33: Creating Rules



14. If you want Orchestrate to trigger a lockdown plan or trigger a revert lockdown action, ensure that the Orchestrate bot has access to the desired plans.

Figure 34: Alta Access Lockdown Plans



6.3 Verifying Alta Access Setup

When a workflow is created in Orchestrate, it can be tested and verified.

NOTE: After saving a workflow, it can take up to one minute for it to become active. Testing triggers usually requires physical access to an entry, or the ability to unlock one remotely.

Procedure:

1. Create a workflow that uses the **Entry Unlocked** event in Alta Access as the trigger for the workflow.
2. Use the Webhook URL in the Orchestrate Config - Alta Access page and configure a Rule in Alta Access for the **Entry Unlocked** event

Figure 35: Creating a Workflow

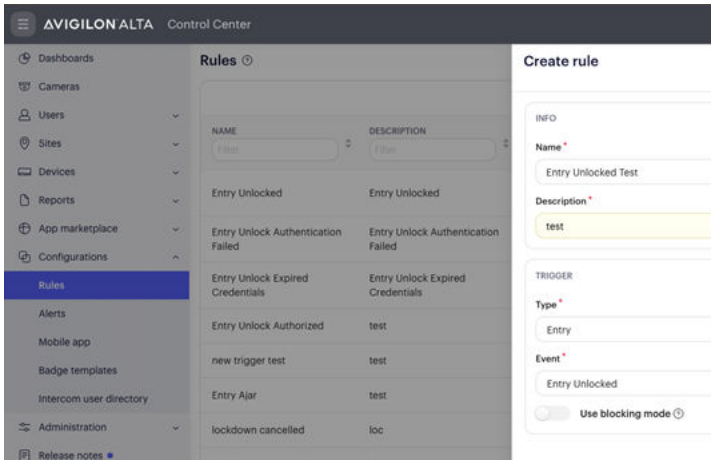
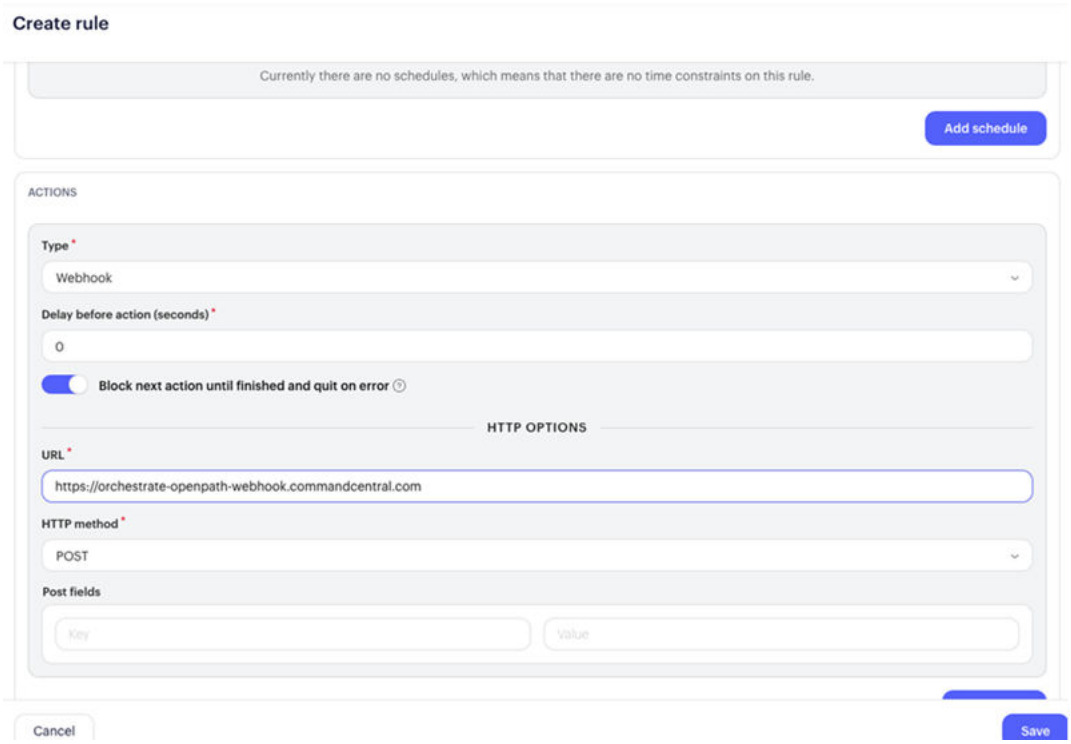


Figure 36: Creating a Rule



3. Click **Save** and wait for your trigger to be discovered into Orchestrate

   This process usually takes one to five minutes.
4. In Orchestrate, create a workflow that uses this trigger and an Alta Access action of your choice.
5. Unlock an entry and monitor the Runtime Data Table in Orchestrate to confirm if the workflow executes successfully.

Chapter 7

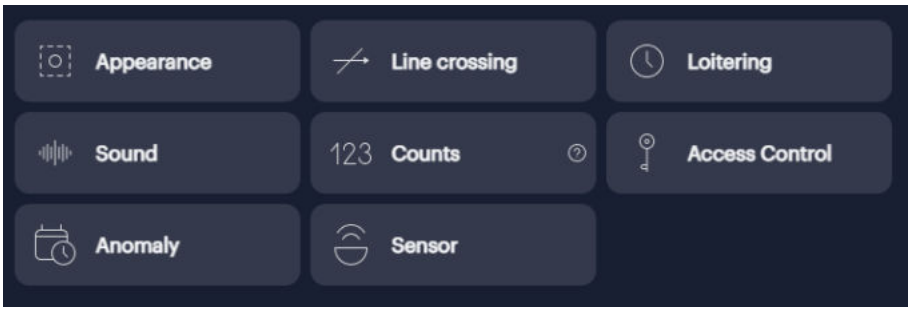
Avigilon Alta Video–Orchestrate Setup

The Alta Video–Orchestrate integration provides a cloud layer to create workflows between many Motorola Solutions products.

Alta Video Triggers

The Alta Video Triggers defined by Alta Video Rules can be consumed and configured in Orchestrate workflows to create powerful workflows among a variety of downstream products.

Figure 37: Alta Video Rule Types



7.1
Configuring API (Bot) User

Procedure:

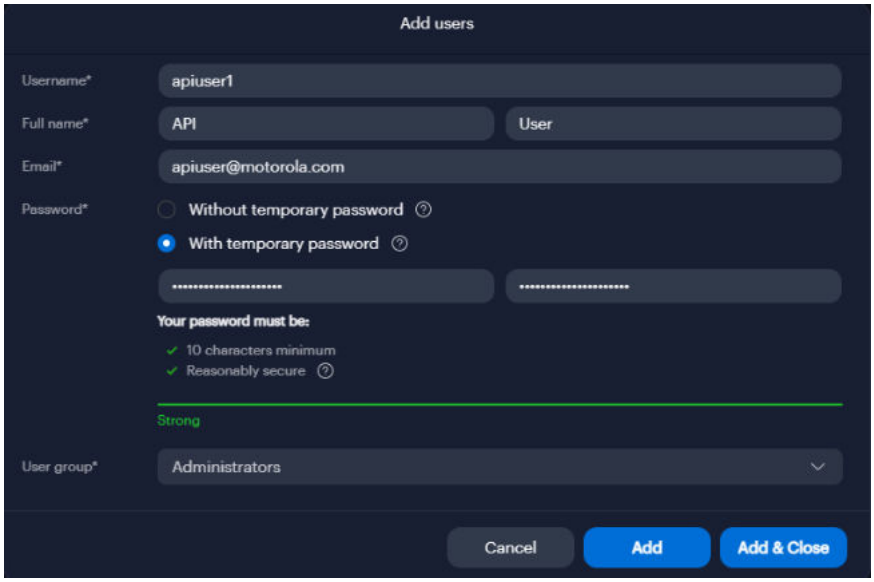
1. In Alta Video, navigate to the **Users** tool and add a user by clicking the plus icon in the top-right corner.

   Figure 38: Adding Users in Alta Video

2. Create an API user with an appropriate email, and note down that email address.

   Orchestrate will use this API User for the connection.

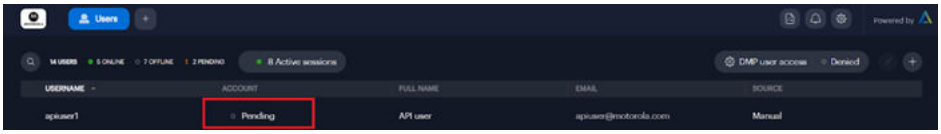
Figure 39: Adding API Users



IMPORTANT: The API User must belong to the **Administrators** user group, **not** to the **Operators** user group.

When the API user is added, it displays as **Pending** in the **Users** table.

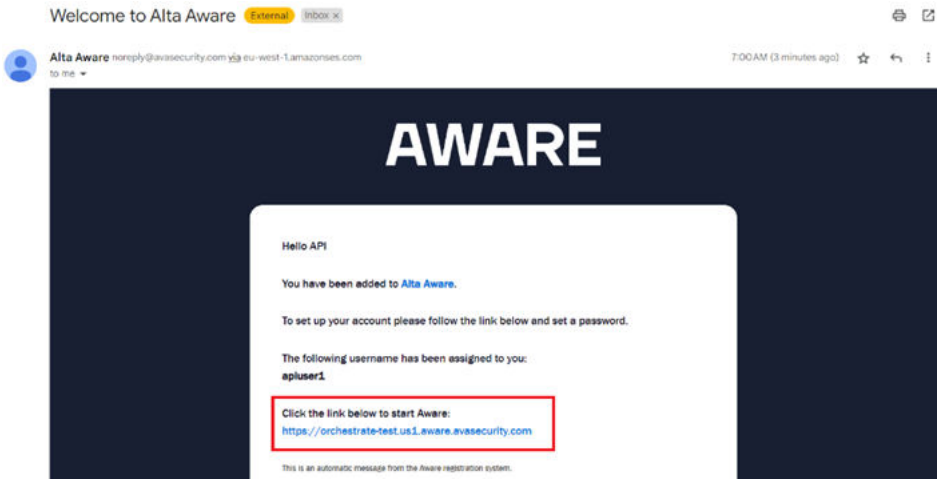
Figure 40: Pending API User



Additionally, a verification email is sent to the account associated with the API user.

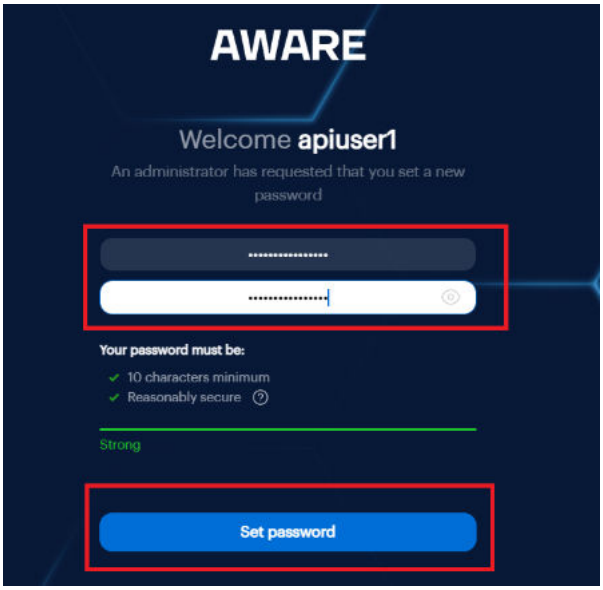
3. Perform the actions described in the email and set up the API User account.

Figure 41: Welcome to Alta Video Email

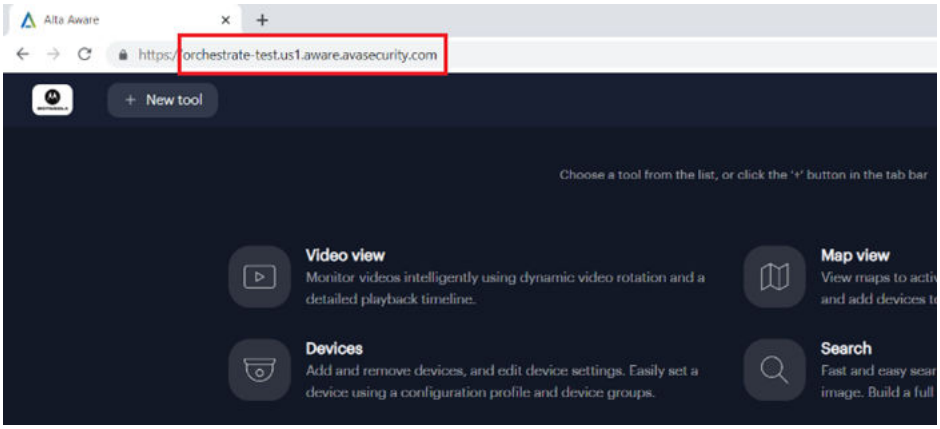


4. Enter the password used during the initial setup of the API User account.

Figure 42: Entering Alta Video Password

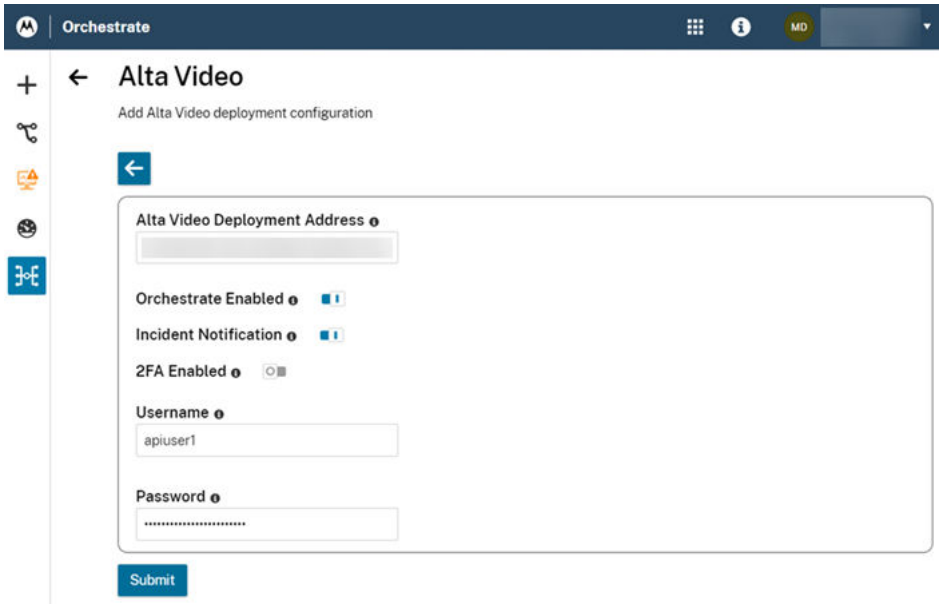


5. From the address bar of the browser, note down the Alta Video Deployment (Cloud Server) Address.
   Do not include the protocol *https://* or any following paths or forward-slashes (“ / “).
   Figure 43: Alta Video Deployment Address



6. Accept Alta Video Terms of Service.
7. In a new tab, access Orchestrate and log on under the desired agency for creating the integration.
8. From the left-hand side navigation, select **Connection Center**.
9. Select **Alta Video**.
10. Click **Configure**.
11. In the top-right corner of the screen, click **Add Deployment**.
12. Fill in the necessary fields and at the bottom of the screen click **Submit** to verify the connection.
    The **Username** and **Password** fields are the ones associated with the bot user account. When the connection is successful, any rules defined in Ava should be discovered in Orchestrate as triggers.

Figure 44: Alta Video Configuration in Orchestrate Connection Center



NOTE: The deployment address used in this section does **not** begin with `https://` and does **not** include any following paths or forward-slashes (“ / “). The **Username** is the email address associated with the bot user.

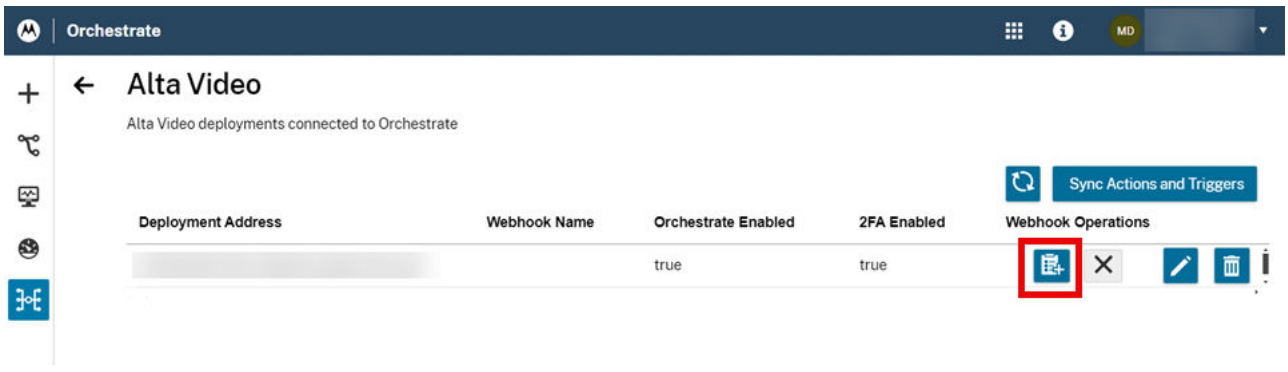
7.2

Configuring Webhook to Receive Alarms from Alta Video

Procedure:

1. Log on to Orchestrate.
2. From the left-hand side navigation, select **Connection Center**.
3. Select **Alta Video**.
4. Click **Configure**.
5. Select a desired Alta Video Deployment and under **Webhook Operations** click the **Add Webhook** icon.

Figure 45: Adding Webhooks



6. Configure the Webhook Name, username and password for securing the webhook connection by using digest authentication.

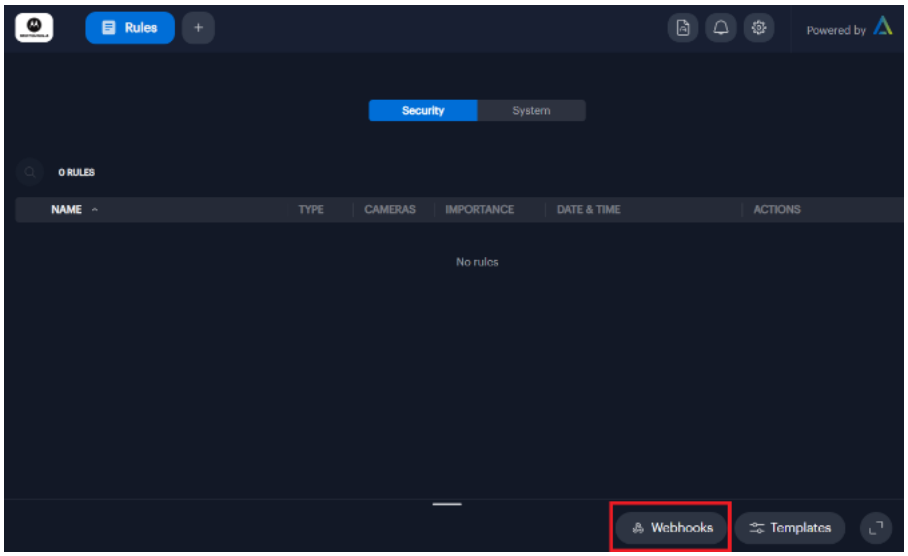
   NOTE: The Webhook Digest Auth Details are separate from the ones used for the API User.

   The webhook connection is now set up in both the Orchestrate Connector and the associated Alta Video Deployment. The webhook will be used to configure rules in Alta Video to communicate with Orchestrate.

   NOTE: The webhook name is **not** automatically generated. You must enter the webhook name in the **Webhook Name** input field – the character limit is 40.

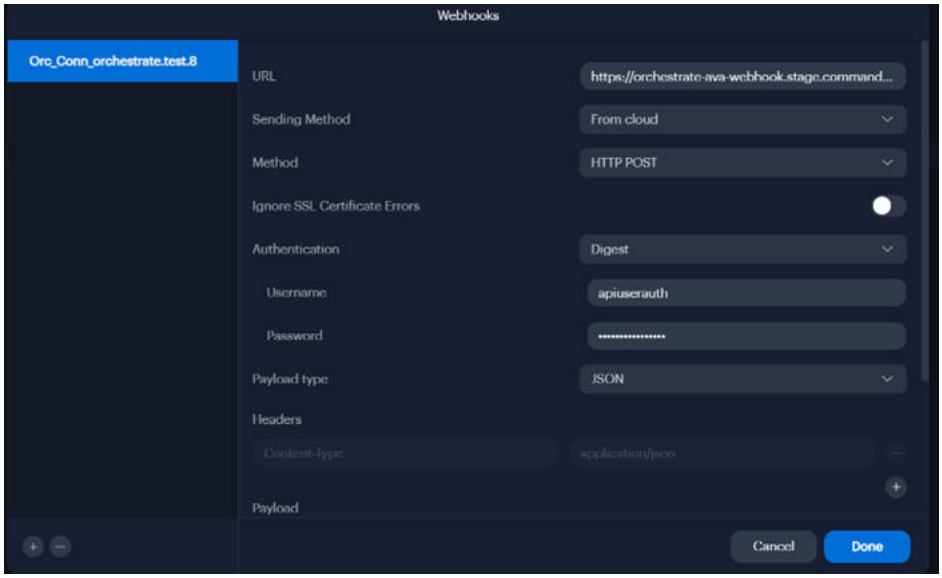
7. To confirm the creation of the webhook, access Alta Video and navigate to the **Rules** tool, then select **Webhooks**.

   Figure 46: Alta Video Rules Tool



   The configured webhook should display in the webhooks list.

Figure 47: Webhooks List



NOTE: You can test the new webhook by using the option at the bottom of the webhook page.

7.3 Creating Rules in Alta Video: Triggers

The Alta Video rules which are Alarms are Triggers in Orchestrate. When a rule is activated in Alta Video, it can be sent to Orchestrate as a Trigger – this mechanism enables a cross-product workflow implementation.

For the complete list of Alta Video rules, see Figure 37: Alta Video Rule Types on page 56.

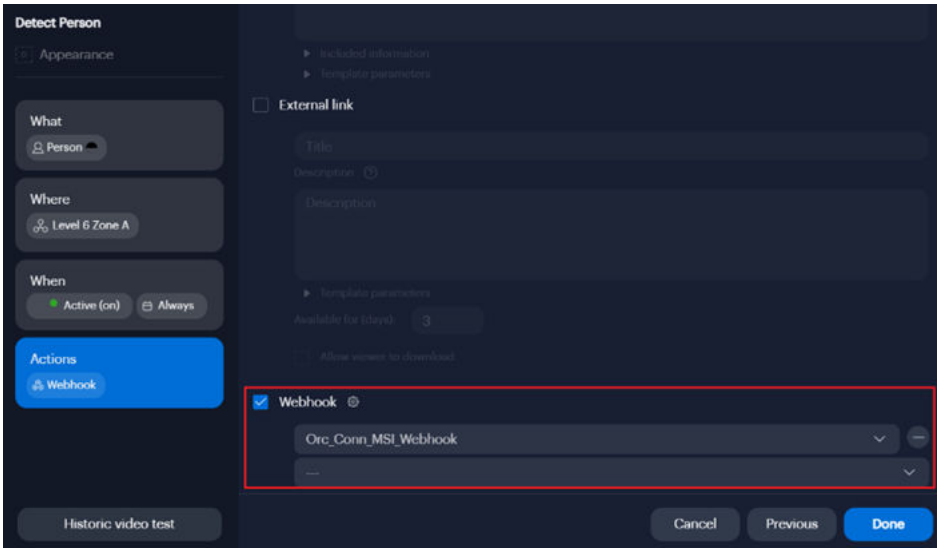
Perform the following steps to create rules in Alta Video to be triggers in Orchestrate.

Procedure:

1. To create rules in Alta Video as triggers in Orchestrate, perform the following actions:
   a. In Alta Video, select **Rules** → **Add a rule**.
   b. Under **Actions**, select the webhook associated with Orchestrate.

   This allows Alta Video to send the alarm events to Orchestrate.

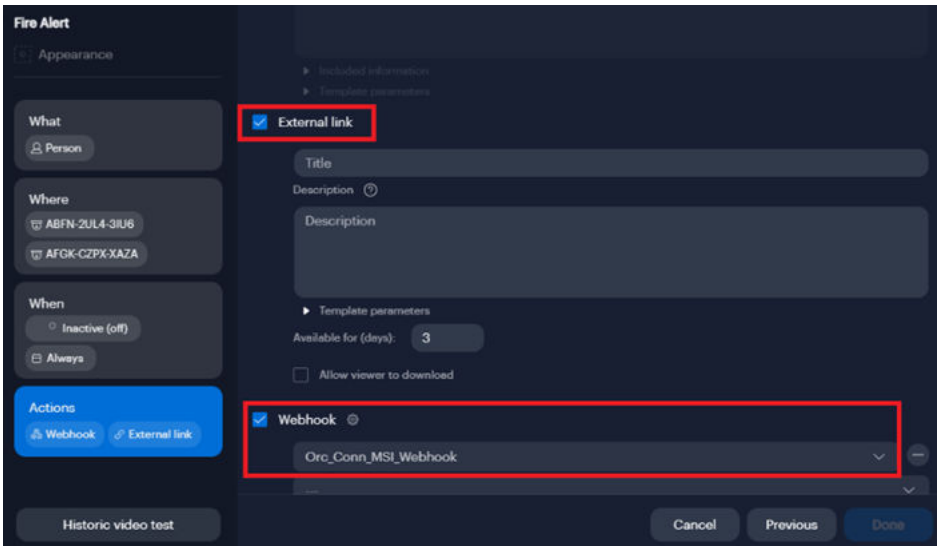
Figure 48: Creating Rules as Orchestrate Triggers in Alta Aware



2. If you want to create a trigger in Orchestrate that includes a video capture, select **External link**.

   This allows Alta Video to send the link to the captured video to Orchestrate.

   Figure 49: Creating Rules as Orchestrate Triggers with Video Captured in Alta Video



7.4 Creating Rules in Alta Video: Actions

When an Orchestrate workflow is triggered, it can be configured to raise an alarm based on a rule in Alta Video. This rule is then displayed in the events list.

Perform the following steps to create rules in Alta Video to be actions in Orchestrate.

For more information, refer to Alta Video documentation.

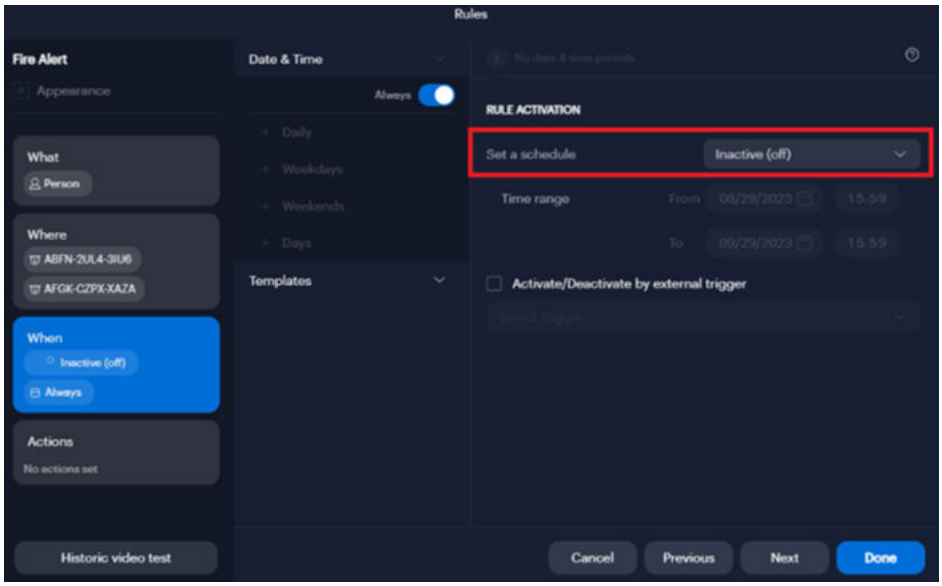
Procedure:

1. In Alta Video, go to **Rules**.
2. Select the desired rule.

3. **NOTE:** Rules are usually initiated in Alta Video by cameras in the Alta system. If you want to ensure that a rule which represents an Orchestrate Workflow is not confused with the same rule being initiated by a camera, you should deactivate the camera.

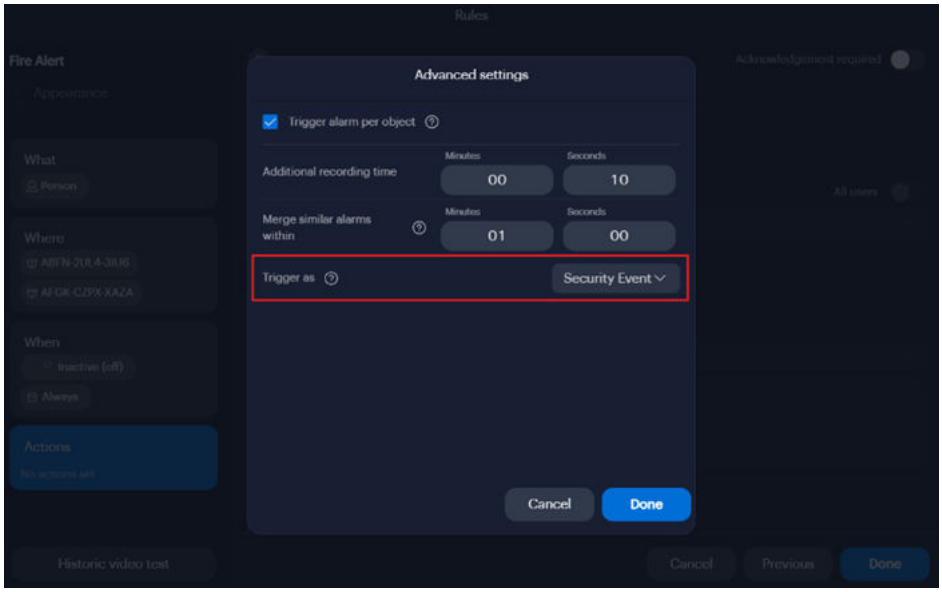
   Under **When**, deactivate the rules defined as actions by setting **Set a schedule** to **Inactive (off)**.

   Figure 50: Rules Deactivation



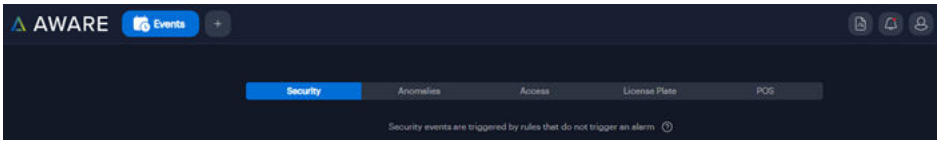
4. Under **Actions**, select **Advanced**, then in **Trigger as** select **Security Event**.

   Figure 51: Alta Video Advanced Settings



Alert Actions triggered by Orchestrate are listed under **Events** tool.

Figure 52: Alarms Tab



7.5

Configuring Two Factor Authentication

NOTE: Enabling Two Factor Authentication (2FA) is optional. By enabling 2FA you add additional security to the API User account.

IMPORTANT: To enable 2FA, you must **only** use the Orchestrate Configuration Page. Do **not** preconfigure 2FA in the Alta Video portal. If 2FA is already configured in the Alta Video Portal for the API User, it must be disabled in the Alta Video Portal first before you enable it in the Orchestrate Configuration Page.

Procedure:

1. Log on to Orchestrate
2. From the left-hand side navigation, select **Connection Center**.
3. Select **Alta Video**.
4. Click **Configure**.
5. Select a desired Alta Video Deployment and click the corresponding **Edit** button.
6. Select the **2FA Enabled** toggle and at the bottom of the page click **Update**.

   2FA Enabled is set to **true**. All subsequent requests from Orchestrate to Alta Video through the API User are 2FA enabled.

Chapter 8

Avigilon Decision Management System–Orchestrate Integration

Avigilon Decision Management System (DMS) is a cloud solution that integrates with physical security systems and supports the decision-making process of the security personnel. Avigilon DMS helps to improve consistency and effectiveness of incident response actions with standard operating procedures, make data-driven decisions, and achieve compliance.

The Avigilon DMS system integration with Orchestrate allows you to integrate Orchestrate workflows with the DMS system. A successful integration results in automatic resource creation in DMS and Orchestrate. Orchestrate actions can trigger DMS incidents and DMS operators can activate Orchestrate triggers manually. The Orchestrate health monitoring service can be used to monitor the DMS integration from Orchestrate.

Data-in-transit between Avigilon DMS and the integrated Orchestrate is encrypted and transferred over HTTPS with a digital certificate provided by Orchestrate. The data-in-transit is owned by the customer and is not stored on the cloud.

For more information on Avigilon DMS, see Avigilon Decision Management System documentation.

8.1 Avigilon Decision Management System Prerequisites

Before configuring Avigilon Decision Management System (DMS), ensure that you have successfully completed the product certification courses and exam.

The training materials and exam are available at he Avigilon Training Platform:

- Avigilon DMS Configuration course (A-223)
- Avigilon DMS Operation course (A-224)
- Avigilon DMS Certification exam (A-513-OL)

Avigilon DMS uses Avigilon Unity Cloud Services for organization management, including users and user groups management.

NOTE:

- Avigilon DMS is currently only hosted in the United States.
- To use Avigilon DMS, you must first create a Unity Cloud Services organization in the United States instance.

Table 5: Unity Cloud Services Considerations

If...	Then...
If you do not have a Unity Cloud Services organization,	go to cloud.avigilon.com, select the US region and click **Not registered? Sign up.**, then follow the steps.
If you do not know how to connect your Unity Video Sites to Avigilon Unity Cloud Services,	see the following tutorial on how to connect your Unity Video Sites to Avigilon Unity Cloud Services.

With the integration of Avigilon DMS with the Prodigy platform, it is now required for the Unity Cloud Services organization to be upgraded to a Unity Organization. The upgrade option is only available if all Unity Video sites configured in that organization are in version 8 or above.

8.2

Configuring Orchestrate for Avigilon Decision Management System

Configuring Orchestrate involves ingesting the Avigilon DMS system into Orchestrate.

Procedure:

1. Log on to Orchestrate as Agency Admin with your CommandCentral credentials.
2. From the Application Switcher select **Admin**.
3. From the left-hand menu, select **Organization Overview**, then select **Organization Information**.
4. Note down the **Organization ID** value.

   This value is used in the DMS subsystem configuration in Configuring Avigilon Decision Management System on page 67.
5. In the Orchestrate Dashboard, next to the workspace name, select  → **Edit**.
6. Under **Select your criteria**, ensure that **Avigilon DMS** triggers and actions are selected, or that **All triggers and actions** option is selected.

8.3

Configuring Avigilon Decision Management System

Avigilon DMS can connect to and communicate with other video security and access control software by using subsystems. The connections between subsystems and sites in the organization display in the **Subsystems** tab. Each site can be connected to multiple subsystems.

Procedure:

1. In the DMS page header menu, click **Configuration**.
2. Click **Subsystems** and select a site.
3. Click **Add**.

   A new empty subsystem is added to your site.
4. In the **Name** field, enter a name for your subsystem.
5. From the **Brand** drop-down list, select **Motorola Solutions**.
6. From the **Model** drop-down list, select **Orchestrate**.
7. Add the following connection data information:

Table 6: Orchestrate-specific Connection Data Information

Setting	Description
Agency ID	The ID of the Orchestrate organization to establish the connection. See Configuring Orchestrate for Avigilon Decision Management System on page 66.
Triggers	A semicolon-separated list of triggers and their descriptions. Triggers are events that flow from DMS to Orchestrate. For example, `Send to radio group; Go to main lobby;` – a trigger **Send to radio group** and its description `Go to main lobby` as the message to be sent to the configured radio group in Orchestrate. **NOTE:** The text field has an input limit of 255 characters.
Actions	A semicolon-separated list of actions. Actions are events that flow from Orchestrate to DMS. For example, `Send to DMS` – an action **Send to DMS** to act as an exit point of an Orchestrate workflow. **NOTE:** The text field has an input limit of 255 characters.

8. Click **Save**.

   If the subsystem is successfully added to your site, the resources are automatically created in DMS and Orchestrate.

8.4

Configuring Incident Behaviors

When the integration between Orchestrate and Avigilon DMS is successful, you can set incident behavior rules in DMS to generate an incident for incoming Orchestrate Actions.

The Orchestrate Actions that can trigger incidents in DMS are the ones you configured while adding a new Orchestrate subsystem in Configuring Avigilon Decision Management System on page 67.

Procedure:

1. In the DMS page header menu, click **Configuration**.
2. Click **Behaviors** and select a desired site.
3. Click **Add**.

   A new empty behavior is added to your site.
4. In the **Trigger** section, perform the following actions:
   a. Select a subsystem from the list of available subsystems for that site.
   b. Select an event type from the list of available event types for the selected subsystem.
   c. Optional: Select the resource from the list of available resources for the selected subsystem.

      IMPORTANT: Either keep the **Resource** field empty, or select the same option for both the **Resource** and the **Event type** fields. If the **Resource** field is configured differently from the **Event type** field, the incident behavior will **not** be triggered in DMS.

   NOTE: When configuring incident behaviors, the event type and resource drop-down options will only list the configured Orchestrate Actions, and not the Triggers. Configured Orchestrate Triggers do **not** trigger DMS incident behaviors, only the Orchestrate Actions do.
5. In the **Properties** section, perform the following actions:
   a. In the **Title** field, enter a name for the behavior.
   b. Select the desired priority for the behavior in the system.

      The available options are **Critical**, **Major**, **Minor**, and **warning**, listed from the highest priority in the system to the lowest.
   c. Select the incident type from the list of available incident types:

      Generic – a general incident type
      Access Control – an access control incident type, typically for access control events.
      Intrusion – an intrusion incident type, typically used for perimeter violations.
      Technical – any other incident type that may be categorized as technical.
   d. Select the desired template from the available Operator Guide templates.
6. Click **Save**.

   IMPORTANT: If an Orchestrate Action triggers a DMS incident more often than every 10 seconds, Orchestrate receives a response successfully, but DMS does not show those actions which happen more often than every 10 seconds. For a system with multiple different actions defined, this 10-second limit applies to each defined action separately.

8.5
Verifying the System Integration

Procedure:

1. To verify if the DMS resources are available in the Orchestrate agency workspace, perform the following actions:
   a. From the Orchestrate dashboard, select your workspace from the **My Workspaces** drop-down menu.
   b. Select  → **Edit**.
   c. Under **Select your criteria**, select the **Avigilon DMS** check box.

      The Triggers and Actions as configured in the DMS subsystem display in the **Preview** panel on the right. You can use those Triggers and Actions in your Orchestrate workflows.
2. To verify if you can activate Orchestrate triggers from the DMS, perform the following actions:
   a. Click on a mapped Orchestrate resource icon that represents an Orchestrate Trigger.
   b. Click on an Orchestrate resource icon in a resource interaction task that is part of an Operator Guide.
   c. In Orchestrate, from the left-hand menu select **Runtime data**.

      The Triggers activated from DMS display in the list of triggers in the Runtime Data table.

Chapter 9

Ally Integration

1. Ensure that a Tenant is registered in Ally.
2. In the Orchestrate Connection Center, in the **Ally** details page click **Configure**.
3. Enter the Tenant Agency Code used when logging on to Ally.
4. Edit your Orchestrate workspace to verify that your Ally Actions have been discovered.

   NOTE: You should see an Action for each sub-agency.

Chapter 10

Email Integration

To add Email to the Orchestrate integration, perform the following steps:

1. In CommandCentral Admin, create any users or user groups that you want to notify.

   NOTE: Users and user groups must have one or more Orchestrate permissions to be available as email recipients.

2. Visit the Email configuration page by selecting **Configure** in the **Connection Center** page.
3. Select the actions that you want to enable for Orchestrate, then click **Save**.

Chapter 11

MOTOTRBO Configuration

11.1 Motorola Edge Node Installation

The Motorola Edge Node is required for text message flow between Orchestrate, Unity Video and MOTOTRBO radios.

For more information, see *Motorola Edge Node Installation Guide*.

IMPORTANT: Deployments are now split into US and non-US regions. Make sure that the appropriate firewall exceptions are used.

11.1.1 Determining Radios and Talkgroups To Be Available in Orchestrate

Procedure:

1. In Radio Management (RM) Radio View, select all radio rows.
2. Select **Grid to File** and save the output as a `.csv` file.
3. By using a text editor, for example Microsoft Excel, modify the table in the `.csv` file to include the following information:

Table 7: Information for the CSV File

Column Name in the Motorola Edge Node CSV File	How to get the Value
SerialNumber	Exported from RM without change
DeviceAlias	**RadioAlias**, exported from RM
ModelNumber	Exported from RM without change
UnitId	**RadioId**, exported from RM
SystemId	The MOTOTRBO system ID (five hexadecimal digits, provided by the customer). **NOTE:** The system ID is a unique ID to identify a radio system under a particular customer. For more details, refer to *Motorola Gateway to LMR Network (MGLN) System Planner*.
Deleted	• `True` – if the radio is no longer in the fleet • `False` – otherwise

NOTE: You can access a CSV template useful in filling the CSV fields.

11.1.2

CommandCentral Unit Management

MOTOTRBO devices supported by an Edge Node are provisioned into CommandCentral Admin. Admin supports multiple use cases which can include linking multiple Devices to a Unit. However, in an Orchestrate deployment, there is a one-to-one relationship between a Device and a Unit. Because the Edge Node uses the Devices while Orchestrate uses the Units, it is important to remember that Devices and Units have a one-to-one relationship in MOTOTRBO deployments.

For an overview of the provisioning process of different types of devices and systems, including MOTOTRBO, refer to the *CommandCentral Aware Location Tracking Administration* training.

NOTE: You should only manually add Devices. Do **not** manually enter Units.

Radio Management supports the concept of Groups and Nested Groups in the radio view. This allows radios to be segregated when exporting to the `.csv` file. For deployments using multiple Unity Servers on a single MOTOTRBO system, the `.csv` file associated with a Unity Server can only have the radios associated with them. It cannot have the entire list of radios in the system. Groups should be used to export the subset of radios for each Edge Node/Unity Video pairing.

To support emergency declaration from the MOTOTRBO device at IP Site Connect and Capacity Plus systems, the emergency location trigger must be set at the MOTOTRBO **Cadences** page in the Unit Management.

NOTE: Emergency location trigger is **not** required to support the emergency declaration at Capacity Max system when Voice and Radio Command (VRC) Gateway is deployed and enabled with license. However, the MOTOTRBO emergency talkgroup must be configured in the talkgroup list at Unit Management – for more information, see Adding Talkgroups Through CSV File on page 75 and Adding Talkgroups Manually on page 75.

11.1.2.1

Creating Agency Groups for MOTOTRBO Devices

Procedure:

1. In CommandCentral Admin, go to **Application settings** → **Unit Management** → **Agency Groups**.
2. Click **Add Agency Group**.
3. In **Agency** tab, fill in **Agency Group ID**.

   Agency Group ID can represent the useful groupings of business rules.
4. In **MOTOTRBO** tab, fill in **MOTOTRBO Tenant ID**.

   This value is provided by the Magellan/MOTOTRBO deployment team.
5. Click **Save**.

11.1.2.2

Adding MOTOTRBO Devices Through CSV File

Procedure:

1. Set **Auto Create Enabled** to **Disabled** by performing the following actions:
   a. In CommandCentral Admin, from the left-hand side menu, select **Application Settings**.
   b. Go to **Unit Management** → **Agency Groups**.

c. Select the MOTOTRBO agency group, and from the **Auto Create Enabled** drop-down list select **Disabled**.

d. Click **Save**.

2. Upload the CSV file which contains the following information for each Device:

   System Type (d10 = MOTOTRBO)
   Area ID (Magellan Tenant ID)
   Magellan System ID (=1)
   Radio ID
   Agency Group ID
   Radio Alias (optional)
   Serial Number (optional)
   Model Number (optional)

Figure 53: Example of a CSV File for Adding MOTOTRBO Devices

	A	B	C	D	E	F	G	H	I	J	K	L
1	System Type*	Area ID*	System ID*	Radio ID*	Agency Group ID*	Radio Alias	Serial Numb	Model Numt	Description	Import Status	(For Server Use Only)	
2	d10	300	1	2	MOTOTRBO-Agency-Group1	Radio2						
3												
4												

3. Set **Auto Create Enabled** to **Enabled** by performing the following actions:

   a. In CommandCentral Admin, from the left-hand side menu, select **Application Settings**.

   b. Go to **Unit Management** → **Agency Groups**.

   c. Select an agency group, and from the **Auto Create Enabled** drop-down list select **Enabled**.

   d. Click **Save**.

   A Unit is automatically created in CommandCentral for a Device when it becomes present on the system. The name of the Unit is the same as the Device's Radio Alias in the CSV file.

   Within 5 minutes of the Device becoming present on the system, an Action for the created Unit appears in Orchestrate.

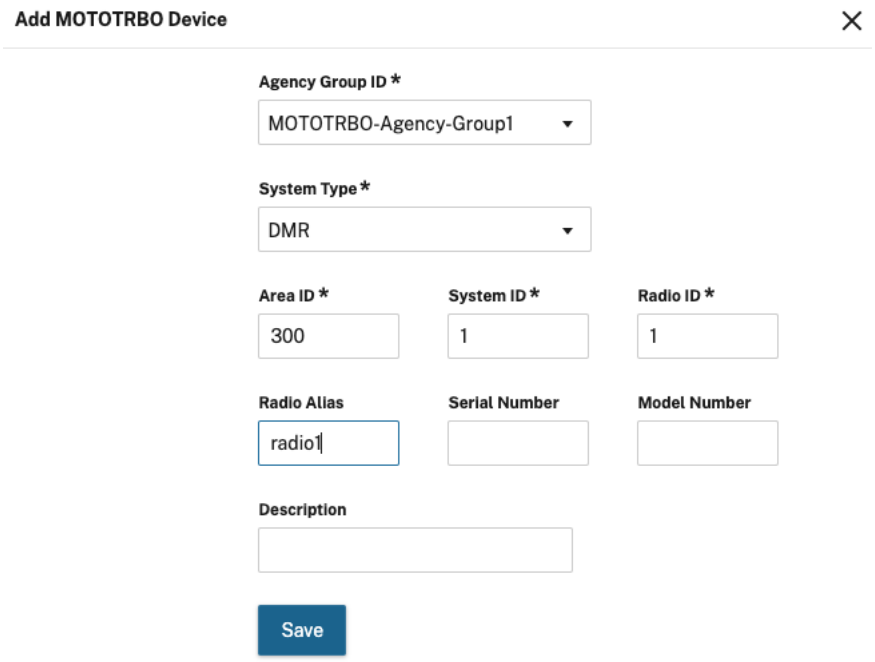
11.1.2.3
Adding MOTOTRBO Devices Manually

Procedure:

1. Set **Auto Create Enabled** to **Disabled**.
2. Enter the following information for each Device manually:

   Agency Group ID
   System Type (d10 = MOTOTRBO)
   Area ID (Magellan Tenant ID)
   Magellan System ID (=1)
   Radio ID
   Radio Alias (optional)
   Serial Number (optional)
   Model Number (optional)

Figure 54: Adding MOTOTRBO Devices Manually



3. When all Devices are added, set **Auto Create Enabled** to **Enabled**.

   A Unit is automatically created in CommandCentral for a Device when it becomes present on the system. The name of the Unit is the same as the Device's Radio Alias in the CSV file.

   Within 5 minutes of the Device becoming present on the system, an Action for the created Unit appears in Orchestrate.

11.1.2.4
Adding Talkgroups Through CSV File

Procedure:

1. Download the CSV template.
2. Enter the following information for each Talkgroup in the template manually:

   System Type (d11 = MOTOTRBO Talkgroup)
   Area ID (Magellan Tenant ID)
   Magellan System ID (=1)
   Talkgroup ID
   Talkgroup Alias
3. Upload the template.

11.1.2.5
Adding Talkgroups Manually

Procedure:

1. Enter the following information for each Talkgroup manually:

   System Type (d11 = MOTOTRBO Talkgroup)
   Area ID (Magellan Tenant ID)

Magellan System ID (=1)
Talkgroup ID
Talkgroup Alias

2. Click **Save**.

11.1.2.6

Configuring Emergency Location in Unit Management

The radio emergency system can be set to three different Modes: **Emergency Alarm**, **Emergency Alarm w/ Voice Follow**, and **Emergency Alarm w/ Call**. The Emergency Location Trigger settings are dependent on the radio emergency system's Mode configuration.

For more information on radio emergency system configuration, see Radio Emergency Configuration Parameters on page 81.

Procedure:

1. Go to **MOTOTRBO Cadences** page.
2. Set the following fields based on the radio emergency system's Mode:

Option	Actions
The radio emergency system's Mode is set to **Emergency Alarm**	Set the **Emergency Cadence** field to `0`
The radio emergency system's Mode is set to **Emergency Alarm w/ Voice to Follow**	a. Set the **Emergency Cadence** field to `0` b. Set the **PTT Location Report Policy** field to `EmergencyPTT` c. Ensure that the radio is upgraded to M2020.2 or beyond.
The radio emergency system's Mode is set to **Emergency Alarm w/ Call**	a. Set the **Emergency Cadence** field to `0` b. Set the **PTT Location Report Policy** field to `EmergencyPTT` c. Ensure that the radio is upgraded to M2020.2 or beyond.

3. Click **Save**.

Postrequisites: In the Capacity Max system settings, select the **Enhanced Data Enabled** option – for more information, see MNIS Capacity Max Configuration Parameters on page 86.

11.1.2.7

Adding Device Range for MOTOTRBO Radios in a Carrier System Model

Each Orchestrate customer is assigned one contiguous radio ID range. It is recommended that the Carrier operator allocates sufficient device range during the initial assignment to prevent device deletion when adjusting the range at a later stage.

Procedure:

1. In CommandCentral Admin, go to **Application settings** → **Unit Management** → **Radio System**.
2. Ensure that the radio system intended for sharing is in a ready state and then select it.

3. Select the **Device Assignment** tab.
4. Click **Start Editing**.
5. Click **Add Range**.
6. Fill in **From** for the beginning of the device range, **To** for the end of the device range, and **Customer ID** for the CommandCentral Agency ID

   The CommandCentral Agency ID can be found at **Agency Overview** → **Agency Information** → **Agency ID** when logging on to the customer's CommandCentral agency.
7. Click **Add**.
8. After you finish adding all the device ranges, click **Done Edit**.
9. Click **Save Changes**.

11.1.2.8
Adding Talkgroup Range for MOTOTRBO Radios in a Carrier System Model

Each Orchestrate customer is assigned one contiguous talkgroup ID range and one contiguous radio ID range. The talkgroup range can only be added after the radio ID range has been added for the customer. It is recommended that the Carrier operator allocates sufficient device and talkgroup range during the initial assignment to prevent device and talkgroup deletion when adjusting the range at a later stage.

Procedure:

1. In CommandCentral Admin, go to **Application settings** → **Unit Management** → **Radio System**.
2. Ensure that the radio system intended for sharing is in a ready state and then select it.
3. Select the **Talkgroup Assignment** tab.
4. Click **Start Editing**.
5. Click **Add Range**.
6. Fill in **From** for the beginning of the talkgroup range, **To** for the end of the talkgroup range, and **Customer ID** for the CommandCentral Agency ID

   The CommandCentral Agency ID can be found at **Agency Overview** → **Agency Information** → **Agency ID** when logging on to the customer's CommandCentral agency.
7. Click **Add**.
8. After you finish adding all the talkgroup ranges, click **Done Edit**.
9. Click **Save Changes**.

11.1.3
MOTOTRBO Data Messaging System Requirements

Supporting data between Orchestrate and a MOTOTRBO system requires MOTOTRBO Network Interface Service (MNIS) for all system types, and Device Discovery and Mobility Service (DDMS) for IPSC and Capacity Plus system types.

Two different deployment platforms for MNIS and DDMS are available: standalone Windows and Edge Node. Starting from July 2023, the MNIS and DDMS can be hosted at the Motorola Edge Nodes, which are installed, maintained, and monitored by Motorola Solutions. To configure and enable Edge Node based MNIS and DDMS, use the Edge Node Management Portal. For more information, see "Motorola Edge Node Configuration" in the *Motorola Edge Node Installation Guide*. If you want to deploy MNIS and DDMS on a PC with Windows, refer to the following sections.

The Windows versions are found on Motorola On Line (MOL), and may use a VM with the following requirements:

- Supported Operating Systems: Windows 8.1 (32-bit), Windows 10 (64-bit), Windows Server 2016 (64-bit), Windows Server 2012 R2 (64-bit),
- Memory MNIS and DDMS: 1 GB and above required by host Operation System,
- Hard Disk MNIS and DDMS Programmer Install: 5 GB (Program Files and Database).

IMPORTANT: Do **not** deploy radios configured to support Orchestrate text messaging before DDMS is deployed. This can place a significant load on the system.

NOTE: Data Licenses (NAI or MNIS DGW) are not required to support Text Message Alarms with Orchestrate. However, other 3rd party applications require these licenses.

11.1.3.1
Installing Windows DDMS

After downloading from MOL, installation of DDMS follows the standard Windows application installation process. For non-Capacity Max systems, DDMS should be deployed on the same machine as MNIS.

11.1.3.2
Installing Windows MNIS

After downloading from MOL, installation of MNIS follows the standard Windows application installation process.

IMPORTANT: Windows MNIS can only work with Windows DDMS.

11.2
Capacity Max Voice and Radio Command Gateway

Supporting control signaling, for example emergency declaration and cancellation notification between Orchestrate and a MOTOTRBO Capacity Max system, requires a Voice and Radio Command (VRC) Gateway.

The VRC Gateway is hosted at the Capacity Max System Server (CMSS), which is shipped pre-loaded with the latest software versions. If it does not have the latest version, a software application (ESU) is provided to upgrade the software. For more information, see *Capacity Max System Release Upgrade Guide*.

Before the configuration of the VRC gateway, ensure that the Capacity Max MNIS VRC Gateway license is enabled in the Radio Management.

11.3
Accessing the Edge Node Management Portal

The Edge Node Management Portal is a part of the CommandCentral Admin application. The user account information for the customer is provided by Motorola Solutions. To obtain the Edge Node Management Consolidated Gateway Portal address, refer to the CA option available in the invoice. Depending on the CA option value, use one of the following URLs to access the Portal.

Table 8: Invoice CA Options

CA Option	CA Admin URL
CA03770AA	https://admin2.commandcentral.com

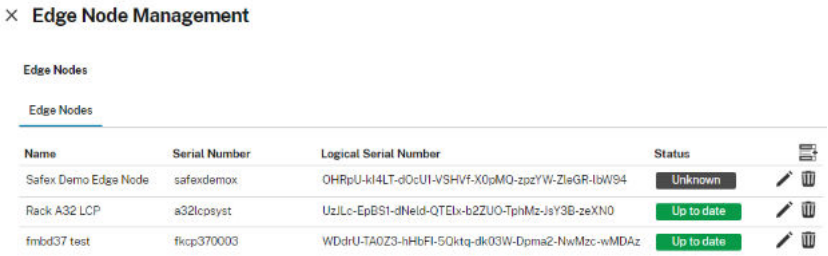
CA Option	CA Admin URL
CA03772AA	https://admin2.commandcentral.ca

Procedure:

1. Log on to the CommandCentral Admin application.
2. Go to **Application settings** and select **Edge Node Management**.

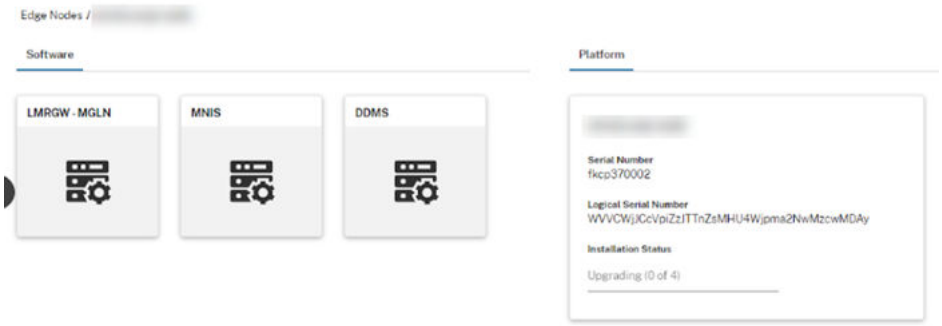
   The **Edge Node Management** dashboard displays. It contains all purchased and attached Motorola Edge Node devices.

   Figure 55: Edge Node Management Dashboard



3. Click on a specific Motorola Edge Node device to view applications.

   Figure 56: Edge Node Management Application View



4. To view the MNIS, DDMS, or LMRGW - MGLN application settings, select the corresponding tile.

11.4 Standard Radio and Repeater Configuration Parameters

In the majority of deployments, the MOTOTRBO Radio default values for the following parameters should be used. If an IP Address or UDP Port conflict exists on the network, those values can be modified in Customer Programming Software (CPS) 2.0 or Radio Management (RM).

- **Network** → **Radio Network** → **CAI Network**: default = 12 (radio and repeater)
- **Network** → **Radio Network** → **CAI Group Network**: default = 255 (radio and repeater)
- **Network** → **Services** → **ARS Radio ID**: MNIS Application ID
- **Network** → **Services** → **TMS Radio ID**: MNIS Application ID
- **Network** → **Services** → **TMS UDP Port**: default = 4007

The **CAI Network** and **CAI Group Network** must also match in the repeaters.

For non-Capacity Max systems, the Automatic Registration Service must be enabled for the radio. In Capacity Max it is automatically enabled.

- **Network** → **Services** → **ARS UDP Port**: default = 4005
- **Zone/Channel Assignment** → **Zone** → *<Zone_Name>* → **Position** → **ARS**
  - **On System Change** for single site deployments
  - **On System/Site Change** for multi-site deployments

NOTE: ARS Radio ID must be the same as both the TMS Radio ID and the MNIS Application ID (for information on the MNIS Application ID, see Windows DDMS Watcher Configuration on page 83).

11.5 Optimized Radio and Repeater Configuration Parameters

For Conventional Single Site and IP Site Connect deployments, enabling Enhanced Channel Access in the radios improves channel utilization by providing a robust collision detection mechanism. No configuration is needed in the repeaters, as this is automatically supported. This type of functionality is inherent in Capacity Plus and Capacity Max systems, so no configuration is required in those system types.

Channels → **Zone** → **Digital Channel** → **Enhanced Channel Access** (enable)

For all system types, the following optimizations are recommended:

Channels → Zone → Digital Channel → TX: Data Call Confirmed (enable)
Increases Individual Text Message Reliability.

General Settings → TX Preamble Duration (ms): 960 ms default
To minimize channel utilization per text message, set to 120 ms if receiving radios are not scanning other channels.

Channels → Zone → Digital Channel → Compressed UDP Header: (select DMR)
Minimizes channel utilization per text message.

You should assign an Alias Name for Orchestrate

Alias = `Orchestrate` or `Alert` (for example)
Call Type = **PC**
ID = *<MNIS ID>*

11.6 Radio Text Message Customization Configuration Parameters

The following is a reference to the location of the text message optimizations in CPS or RM.

General Settings → Menu → General → Message
Selecting this option allows the user to access messages through the menu.

General Settings → Alerts → Text Message Alert Tone Duration (min)
Default = 5 minutes

Text Message → Text Message Length
Short = 138 characters (supported by all MOTOTRBO radios that support text messaging) – recommended.

Long = 238 characters

Announcement → Announcement Type → Text to Speech

Requires Text to Speech license.

Only available on XPR7550e and XPR7580e.

11.7

Predefined Text Message for Radio User Acknowledgements

Users can unpause a workflow after addressing the situation by responding to the received Alarm text message with a text message of 1. A predefined text message may be configured in the device to make the response easier for the user. For non-keypad devices, this is required to enable User Acknowledgement functionality.

To enter the predefined text message, perform the following steps:

1. Open the **Text Message** folder and click **Add** to enter the predefined text message.
2. In the new message row, enter the numeric value of 1

11.8

Radio Emergency Configuration Parameters

The following is the required emergency configuration in Customer Programming Software (CPS) or Radio Management (RM).

Select Emergency System

For non-Capacity Plus Single Site or Multi Site system: **System** → **Digital Emergency Systems**.

For Capacity Plus Single Site or Multi Site system: **System** → **Capacity Plus Emergency Systems**.

Configure Emergency System

Alarm Type must **not** be disabled.

Mode must be set to **Emergency Alarm**, **Emergency Alarm w/ Call**, or **Emergency Alarm w/ Voice to Follow**. For information on the recommended Emergency Location Trigger setting based on the radio emergency system's Mode setting, see Configuring Emergency Location in Unit Management on page 76.

Impolite Retries must be set to the **Maximum**, which improves the emergency alarm reliability.

Polite Retries must be set to the **Maximum**, which improves the emergency alarm reliability.

Contact must be set to the targeted emergency talkgroup.

ACK Required setting (for conventional and IPSC system only) is recommended – if it is not checked, the radio continues sending emergency alarm until the configured number of attempts is reached, regardless if Emergency Alarm is received or not. This can delay the emergency declaration at Orchestrate.

Assign Emergency System to a Channel / Personality

For Conventional Single Site and IP Site Connect deployments: **Channels** → **Zone** → **Digital Channel** → **RX/TX** → **TX** → **Emergency System**.

For Capacity Plus Single Site deployments: **Channels** → **Zone** → **Capacity Plus Personality** → **RX/TX** → **TX** → **Emergency System**

For Capacity Plus Multi Site deployments: **Channels** → **Zone** → **Capacity Plus Personality (Linked)** → **RX/TX** → **TX** → **Emergency System**.

Assign a configured emergency system to each channel or personality.

Enable Emergency Alarm Acknowledgement in Supervisor Radio

For conventional and IPSC system, either a supervisor radio or a dispatch console application should acknowledge the emergency alarm if **ACK Required** is enabled in the Emergency System configuration.

For Conventional Single Site and IP Site Connect deployments: **Channels** → **Zone** → **Digital Channel** → **RX/TX** → **RX**.

For Capacity Plus Single Site deployments: **Channels** → **Zone** → **Capacity Plus Personality** → **RX/TX** → **RX** → **Emergency System**.

For Capacity Plus Multi Site deployments: **Channels** → **Zone** → **Capacity Plus Personality (Linked)** → **RX/TX** → **RX** → **Emergency System**.

Select **Emergency Alarm Indication**.

Select **Emergency Alarm Ack**.

Assign Radio Buttons to Trigger/Cancel Emergency

The emergency can be triggered from a predefined button on the radio or the attached accessory.

General Settings → **Control Buttons** → **Conventional Radio Buttons Portable**.

General Settings → **Control Buttons** → **Conventional Accessory Buttons Portable**.

Orange Button Short Press = Emergency On

Orange Button Long Press = Emergency Off

Enable Emergency Cancellation Notification

For Capacity Max system, the emergency cancellation notification is sent out based on the radio configuration in the Emergency System configuration.

Systems → **Signaling Systems** → **Digital**
Cancel Emergency = With Notification

11.9
Radio Outdoor Location Configuration Parameters

The following is the required location configuration in Customer Programming Software (CPS) or Radio Management (RM).

General → **General Settings** → **General**
Select **GNSS**.

General → **General Settings** → **Persistent LRRP Requests**
Leave unselected.

Verify if the GPS satellite dish icon is shown on the radio display.

11.10
DDMS Configuration

The following configurations are the same regardless of the MOTOTRBO system type.

NOTE: Starting from July 2023, the MNIS and DDMS can be hosted at the Motorola Edge Nodes, which are installed, maintained, and monitored by Motorola Solutions. To configure and enable Edge Node based MNIS and DDMS, use the Edge Node Management Portal. For more information, see “Motorola Edge Node Configuration” in the *Motorola Edge Node Installation Guide*. If you want to deploy DDMS on a PC with Windows, refer to the following sections.

11.10.1

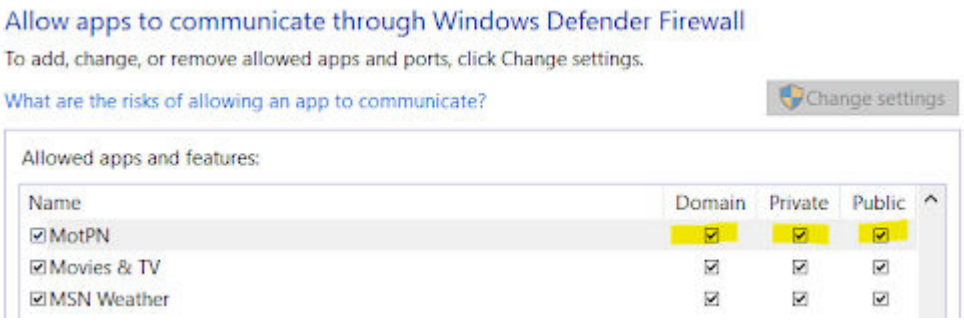
Configuring Windows Firewall Settings for DDMS running at Windows

DDMS running at Windows must be allowed on the Domain, Private, and Public networks, so that it can process the radio presence messages.

Procedure:

1. From the Windows Start Menu, open Windows Defender Firewall
2. In the **Windows Defender Firewall** window, from the left-hand menu, select **Allow an app or feature through Windows Defender Firewall**.
3. Scroll down to **MotPN**.
4. Click **Change settings**.
5. Ensure that **Domain**, **Private** and **Public** networks are checked.

   Figure 57: Allowed Apps and Features – MotPN



6. Click **Ok**.

11.10.2

Windows DDMS Watcher Configuration

Interface → Watcher Settings → Port Watcher = 3000 (default)

If there is a Port conflict, use the following procedure to change the Port number:

1. Stop the Service.
2. Change the value to the desired value.
3. Click the save button.
4. Restart the service.

NOTE: A help document is available through DDMS Configuration Utility.

Interfaces → ARS Settings → Device Refresh Time

The time period between device ARS requests in minutes.

11.11
MNIS Configuration

Depending on the MOTOTRBO system type, the MNIS configuration parameters may be different. Configure MNIS per the MOTOTRBO system type in the deployment.

NOTE: Starting from July 2023, the MNIS and DDMS can be hosted at the Motorola Edge Nodes, which are installed, maintained, and monitored by Motorola Solutions. To configure and enable Edge Node based MNIS and DDMS, use the Edge Node Management Portal. For more information, see “Motorola Edge Node Configuration” in the *Motorola Edge Node Installation Guide*. If you want to deploy MNIS on a PC with Windows, refer to the following sections.

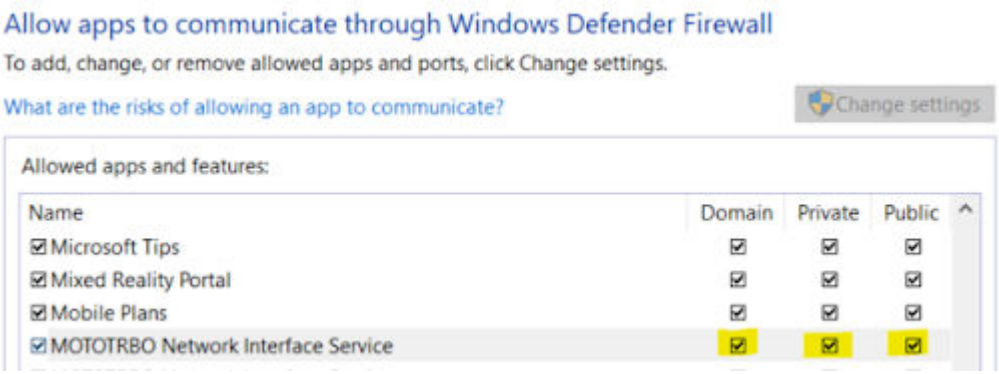
11.11.1
Configuring Windows Firewall Settings for MNIS running at Windows

MNIS running at Windows must be allowed on the Domain, Private, and Public networks, so that it can process the radio presence messages.

Procedure:

1. From the Windows Start Menu, open Windows Defender Firewall
2. In the **Windows Defender Firewall** window, from the left-hand menu, select **Allow an app or feature through Windows Defender Firewall**.
3. Scroll down to **MOTOTRBO Network Interface Service**.
4. Click **Change settings**.
5. Ensure that **Domain**, **Private** and **Public** networks are checked.

   Figure 58: Allowed Apps and Features – MNIS



6. Click **Ok**.

11.11.2
MNIS IPSC Configuration Parameters

MNIS Application ID = X

X can be any valid Radio ID value that is not already allocated to a radio.

X is the same value as ARS and TMS ID configured in the radios.

Group List → List1 → Group Call ID Ranges
The TG ID(s) to be used with Orchestrate.

Conventional Domain → Master IP Address
The IP Address of the IPSC Primary (Intermediary) Repeater.

Conventional Domain → Master UDP Port
The UDP Port of the IPSC Primary (Intermediary) Repeater.

Conventional Domain → Repeater Slot 1
Select **List 1** from above (only required if the TGs in List 1 are operating on slot 1).

Conventional Domain → Repeater Slot 2
Select **List 1** from above (only required if the TGs in List 1 are operating on slot 2).

NOTE: Even though only one Group List can be assigned to a slot, different group lists can be created and assigned to slot 1 or slot 2. The slot at the repeater can be local area channel or wide area channel.

11.11.3
MNIS Capacity Plus Single Site Configuration Parameters

MNIS Application ID = X

X can be any valid Radio ID value that is not already allocated to a radio.

X is same value as ARS and TMS ID configured in the radios.

Group List → List1 → Group Call ID Ranges
The TG IDs to be used with Orchestrate.

Capacity Plus → Master IP Address
The IP Address of the Capacity Plus Primary (Intermediary) Repeater.

Capacity Plus → Master UDP Port
The UDP Port of the Capacity Plus Primary (Intermediary) Repeater.

Capacity Plus → Group List
Select **List 1** from above.

11.11.4
MNIS Capacity Plus Multi Site Configuration Parameters

MNIS Application ID = X

X can be any valid Radio ID value that is not already allocated to a radio.

X is same value as ARS and TMS ID configured in the radios.

Group List → List1 → Group Call ID Ranges
The TG IDs to be used with Orchestrate.

Linked Capacity Plus → Master IP Address
The IP Address of the Linked Capacity Plus Primary (Intermediary) Repeater.

Linked Capacity Plus → LCP Domain 1 → Master UDP Port
The UDP Port of the Linked Capacity Plus Primary (Intermediary) Repeater.

Linked Capacity Plus → LCP Domain 1 → Sites
Add row for each repeater site in the system:

Site ID: ID of the repeater site
Group List: select List 1 from above

11.11.5
MNIS Capacity Max Configuration Parameters

Procedure:

1. In Radio Management (RM), edit Data MNIS Config by performing the following actions:
   a. Go to **Configuration** → **MNIS** → **MNIS System** → **Data Gateway Radio ID =** *<X>*

      where *<X>* can be any valid Radio ID value that is not already allocated to a radio.

   b. Go to **Green Gear Button** → **Manage** → **Capacity Max System Server Data** → **Subscriber Access Control** and add Data Gateway Row for Data Gateway.

      Device ID = **X** (the Data Gateway Radio ID)
      Select the check box for **Group Data Call** and **Individual Data Call** columns

   c. Go to **Green Gear Button** → **Manage** → **Capacity Max System Server Data** → **Talkgroup Site Association** and add row for talkgroup ID.

      Set **Allowed Sites** to be either **All Sites**, or edit the **Allowed Site List** so that the **Allowed** check box is selected for the Data Gateway site.

   d. Go to **Configuration** → **MNIS** → **MNIS System**

      If the **PTT Location Report Policy** in the **Unit Management Cadence** setting for the selected agency group is set as `everyPTT` or `emergencyPTT`, enable the **Enhanced Data Enabled** field.
2. Write the CMSS.

11.11.5.1
Sending Data MNIS Configuration from Radio Management into MNIS (Windows-based MNIS deployment)

Perform the following steps if you have MNIS deployed on a PC with Windows.

Procedure:

1. In the Radio View in RM, right-click the Data MNIS row.
2. Select **Export** → **GWCFGX**.
3. Save the file to the computer's Desktop.
4. Open the MNIS Data Gateway Configuration Utility.
5. Go to **Configuration** → **Import**.
6. Select the MNIS configuration file that you saved to the computer's Desktop.
7. Go to **Configuration** → **Select Active Configuration**.
8. Select the MNIS configuration that you just imported.

11.11.5.2
Sending Data MNIS Configuration from RM into MNIS (Edge Node-based MNIS deployment)

Perform the following steps if you have MNIS deployed on Edge Node.

Procedure:

1. In the Radio View in RM, right-click the Data MNIS row.

2. Select **Export** → **GWCFGX**.
3. Save the file to the computer's Desktop.
4. Open the MNIS Data Gateway Configuration Utility.
5. Access the MNIS application in the Edge Node Management Portal.

   For more information, see Accessing the Edge Node Management Portal on page 78.
6. Select the **All Configurations** tab, then select the drop-down menu from the type of system for which you want to add a new configuration for MNIS (**Conventional**, **Capacity Plus Single site**, **Capacity Plus Multisite**, or **Capacity Max**).
7. Perform the following actions:
   a. To import new configuration of MNIS for the Capacity Max system, select **Click to import configuration**.
   b. Complete the following fields:

      Configuration Name
      Configuration Description (optional)
   c. Select **Add File** and load the **GWCFGX** file with the MNIS configuration that was earlier exported from Radio Management.
   d. To import this configuration, select **Import**.

   In the **All Configurations** tab at the drop-down menu for the system type for which you created the new configuration you should see a box for the configuration with the name that you provided in the **Configuration Name** field.
8. To start the MNIS application, in the **Dashboard** under **Status** select the **three dots** icon, then select **Start**.
9. To activate the new MNIS configuration, in the top-right corner of the box for the new configuration click the vertical ellipsis button and select **Set as Active**.

   The configuration is loaded. In the **Dashboard** tab for MNIS, the `Running` status should display. In the **Selected Configuration** section, the box with the name of the new configuration should display.

   NOTE: The MNIS application must be in the `Running` state for the active configuration to display in the **Dashboard**.

11.12 Configuring Capacity Max Voice and Radio Command Gateway

To get the emergency declaration and cancellation notification from the MOTOTRBO radio at Capacity Max system without an emergency location report, the Voice and Radio Command (VRC) must be enabled with license and configured. The VRC talkpath license is not required.

For more information, see “MNIS VRC Gateway Configuration” in *Capacity Max Installation and Configuration Manual*.

Set the VRC Gateway’s IP address and TCP port at the MGLN System Management portal.

Procedure:

1. Log on to the CommandCentral Admin application.
2. Go to **Application settings** and select **MGLN Systems Management.**

The **MGLN Systems Management** dashboard displays. It contains all MGLN Systems the customer has access to.

3. To view the system status, info, settings and provisioning, click on a specific MGLN System.
4. Select **Settings** → **VRC**.
5. Set the VRC IP address and TCP port.

   Ensure that the VRC TCP port matches with the settings at VRC Gateway: **MNIS Network** → **Server TCP Port**.

11.13 MOTOTRBO Software Version Requirements

The following are the software version requirements for MOTOTRBO systems to integrate with Orchestrate:

- Repeaters, Radios and CMSS – all software versions underneath current Essential MOTOTRBO support agreements are supported.
- Windows DDMS – software version 3.90.5001.0 or later.
- Windows MNIS – software version 2021.04 or later.
- Radio software version M2022.02 or later is required to support MOTOTRBO emergency as an Orchestrate trigger.
- Radio software version M2022.01 or later is required to support MOTOTRBO Group Text Message Service (TMS) Reliability.
- Capacity Max Voice and Radio Command Gateway (VRC) software version M2020.02 or later is required, along with a valid license enabled, to support MOTOTRBO emergency cancellation notification.

11.14 MOTOTRBO Maintenance

Over time it is possible that cameras, radios or talkgroups are added to the deployment.

The following are some maintenance considerations.

Deleting MOTOTRBO devices

1. Set **Auto Create Enabled** to **Disabled**.
2. Manually delete the desired Devices.
3. Manually delete the desired Units associated with the deleted Devices.
4. When all the desired Devices are deleted, set **Auto Create Enabled** to **Enabled**.

Within one minute, the deleted Unit is no longer present as an available Action in Orchestrate.

If the Action is deployed in a workflow that is not part of a group, then the Action is flagged and the user has the option to delete or replace the Action.

If the Action is deployed in a workflow that is part of a group then the Action is removed from the group with no indication.

NOTE:
Device deletion is not supported through a CSV file.

If only the Unit is deleted, when the device becomes present, another Unit is created for the device.

If only the Device is deleted, the Unit Action is still present in Orchestrate, and no indication is given that workflows incorporating the Unit will fail.

Changing MOTOTRBO Device Alias

1. Set **Auto Create Enabled** to **Disabled**.
2. Manually delete the desired Devices.
3. Manually delete the desired Units associated with the deleted Devices.
4. When all Devices are deleted, set **Auto Create Enabled** to **Enabled**..
5. Verify in Orchestrate that Action Node is removed.
6. Set **Auto Create Enabled** to **Disabled**.
7. Add device manually or with CSV upload.
8. Set **Auto Create Enabled** to **Enabled**.
9. When Action Node appears in Orchestrate, replace in workflows the Action Node with the previous Alias with the Action Node with the new Alias.

NOTE: There is a known issue that after the device alias is changed for an existing Action Node in Orchestrate, the Action Node may disappear from Orchestrate. The workaround is to power cycle the device to make it appear in Orchestrate.

Deleting MOTOTRBO Talkgroups

In CommandCentral Admin, click on the garbage can icon for the Talkgroup to be deleted.

Changing MOTOTRBO Talkgroup Alias

Do **not** directly change the Talkgroup Alias in CommandCentral Admin, as this may result in an inoperable workflow. Instead, perform the following steps:

1. Delete the MOTOTRBO Talkgroup.
2. Add a Talkgroup with the new Alias per the process defined in CommandCentral Unit Management on page 73.

Chapter 12

WAVE PTX Integration and Configuration

After the WAVE PTX devices are boarded at the WAVE PTX OnCloud portal, they must also be provisioned into CommandCentral Admin before they show in the Orchestrate Action list.

For more information on WAVE PTX devices administration at the WAVE PTX OnCloud portal, see *WAVE PTX Administrator* training.

At the initial activation of Orchestrate with WAVE PTX Alert, you receive a confirmation email with a CSV file of all WAVE PTX devices.

If you intend to add new devices for Orchestrate WAVE PTX Alert after the initial activation, ensure that the new devices are activated on WAVE PTX OnCloud, then ask the WAVE PTX Partner to send an email to waveptx.admin@motorolasolutions.com, with the following information:

- Phone number of an existing WAVE PTX device under the WAVE PTX Agency
- WAVE PTX Partner Contact Email
- Offer Name as “Orchestrate WAVE PTX Alert”

After the activation is finished, you receive a confirmation email with a CSV file of all WAVE PTX devices.

CommandCentral WAVE PTX Provisioning

CommandCentral Admin supports multiple use cases which can include linking multiple Devices to a Unit. However, in an Orchestrate deployment, there is a one-to-one relationship between a Device and a Unit.

For an overview of the provisioning process of different types of devices and systems, including WAVE PTX devices, refer to the *CommandCentral Aware Location Tracking Administration* training.

NOTE: You should only manually add Devices. Do **not** manually enter Units.

Although only some of the WAVE PTX devices are planned to receive the Orchestrate alarm alert, all the devices are activated and can be added in CommandCentral Admin.

12.1 Creating Agency Groups for WAVE PTX Devices

Procedure:

1. In CommandCentral Admin, go to **Application settings** → **Unit Management** → **Agency Groups**.
2. Click **Add Agency Group**.
3. In **Agency** tab, fill in **Agency Group ID**.

   Agency Group ID can represent the useful groupings of business rules.
4. In **WAVE** tab, fill in **WAVE Group ID**.

   This value is provided as the WAVE PTX customer domain name in the waveptx.admin's confirmation email.
5. Click **Save**.

   NOTE: If multiple Agency Groups are assigned with the same WAVE PTX Group ID, the WAVE PTX devices must be added with a specific Agency Group. This can be done manually or by using CSV file, instead of by using Auto Create Unit.

12.2
Adding WAVE PTX Devices Through Auto Create Unit

Procedure:

Enable Auto Create Unit at the Agency Group.

A Unit and a Device are automatically created in CommandCentral for a device when it becomes present on the system. The name of the Unit is the same as the WAVE PTX Device ID. To update the device alias and the name of the Unit see Changing WAVE PTX Device Alias Manually on page 94.

NOTE:
There is a known issue that after the non-text capable device (for example TLK) alias is changed, the non-text capable device may appear as an Action Node at Orchestrate. The workaround is to power cycle the device to make it disappear from Orchestrate. It is recommended to add the devices manually or through CSV file with the device alias, and then enabling Auto Create Unit at the Agency Group.

12.3
Adding WAVE PTX Devices Through CSV File

Procedure:

1. Disable Auto Create Unit.
2. Upload the CSV file which contains the following information for each device:

   Kodiak Device ID (10 or 15 digitals)
   Kodiak Device Alias (optional)
   Agency Group ID
   Description (optional)

   The Kodiak Device ID and the Kodiak Device Alias can be retrieved from the CSV file in the activation confirmation email.

   The Agency Group ID can be found on the Agency Groups page of the CommandCentral Admin Unit Management portal.

   Figure 59: Example of a CSV File for Adding Wave PTX Devices

	A	B	C	D	E	F
1	Kodiak Device ID*	Kodiak Device Alias	Agency Group ID*	Description	Import Status (For Server Use Only)	
2	19193028888	User2	WAVE-Agency-Group-1			
3						

3. Enable Auto Create Unit.

   A Unit is automatically created in CommandCentral for a device when it becomes present on the system. The name of the Unit is the same as the device's WAVE PTX Device Alias in the CSV file.

   Within 10 minutes of the device becoming present on the system, an Action for the created Unit appears in Orchestrate.

12.4
Adding WAVE PTX Devices Manually

Procedure:

1. Disable Auto Create Unit.

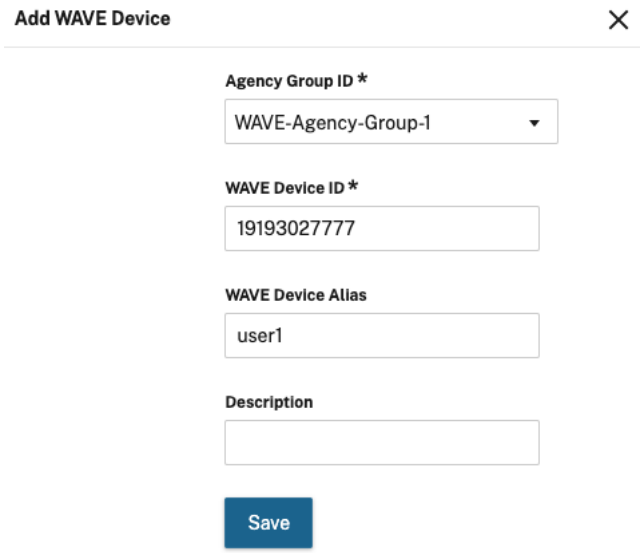
2. Enter the following information for each device manually:

   Agency Group ID
   WAVE Device ID (10 or 15 digitals)
   WAVE Device Alias
   Description (optional)

   The Kodiak Device ID and the Kodiak Device Alias can be retrieved from the CSV file in the activation confirmation email.

   The Agency Group ID can be found on the Agency Groups page of the CommandCentral Admin Unit Management portal.

   Figure 60: Adding Wave PTX Device Manually



3. When all Devices are added, enable Auto Create Unit.

   A Unit is automatically created in CommandCentral for a device when it becomes present on the system. The name of the Unit is the same as the device's WAVE PTX Device Alias in the CSV file.

   Within 10 minutes of the device becoming present on the system, an Action for the created Unit appears in Orchestrate.

12.5 Enabling WAVE PTX Emergency Location Trigger

Procedure:

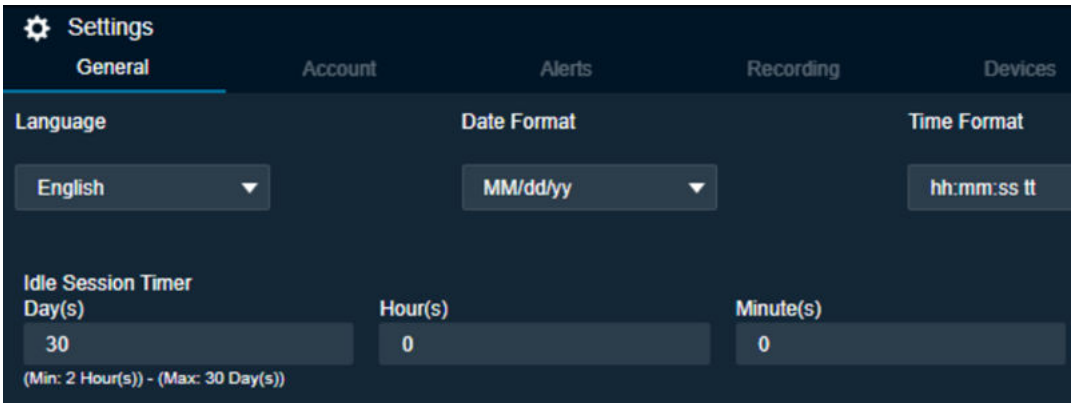
1. Go to **Cadences/WAVE** page.
2. Select the Agency Group which has been created for WAVE PTX devices.
3. Set the **Emergency Cadence** to a non-zero value.

12.6 WAVE PTX Emergency Configuration Parameters

To successfully trigger the emergency from a WAVE PTX device, at least one group member must be in the **Available** or **Do Not Disturb** state. It is recommended that the WAVE PTX device initiates the emergency targeted to a Dispatch talkgroup. At least one of the dispatch users should be always logged in the WAVE

PTX Dispatch application. Setting the **Idle Session Timer** in the WAVE PTX Dispatch application can help the dispatch user to stay online up to 30 days without re-login, as shown in the following figure.

Figure 61: Idle Session Timer Settings



12.7 Creating Dispatch Talkgroups

Procedure:

1. Create a dispatcher user.

   Refer to “Adding a Mobile, Tablet, or WAVE PTX Dispatch User” in the *WAVE PTX Portal User Guide*.
2. Create a dispatch talkgroup.

   Refer to “Creating a Talkgroup” in the *WAVE PTX Portal User Guide*.
3. Assign the dispatcher user and the WAVE PTX device to the dispatch talkgroup.

   Refer to “Associate Dispatchers and Users to Talkgroups” in the *WAVE PTX Portal User Guide*.

12.8 Enabling Emergency Initiation for WAVE PTX Devices

Procedure:

1. Go to **Users** page.
2. Under **CONTACTS AND FEATURES**, click **Manage**.
3. Click **Features**.
4. Set **Allow Emergency Initialization** to **Yes**.
5. Set **Destination** to **Admin Selected Contact or Talkgroup**.
6. Select **Talkgroup** for Primary.
7. Select a dispatch talkgroup from the list.
8. Click **Save**.

NOTE: For more details, refer to “Features Authorization” in the *WAVE PTX Portal User Guide*.

12.9
WAVE PTX Maintenance Considerations

Over time it is possible that new devices are added to the deployment.

The following are some maintenance considerations.

Deleting WAVE PTX Devices

The operation of deleting devices should be conducted when a device is lost or subscription is no longer active.

1. Manually delete the desired Devices.
2. Manually delete the desired Units associated with the deleted Devices.

Within 10 minutes, the deleted Unit is no longer present as an available Action in Orchestrate.

If the Action is deployed in a workflow that is not part of a group, then the Action is flagged and the user has the option to delete or replace the Action.

If the Action is deployed in a workflow that is part of a group, then the Action is removed from the group with no indication.

NOTE:
Device deletion is **not** supported through a CSV file.

If only the Unit is deleted, when the device becomes present, another Unit is created for the device.

If only the Device is deleted, the Unit Action is still present in Orchestrate, and no indication is given that workflows incorporating the Unit will fail.

Changing WAVE PTX Device Alias Manually

Manually update the WAVE PTX Device Alias in the WAVE PTX Device record.

The name of the Unit in CommandCentral is automatically updated as the Device's WAVE PTX Device Alias in CommandCentral. The default display name of Action Node in Orchestrate is also automatically updated.

NOTE: There is a known issue that after the non-text capable device (for example TLK) alias is changed, the non-text capable device may appear as an Action Node at Orchestrate. The workaround is to power cycle the device to make it disappear from Orchestrate.

Changing WAVE PTX Device Alias Through CSV File

Upload the CSV file which contains the following information for each device:

Kodiak Device ID (10 or 15 digitals)
Agency Group ID
Kodiak Device Alias (optional)
Description (optional)

The Kodiak Device ID and Kodiak Device Alias can be retrieved from the CSV file in the activation confirmation email.

The Agency Group ID can be found on the Agency Groups page of the CommandCentral Admin Unit Management portal.

The name of the Unit in CommandCentral is automatically updated as the Device's WAVE PTX Device Alias in CommandCentral. The default display name of Action Node in Orchestrate is also automatically updated.

NOTE: There is a known issue that after the non-text capable device (for example TLK) alias is changed, the non-text capable device may appear as an Action Node at Orchestrate. The workaround is to power cycle the device to make it disappear from Orchestrate.

Chapter 13

ASTRO Integration and Configuration

After the ASTRO devices are boarded at the WAVE PTX OnCloud portal for inter-operation, they must also be provisioned into CommandCentral Admin before they show in the Orchestrate Action list.

At the initial activation of Orchestrate with ASTRO Alert, you receive a confirmation email with a CSV file of all ASTRO devices and the Critical Connect customer domain Name.

If you intend to add new devices for Orchestrate ASTRO Alert after the initial activation, ask the Motorola Solutions ASTRO Sales Account Manager to send an email to waveptx.admin@motorolasolutions.com with the following information:

- ASTRO Critical Connect Customer Domain Name
- Network ID, System ID and Device ID of an existing ASTRO® P25 device under the ASTRO Critical Connect Agency
- Offer Name as **Orchestrate ASTRO Alert**

After the activation is finished, you receive a confirmation email with a CSV file of all ASTRO devices.

CommandCentral ASTRO Provisioning

CommandCentral Admin supports multiple use cases which can include linking multiple Devices to a Unit. However, in an Orchestrate deployment, there is a one-to-one relationship between a Device and a Unit.

For an overview of the provisioning process of different types of devices and systems, including Astro devices, refer to the *CommandCentral Aware Location Tracking Administration* training.

NOTE: You should only manually add Devices. Do **not** manually enter Units.

Although only some of the ASTRO devices are planned to receive the Orchestrate alarm alert, all the devices are activated and can be added in CommandCentral Admin.

13.1 Creating Agency Groups for ASTRO Devices

Procedure:

1. In CommandCentral Admin, go to **Application settings** → **Unit Management** → **Agency Groups**.
2. Click **Add Agency Group**.
3. In **Agency** tab, fill in **Agency Group ID**.

   Agency Group ID can represent the useful groupings of business rules.
4. In **WAVE** tab, fill in **WAVE Group ID**.

   This value is provided as the ASTRO Critical Connect customer domain name in the waveptx.admin's confirmation email.
5. Click **Save**.

   NOTE: If multiple Agency Groups are assigned with the same WAVE PTX Group ID, the ASTRO devices must be added with a specific Agency Group. This can be done manually or by using CSV file, instead of by using Auto Create Unit.

13.2 Adding ASTRO Devices Through Auto Create Unit

Procedure:

Enable Auto Create Unit at the Agency Group.

A Unit and a Device are automatically created in CommandCentral for a device when it becomes present on the system. The name of the Unit is the same as the ASTRO Device ID. To update the device alias and the name of the Unit see Changing ASTRO Device Alias Manually on page 98.

NOTE: There is a known issue that after the device alias is changed for an existing Action Node in Orchestrate, the Action Node may disappear from Orchestrate. It is recommended to add the devices manually or through CSV file with the device alias, and then enabling Auto Create Unit at the Agency Group.

13.3 Adding ASTRO Devices Through CSV File

Procedure:

1. Disable Auto Create Unit.
2. Upload the CSV file which contains the following information for each device:

   Network ID (between 1 and 1048574)
   System ID
   Radio ID
   Agency Group ID
   Serial Number (optional)
   Radio Alias (optional)
   Smart Connect Enabled (set to **FALSE**)
   Location Enabled (set to **TRUE**)
   Sensor Enabled(For LRRP Only) (optional, set to **FALSE**)
   Description (optional)

   The Network ID, System ID, Radio ID and the Radio Alias can be retrieved from the CSV file in the activation confirmation email.

   The Agency Group ID can be found on the Agency Groups page of the CommandCentral Admin **Unit Management** portal.

   Figure 62: Example of a CSV File for ASTRO Devices

Network ID*	System ID*	Radio ID*	Agency Group ID*	Serial Number	Radio Alias	SmartConnect Enabled*	Location Enabled*	Sensor Enabled(For LRRP Only)	Description
781841	64	106	kodiakagencygroup123			FALSE	TRUE	FALSE	
781841	64	84	kodiakagencygroup123			FALSE	TRUE	FALSE	
781841	64	300	kodiakagencygroup123			FALSE	TRUE	FALSE	

3. Enable Auto Create Unit.

   A Unit is automatically created in CommandCentral for a device when it becomes present on the system. The name of the Unit is the same as the device's Radio Alias in the CSV file.

   Within 10 minutes of the device becoming present on the system, an Action for the created Unit appears in Orchestrate.

13.4
Adding ASTRO Devices Manually

Procedure:

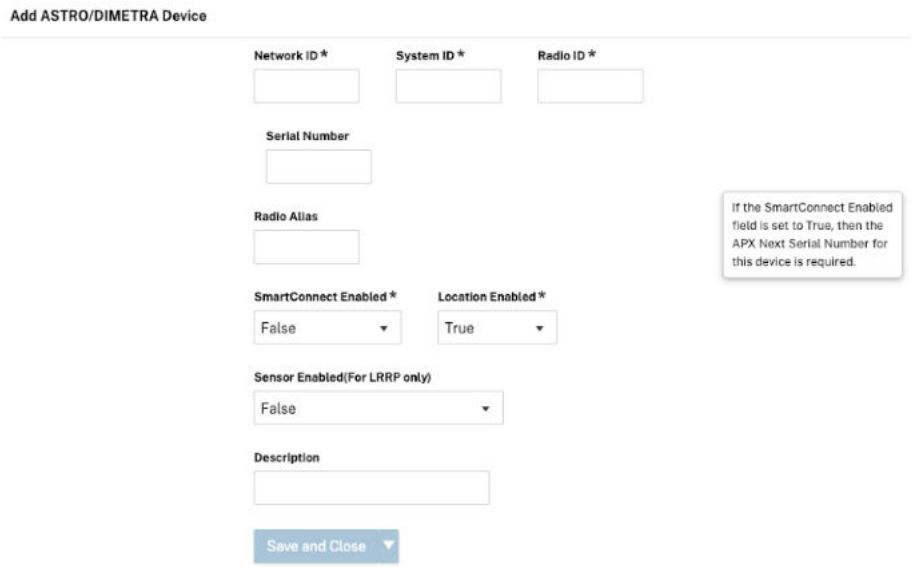
1. Disable Auto Create Unit.
2. Enter the following information for each device manually:

   Agency Group ID
   Network ID (between 1 and 1048574)
   System ID
   Radio ID
   Serial Number (optional)
   Radio Alias (optional)
   Smart Connect Enabled (set to **FALSE**)
   Location Enabled (set to **TRUE**)
   Sensor Enabled(For LRRP Only) (optional, set to **FALSE**)
   Description (optional)

   The Network ID, System ID, Radio ID and the Radio Alias can be retrieved from the CSV file in the activation confirmation email.

   The Agency Group ID can be found on the Agency Groups page of the CommandCentral Admin **Unit Management** portal.

   Figure 63: Adding ASTRO Devices Manually



3. When all Devices are added, enable Auto Create Unit.

   A Unit is automatically created in CommandCentral for a device when it becomes present on the system. The name of the Unit is the same as the device's Radio Alias in the CSV file.

   Within 10 minutes of the device becoming present on the system, an Action for the created Unit appears in Orchestrate.

13.5
Enabling ASTRO Emergency Location Trigger

Procedure:

1. Go to **Cadences** → **ASTRO/DIMETRA** page.
2. Select the Agency Group which has been created for ASTRO devices.
3. Set the **Emergency Cadence** to a non-zero value.

   NOTE: There is a known issue that the change of the emergency cadence is not propagated to the device. Keep the **Emergency Cadence** value to the default value of 30 seconds.

13.6
ASTRO Emergency Configuration Parameters

Contact your local Motorola Solutions account manager to ensure that the emergency notification related configurations have been set up.

13.7
ASTRO Devices Maintenance Considerations

Over time it is possible that new devices are added to the deployment.

The following are some maintenance considerations.

Deleting ASTRO Devices

The operation of deleting devices should be conducted when a device is lost or subscription is no longer active.

1. Manually delete the desired Devices.
2. Manually delete the desired Units associated with the deleted Devices.

Within 10 minutes, the deleted Unit is no longer present as an available Action in Orchestrate.

If the Action is deployed in a workflow that is not part of a group, then the Action is flagged and the user has the option to delete or replace the Action.

If the Action is deployed in a workflow that is part of a group, then the Action is removed from the group with no indication.

NOTE:
Device deletion is **not** supported through a CSV file.

If only the Unit is deleted, when the device becomes present, another Unit is created for the device.

If only the Device is deleted, the Unit Action is still present in Orchestrate, and no indication is given that workflows incorporating the Unit will fail.

Changing ASTRO Device Alias Manually

Manually update the ASTRO Radio Alias in the ASTRO/Dimetra Device record.

The name of the Unit in CommandCentral is automatically updated as the Device's ASTRO Radio Alias in CommandCentral. The default display name of Action Node in Orchestrate is also automatically updated.

NOTE: There is a known issue that after the device alias is changed for an existing Action Node in Orchestrate, the Action Node may disappear from Orchestrate. The workaround is to power cycle the device to make it re-appear in Orchestrate.

Changing ASTRO Device Alias Through CSV File

Upload the CSV file which contains the following information for each device:

Network ID (between 1 and 1048574)
System ID
Radio ID
Agency Group ID
Serial Number (optional)
Radio Alias (optional)
Smart Connect Enabled (set to **FALSE**)
Location Enabled (set to **TRUE**)
Sensor Enabled(For LRRP Only) (optional, set to **FALSE**)
Description (optional)

The Network ID, System ID, Radio ID and the Radio Alias can be retrieved from the CSV file in the activation confirmation email.

The Agency Group ID can be found on the Agency Groups page of the CommandCentral Admin **Unit Management** portal.

The name of the Unit in CommandCentral is automatically updated as the Device's ASTRO Radio Alias in CommandCentral. The default display name of Action Node in Orchestrate is also automatically updated.

NOTE: There is a known issue that after the device alias is changed for an existing Action Node in Orchestrate, the Action Node may disappear from Orchestrate. The workaround is to power cycle the device to make it re-appear in Orchestrate.

Chapter 14

VehicleManager Enterprise Cloud Service Setup

Procedure:

1. Log on to VehicleManager Enterprise Administrator Endpoint.
2. Go to **Site Management** and verify if the Site already exists.

Option	Action
The Site is available.	Set up Proxy User with Target Alert Service (TAS) Alert permissions.
The Site does not exist.	Review the Purchase Order (PO) or the Sales Order (SO) to verify if the VehicleManager Enterprise Customer Form (VCF) is available, and perform one of the following actions: • If VCF is available, set up the Site. • If VCF is not available, contact Accounts Management or the Regional Sales Manager (RSM) associated with the account.

3. Return to **Site Management**.
4. Set up a mapping to the Orchestrate Integration by using the CommandCentral Agency ID provided by Orchestrate.
5. Generate a single alert that can be mapped in Orchestrate.

Chapter 15

Rave Panic Setup

Rave Panic Button is a smartphone mobile application which can be used to instantly communicate emergency to 9-1-1, while simultaneously being connected to first responders and the necessary personnel.

IMPORTANT:
You must be designated as a BETA customer for Rave Panic in Orchestrate.

Rave 9-1-1 is **not** compatible with the initial release.

15.1 Configuring Rave Panic

Prerequisites: Ensure that your Rave Panic Button is set up in Rave.

Procedure:

1. In Orchestrate, copy your Agency name and Agency ID.

   This information can be found under **Information** icon in the header bar.
2. Go to Rave Facility and paste your Agency name and Agency ID under **Integrations** into the appropriate field.
3. For BETA, contact `techsupport@ravemobilesafety.com` and request to make the final connection.
4. Click **Save**.

   A toast message should appear in Rave confirming the connection.
5. Verify that Rave Panic Triggers are discovered and available in Orchestrate.

   Discovery will occur within five minutes.
6. **NOTE:** When using Rave Panic, it is recommended that Orchestrate Suppression is toggled off. This eliminates a risk of repeat alarms of the same type being missed due to suppression behavior.

   Toggle off the suppression by performing the following actions:

   a. Go to Orchestrate.
   b. From the left-hand menu select **Settings**.
   c. Disable the **Workflow suppression** toggle.
7. Create and test a workflow that uses Rave Panic Triggers.

   No configuration internal to Orchestrate is required for Rave Panic, so the **Configure** button in the Rave Panic Details page is disabled. This has no impact on the Rave connection.

Chapter 16

Rave Alert Setup

Rave Alert is a FedRAMP-authorized mass notification system that enables the customers to quickly send messages, including desktop notifications.

With Rave Alert you can send a message in an emergency through text, email, desktop, voice, IPAWS-OPEN, WebEOC, public address systems, social media, digital signage, Smart911 app, and more.

16.1 Configuring Rave Alert

Procedure:

1. In Orchestrate, copy your Agency ID.

   This information can be found under **Information** icon in the header bar.
2. Log on to Rave.
3. From the left-hand menu, select **System** → **Integration** → **Motorola Solutions**.
4. Under **Agency ID**, paste your Agency ID and click **Continue**.

   Your agency name is auto-populated based on your provided Agency ID.
5. Click **Save**.
6. Verify that Rave Alert Actions are discovered and available in Orchestrate.

   Discovery will occur within five minutes.
7. Create and test a workflow that uses Rave Alert Actions.

Chapter 17

System Configuration and Verification

17.1 Orchestrate Rules Configuration

You must create alarms in Unity Video, and then you must onboard MOTOTRBO radios, talkgroups, and WAVE PTX devices. When this is complete, the Ally, the configured alarms, the MOTOTRBO radios and talkgroups, and the WAVE PTX devices are available in Orchestrate for custom workflows creation.

For more information, see *Orchestrate User Guide*.

17.2 Triggering Alarms

Testing a workflow can be performed by:

- manually triggering the Alarm (for example, opening a door),
- or configuring a keystroke on a Unity Client to trigger an Alarm, and pressing the key.

  NOTE: This is not supported with Unity Cloud Services.

Perform the following steps to configure a keystroke to activate an Alarm:

Procedure:

1. In the Unity Client, configure an alarm that triggers on an External Software Event. The integration user must be an alarm recipient.
2. Add a Rule to trigger the alarm using a keyboard command by performing the following actions:
   a. In the **Setup** tab, click **Rules**.
   b. Click **Add** and then select **User Events** → **Custom keyboard command triggered**.
   c. Click the **number 0** to change the keyboard command. Click **Next**.
   d. Select **AlarmActions** → **Trigger an alarm**.
   e. Click **an alarm** and select the alarm from step 1. Click **Next**.
   f. Click **Next** again and enter a rule name and description. Click **Finish**.
3. In the **New Task menu**, under **View**, click **Alarms**.
4. Trigger the alarm by performing the following actions:
   a. Press `Ctrl + K`
   b. Enter the keyboard command and then press `Enter`
5. Verify that the alarm appears in the **Alarms** tab.

17.3 Action Verification

When a workflow is created in Orchestrate it can be tested and verified.

NOTE:
After saving a workflow, it can take up to one minute for it to become active.

When an Alarm is triggered, another triggering of the Alarm does not result in a new Action for 10 minutes, unless a User Response text message of “1” is sent from a non-Ion MOTOTRBO radio. The WAVE PTX and MOTOTRBO Ion User Response does not unsuppress the 10 minute suppression period.

17.4 Optimizing Unity Video Alarms

When the Orchestrate system has been operationally verified with the test alarms in the checklist, the customer’s workflows can be deployed. One aspect is configuring the workflow triggers for Unity Access and Unity Video Events to Unity Video Alarms in the Unity Video. In general, a good system deployment does not send Alarm text messages to the same radios frequently.

Users will have a threshold where receiving the Text Alarm transitions from beneficial to nuisance, and another threshold where it transitions from nuisance to unusable. Before the customer’s desired workflows are created, it is recommended to evaluate the frequency of occurrence of each Unity Video Alarm over a period of time. This should help to limit customer overload (too many alarms) when the actual workflows are enabled. Even with a 10 minute duplicate Alarm suppression period, unless released earlier with a user text message response of 1, receiving an Alarm every 10 minutes may be considered a nuisance.

The following process is recommended to evaluate and optimize the configured Alarms so that they are beneficial to the radio users.

Procedure:

1. In the Unity Video, create all of the customer’s desired Alarms with Rules.
2. In CommandCentral Admin, enter the **Unit Management** section, and enter a placeholder radio that is not on the system.

   It should be either a radio that will be powered off through the entire evaluation/optimization phase, or a radio that does not even exist in the system.
3. Create a workflow for each Unity Video Alarm to the placeholder radio.
4. Allow the system to run for at least one day.
5. From Orchestrate, export logged workflow data to a CSV file.
6. Input the CSV file into a graphing tool.
7. Examine the number and time of occurrences for each Unity Video Alarm.
8. Modify alarm (for example the time duration of door open or beam crossing location) for each alarm where the occurrence is deemed excessive.
9. Return to step 1 until all Alarm occurrences are deemed acceptable, then proceed to step 10.
10. Create and start all customer desired workflows.

    The purpose of using the placeholder radio is to keep Alarm Text Message traffic off of the system until the desired frequency of Alarms is obtained. Excessive Alarm Text Message traffic may impact voice channel access. The MOTOTRBO system design tools can then be used to determine channel loading with the text message alarms when the text message frequency is known.

    The following figure is an example of two Motion Detect Alarms after the exported CSV file is input into a graphing tool. The total number of triggered alarms for either of the two alarms is

the summation of **completed**, **in progress** and **suppressed**. Duplicate alarms are suppressed for 10 minutes or until a user response text message of 1 is received. In this example, the Door 51 Motion Alarm can be triggered hundreds of times per busy hour. This may be an extreme example, but it demonstrates what to look for when optimizing an alarm for a customer's desired frequency of occurrence.

Figure 64: Unity Video Alarm Occurences

Sheet 1

				Event Header Label / Actionable Event Status					
				Null	Door 51 Motion Alarm			Door 53 Motion Alarm		
Year of Eve..	Month of E..	Day of Even..	Hour of Eve..	Null	COMPLE..	IN_PRO..	SUPPRE..	COMPLE..	IN_PRO..	SUPPRE..
2021	June	24	23		2	4	24	5	10	79
		25	0		3	6	7	3	6	13
			1		3	6	5	4	8	14
			2		2	4	2	1	2	3
			3		2	4	6	4	8	16
			4		1	2	1	1	2	9
			5		2	4	2	2	4	4
			6		1	2	7	2	4	4
			7		1	2	9	1	2	3
			8		2	4	4	3	6	19
			9		5	10	19	4	8	32
			10		3	6	11	4	8	28
			11		1	2	13	2	4	14
			12		5	10	43	4	8	36
			13		5	10	49	5	10	51
			14		4	8	40	5	10	75
			15		6	12	336	5	10	63
			16		6	12	428	5	10	51
			17		5	10	63	5	10	97
			18		2	4	12	3	6	23
		28	14		5	12	35	5	12	41
			15		4	8	36	5	10	105
			16		3	6	55	3	6	115
		29	20					1	2	
			21		5	10	63	5	10	99
			22		5	10	43	5	10	69

Chapter 18

Troubleshooting

The following sections discuss how to solve common issues that may occur while using Orchestrate.

18.1 Unity Video Configured Alarms Not Appearing in Orchestrate as Unity Video Triggers

When a Unity Video or Unity Access Event is configured as an Alarm along with a Rule for the WEP Service to send the Alarm, then for connection through the Unity Cloud Services Connector perform the following actions:

- Check the WEP log that the Alarm Definition is being sent to Unity Cloud Services by searching for `Setup/Alarms` as part of the directory messages sent.
  - If the `Setup/Alarms` message is not in the WEP log, check the Unity Video/WEP version to ensure the version used is at least 7.14.2 or above.
  - If the version used is correct, collect logs and restart Unity Video and WEP.
- Check the WEP log for the actual alarm name of the Alarm that was created.

  If you cannot find the Alarm, collect logs and restart Unity Video and WEP.
- Check if the alarm has been disabled – if so, ensure that the alarm is enabled.

18.2 Triggered Alarms Not Received by Orchestrate

Orchestrate provides a diagnostics page to help troubleshoot deployments.

If the configured Alarm appears in Orchestrate, perform the following actions:

1. Create a workflow with the desired Alarm (Trigger) and any available Action.
2. Open the Runtime Data page.
3. Trigger the Alarm (manually or through keyboard shortcut).

The triggered Alarm should appear in the Runtime Data page when deployed correctly.

If it does not appear in the Runtime Data page, you must verify if the alarms are configured correctly within your specific product.

For example, for Unity Video verification, perform the following actions:

1. Check if Unity Video Web Endpoint Service is enabled.
2. Check if the Unity Video Alarm appears in the Unity Video Client software's **Alarm** tab.

   If not, check the Alarm settings in the **Site setup** tab.
3. Check if the workstation is configured to never sleep. If not, change the **Power Options** setting and restart the workstation.
4. **For connection through the Unity Cloud Services Connector:**
   - Check if the alarm is showing in the Alarm view of the Customer organization that the Unity Video site is connected to.

- Check if the Cloud Connector is turned off.
- Check if the alarm is in the supported list in Unity Video/Unity Access Alarm Configuration on page 46.
- Check if the alarm recipients are set to **Cloud Administrator** and **Cloud Viewers**.

18.3 Alarms Not Received by Radios

If a configured workflow Alarm (Trigger) is not received through text message by a radio, first verify that the Alarm is received by Orchestrate.

Go to the Runtime Data page and verify that the Alarm was received by Orchestrate.

If it was not received (it does not appear in the Runtime Data page), follow the steps in Triggered Alarms Not Received by Orchestrate on page 106.

If it was received by Orchestrate, perform the following actions:

- Check if Magellan Edge Node is properly installed and operational.

  Check that the Provisioning health check status at the Edge Node web portal is "green".

  For more information, see “Troubleshooting the Installation” in *Motorola Edge Node Installation Guide*.
- Check DDMS.

  Check that the Presence health check status at the Edge Node web portal is "green".

  For more information, see “Troubleshooting the Installation” in *Motorola Edge Node Installation Guide*.
- Check MNIS.

  Check that the TMS health check status at the Edge Node web portal is "green".

  For more information, see “Troubleshooting the Installation” in *Motorola Edge Node Installation Guide*.
- Check if the target radios are turned on and tuned to the correct channel/system.
- Check if the target radios are reachable by `Ping` command from **MNIS** → **Diagnostic page** in the Edge Node Management Portal when MNIS is hosted at the Edge Node, or by `Ping` command from a Windows terminal where Windows MNIS is running.
- Check if Automatic Registration Service (ARS) is enabled in target radio.
  - An Alarm text message is not sent to radios that have not indicated presence on the system.
  - For IP Site Connect and Capacity Plus, multi-site ARS must be configured to occur on site change.

18.4 Alarms Not Received by Ally

If a configured workflow Alarm (Trigger) is not received through text message by a radio, first verify that the Alarm is received by Orchestrate.

Go to the Runtime Data page and verify that the Alarm was received by Orchestrate.

If it was not received (it does not appear in the Runtime Data page), follow the steps in Triggered Alarms Not Received by Orchestrate on page 106.

If it was received by Orchestrate, see *Ally Avigilon Orchestrate Integration Setup Instructions*.

18.5 Workflows Continue to Run After Pausing in Orchestrate

There is up to one minute of delay between Pausing in Orchestrate and the workflows being paused.

18.6 New/Modified Workflow Not Operational After Saving

There is up to one minute of delay between saving a new or modified workflow in Orchestrate and the workflow being functional.

18.7 New/Modified Alarm Not Appearing in Orchestrate

There is up to five minutes of delay between creating a new or modified Alarm and it appearing as a Trigger in Orchestrate.

18.8 Text Message Never Received or Received with Significant Delay by Target

If the connection between the Edge Node and the Cloud is broken and then restored, text messages newer than one hour are sent, and text messages older than one hour are discarded.

18.9 Workflow Never Triggered by MOTOTRBO Radio's Emergency Declaration

If the MOTOTRBO radio successfully enters emergency state, but the Unit Enters Emergency workflow is not triggered, check if the emergency location trigger is set in Unit Management, which is required for a non-Capacity Max system and for a Capacity Max system without a VRC Gateway.

For more information, see Configuring Emergency Location in Unit Management on page 76.

18.10 Alarms Not Received by WAVE PTX Device

If a configured workflow Alarm (Trigger) is not received through text message by a WAVE PTX device, first verify that the Orchestrate Runtime data is logging the event to confirm if the alarm is received by Orchestrate.

If it was not received (it does not appear in the Runtime Data page), follow the steps in Triggered Alarms Not Received by Orchestrate on page 106 .

If it was received by Orchestrate, perform the following actions:

- Check if the User has logged in the WAVE PTX Mobile Application at the WAVE PTX device.
- Check if the WAVE PTX device has a broadband connection.

Appendix A

Networking Diagrams

The following diagrams illustrate the Avigilon and MOTOTRBO components required for the Orchestrate deployment and their IP Address and UDP Port requirements.

Figure 65: Customer Enterprise Network: Avigilon with Unity Cloud Services – Unity Access Global Actions NOT Supported

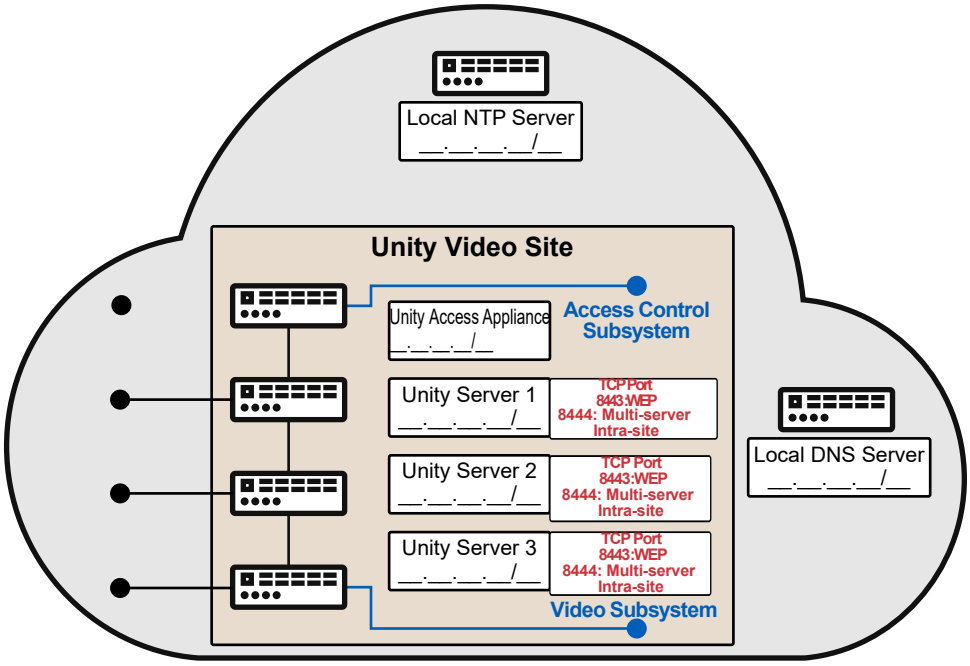


Figure 66: Customer Enterprise Network: Avigilon with Unity Cloud Services – Unity Access Global Actions Supported

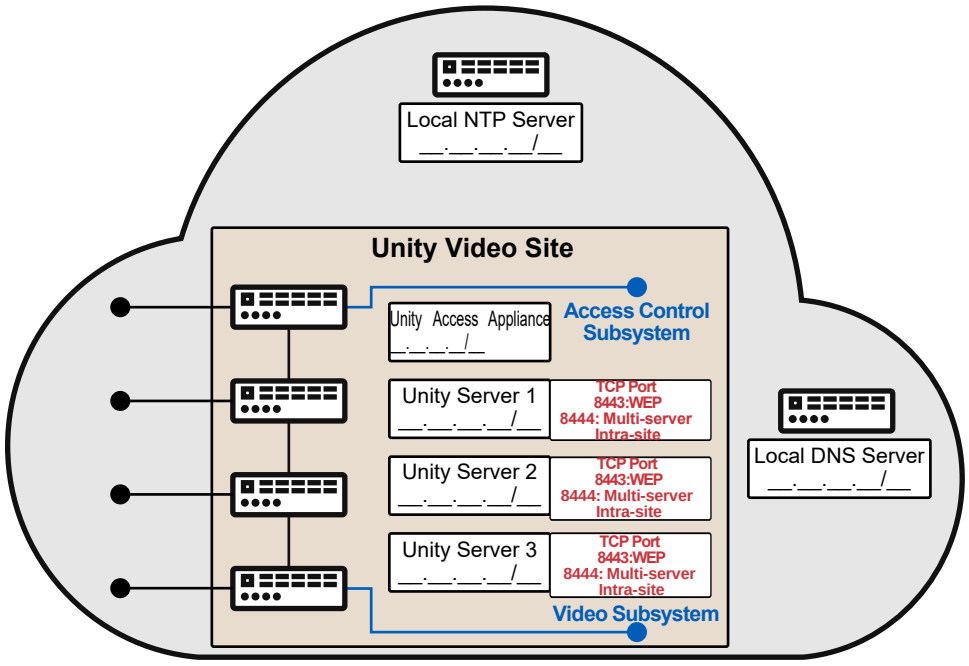
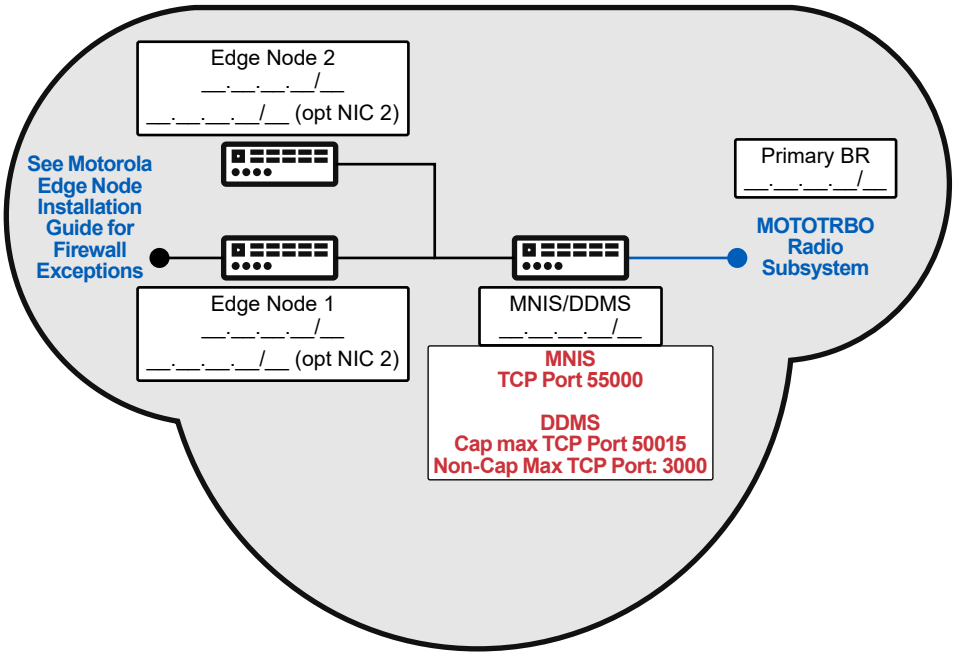


Figure 67: Customer Enterprise Network – MOTOTRBO (Standalone Windows-based deployment for MNIS and DDMS)



NOTE:

1. A Unity Video site requires only one Unity server, but the diagram illustrates a solution where three Unity servers are clustered together.
2. DDMS and MNIS must reside on the same hardware.

For the list of the firewall rule exceptions required when the customer network restricts outbound access, refer to the *Motorola Edge Node Installation Guide*. If the customer network does not restrict outbound access, then no firewall exceptions are required for the deployment.

Figure 68: Customer Enterprise Network – MOTOTRBO (Edge Node-based deployment for MNIS and DDMS – shared system)

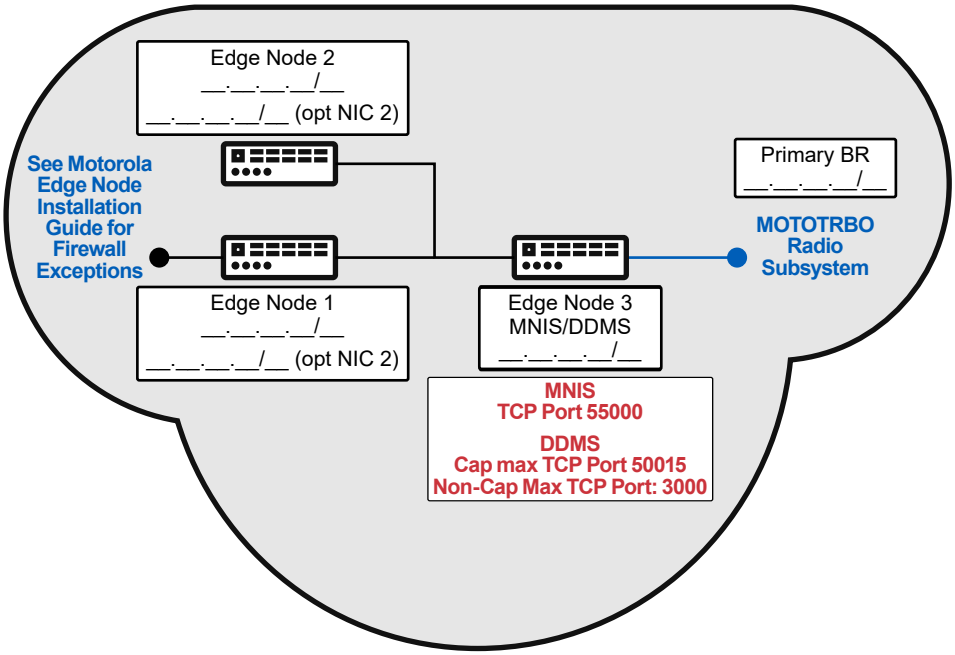
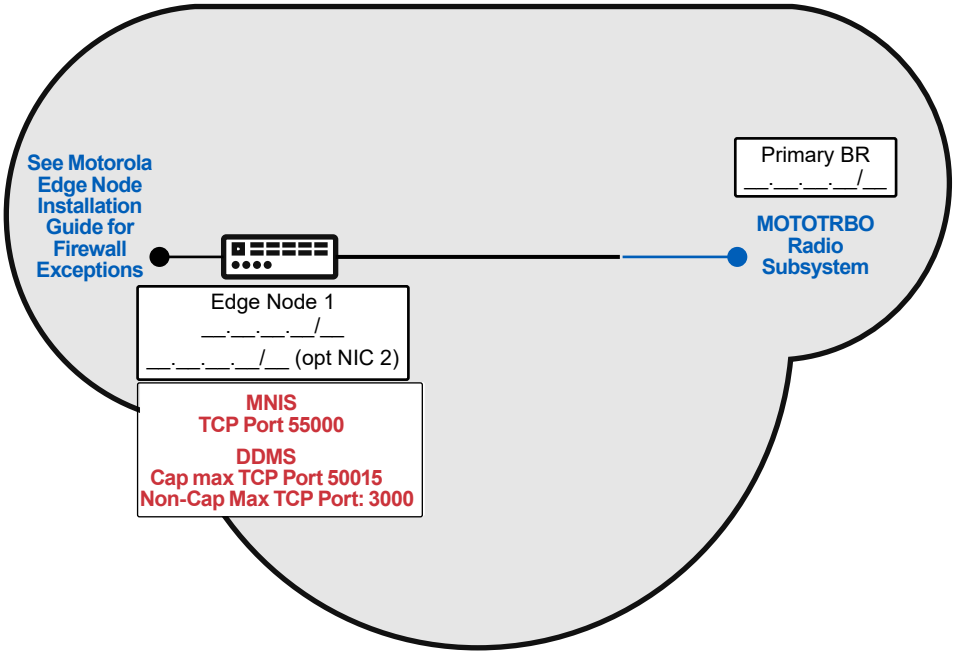


Figure 69: Customer Enterprise Network – MOTOTRBO (Edge Node-based deployment for MNIS and DDMS – system with one Edge Node)



NOTE:
In the Capacity Max System, **NIC 1** and **NIC 2** must be configured (**NIC 1** must be connected to the Internet and **NIC 2** must be connected to the Radio System). Custom routing must be added for **NIC 2**.

In non-Capacity Max Systems, **NIC 1** must be connected to the Internet and the Radio System.