ASTRA

INSTALLATION AND ADMINISTRATION MANUAL FOR MILESTONE XPROTECT 2023

ACTIVE INTELLIGENCE

THIS PAGE INTENTIONALLY BLANK

Table of Contents

Introduction

This document is provided by Active Intelligence to help guide administrators and integrators in installing ASTRA Anomaly Detection software. This guide will provide instructions on the installation of ASTRA software, for both the Linux Server and the Windows VMS configuration and licensing.

Prerequisites and Hardware Requirements

Before ASTRA can be installed, the following prerequisites must be met:

1. ASTRA must be provided and installed by an Authorized Channel Partner with ASTRA Certified Associates.
2. The associate must have a firm understanding of the Linux Ubuntu Operating System (OS), working with command line inputs, network configuration, and the VMS to which ASTRA is to be installed. While Active Intelligence provides training on the ASTRA integration, training is not provided on the VMS, network configurations, or operating systems (Linux Ubuntu or Windows).
3. The VMS must be installed and operational.
4. The ASTRA server should have internet connectivity to in order to download and install the prerequisites required for the ASTRA and Nvidia products and must have network connectivity to the Milestone XProtect VMS server.
5. Pre-sales and pre-deployment planning are required. Discuss the client's needs and understand their current and future camera deployment plans. It is crucial that the ASTRA system is based on the client's needs for today and the near future.
6. The Authorized Channel Partner sends a Purchase Order to Active Intelligence with the following information:
    a. Where is ASTRA to be deployed, include name, location, contact information. Also include the number of cameras streams to be activated within ASTRA, and the VMS which it is being installed on.
7. The authorized associate installing ASTRA will email Active Intelligence support with the seed key information to obtain a license file. The email must include the PO number, client, location, and camera counts.
    a. These tasks should be completed well in advance to avoid any delays in receiving the license key to be utilized during the installation process. The system can run for five (5) days without a license key to allow learning to begin, however, no anomalies will be received until the key is applied.

Note: Always check the Active Intelligence website for the latest hardware requirements and the current version of the ASTRA Software.

Considerations:

- Ensure that the server(s) used to host the Astra Hypermedia Search Engine (HSE) are time synchronized with the Video Management System (VMS).
- Know the IP addresses for the systems and have them on hand to avoid mistakes.
- Ubuntu admin level user is required for parts on the installation process.
- Windows administrator permissions are required to install ASTRA software on the Windows VMS server.
- Verify the appliance hosting the Hypermedia Search Engine (HSE) **DOES NOT** have MySQL installed.
- When choosing hardware for the ASTRA server, make sure it is sized properly and provides processing headroom for future growth and remains within the hardware guidelines (quantity of camera streams, resolution, and frames per second (FPS)) presented on the Active Intelligence website. If unsure or the number of camera streams are beyond the guidelines listed on the Active Intelligence website, reach out to the Active Intelligence Sales Engineering team for assistance.

Once the server size has been determined, purchased, and server is in hand, the ASTRA Linux Server install process can begin.

Camera Requirements

The camera streams for which ASTRA is to be active must have a resolution greater than 720P (1080P or better recommended), with a recommended 12-15 Frames Per Second (FPS). A bitrate no higher than an average of 1.5Mbps is also recommended.

Definition

Analytics vs Anomaly

Most analytics software is used forensically, post incident. For example, finding the “person in the red sweater” by defining or applying a rule. Because traditional video analytics are rules-based, they are often forensic and not effective for real-time detection.

ASTRA anomaly detection is excellent for detecting events within the camera’s field of view that have not happened before or have not happened often, in real-time.

Rules-based solutions do not handle real-time detection well, if at all. Typically, they can only look for things they are programmed to look for when searching recorded video. Rules creation is also very time consuming and often needs to ingest the event for the system to recognize it.

ASTRA uses statistical analysis to filter out normal patterns and behaviors in video data and identifies anomalous events in real-time by evaluating sequences of video frames.

For more information on how Anomaly Detection compares to traditional video analytics, refer to Anomaly Detection vs Video Analytics page on our website.

What is ASTRA?

ASTRA is an enterprise-level, multi-site, distributed Anomaly Detection Software product developed by Active Intelligence.

ASTRA is a virtual operator, putting eyes on the entire video security enterprise 24/7/365, monitoring video streams and notifying operators of all anomalous events instantly, in real-time. ASTRA uses machine learning and artificial intelligence, paired with proprietary statistical analysis algorithms to detect anomalous events, allowing critical enterprises to address events that require intervention in real-time. This shifts security operations from investigating negative outcomes to effectively preventing or mitigating them.

How ASTRA Works

The calibrated model uses the first three consecutive frames of video as input and predicts the fourth frame, then compares the predicted fourth frame with the actual fourth frame. If there is a difference in the frames greater than the set threshold, then this is an anomaly, and an alert is sent.

The foundation model only requires one step of calibration, allowing the model to become familiar with the current scene. The foundation model and calibrated model both are retained. Once the calibrated model is ready, detection of anomalies for that scene begins.

Through these approaches, the operators should see less than 1% - 2% of all video data that comes through the ASTRA installed network.

Getting Started with ASTRA

System Architecture

In the ASTRA Communication topology diagram below, the ASTRA Hypermedia Search Engine (HSE) service and Hypermedia Search Engine database are deployed on the Milestone XProtect Management Server. The Milestone Open Network Bridge is required to provide RTSP streams to ASTRA. The ASTRA HSE service and HSE database may be deployed on any Windows server that is on the same network, if the proper ports are open between the servers. The following sections will detail how the services and roles can be broken out to servers if necessary.

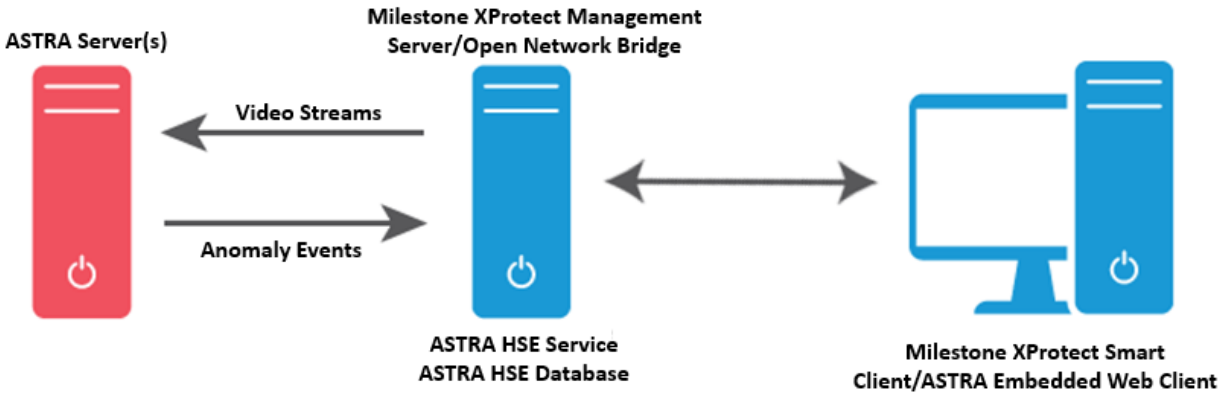


Figure 1: Typical ASTRA Communication Topology

ASTRA Software Installation

There are two ASTRA software applications that must be installed - ASTRA Linux Server application and the ASTRA VMS Windows integration application.

Linux Server ASTRA Installation

These next steps are to install the pre-requisites needed for ASTRA and the ASTRA software:

1. Download the ASTRA zip files:

   wget https://www.activeintelligence.com/dowloands/astra_files.tar.gz

Note: An internet connection to the Active Intelligence download server is required during the install process.

2. Extract files:

   sudo unzip astra_files.tar.gz

Note: If the unzip command is failing to find the software it can be obtained with the command sudo apt-get install unzip

3. Navigate to the astra_files folder

   cd astra_files

4. Run the ASTRA Installation script

   sudo ./astra_install.sh << astra_install.log

   a. A prompt is displayed and will need to be answered before the installation starts, enter the 4 octet IP of the server that is hosting the ASTRA service in Windows (ex. 192.168.1.1).

      i. *Enter the IP of the server hosting the ASTRA Windows Service:*

   Note: Firewall exceptions are made and the firewall will be turned on as part of the installation process.

5. Enroll Cameras streams and check status:
   a. Cameras streams are enrolled on the ASTRA Windows VMS integration application HSE license page by selecting the camera streams under the “Enrolled” column. This inserts a “check mark” in the box as a visual aid showing which camera streams are enrolled.

   b. Check ASTRA Service Status (once complete, it should show as “active (running)” and the date
      i. *sudo service astra_detector status*
   c. Check that the NVIDIA drivers are installed:

      i. *nvidia-smi*

Note: If ASTRA has not been installed on the Windows VMS system, “No Processes Found” will be displayed. “Running” will be displayed when ASTRA has been configured with the cameras streams online and is processing anomalies.

ASTRA Software VMS Server

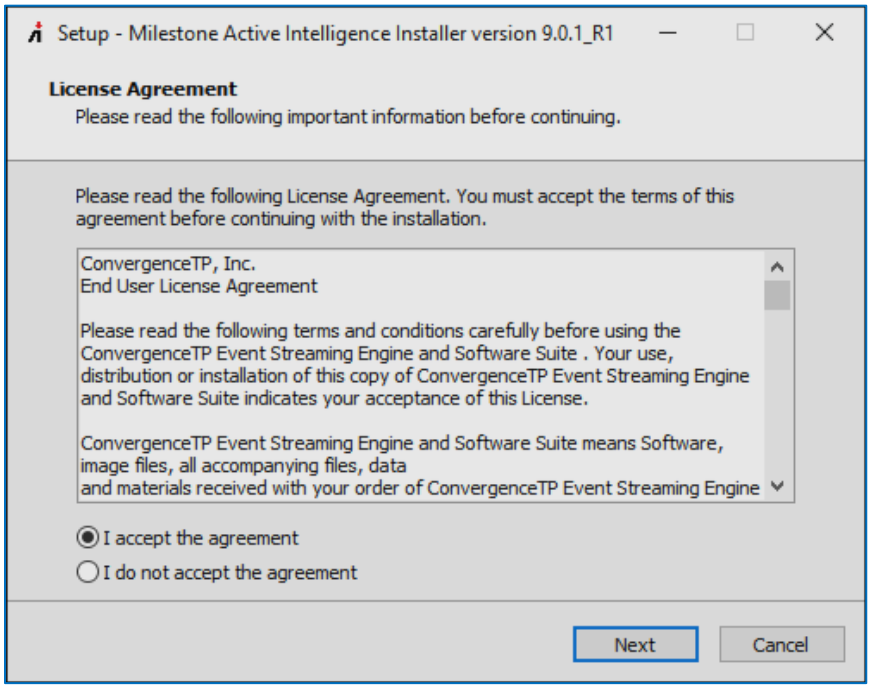
1. This is the Windows-based integration to the VMS connected server.

2. Once the ASTRA software installer has been provided, ALWAYS verify that it is the most up-to-date version. Do not rely on saved versions of the ASTRA installer, always download the current version.

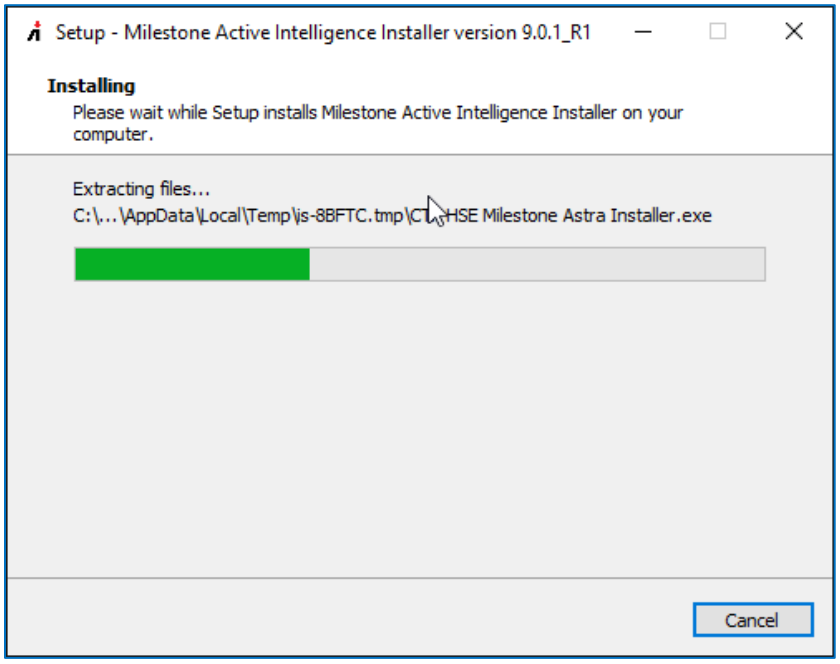
3. The ASTRA applications can reside on their own Server/PC, installed on the VMS Server or the Management and XProtect Smart Clients servers/PC, any of which must be on the same network and communicate with the VMS Server for camera(s) setup and anomaly detection. The location is the installers preference.

4. **ALWAYS** run the ASTRA Windows Installer as Administrator.

5. The License Agreement will display. Once completely read, select “I accept the agreement” to continue with the setup, or “I do not accept the agreement” to terminate the installation process, then select “Next.”



6. ASTRA installer will display a progress bar as the files are loaded onto the server.



7. When the ASTRA installer progress screen is complete, three options will appear:

   a. ***Install Custom HSE Server*** – The Web Server, Database, and licensing components, select this if you do not want to install this on the same server as the ASTRA services (it is recommended to keep all the components together on the same server).

   b. ***Install HSE Database*** - The Web Server, Database, and licensing components.

   c. ***Install Active Intelligence Service*** - ASTRA service, Bridge Service, & Event Stream Engine.

8. Use the check boxes to select the items to be installed.

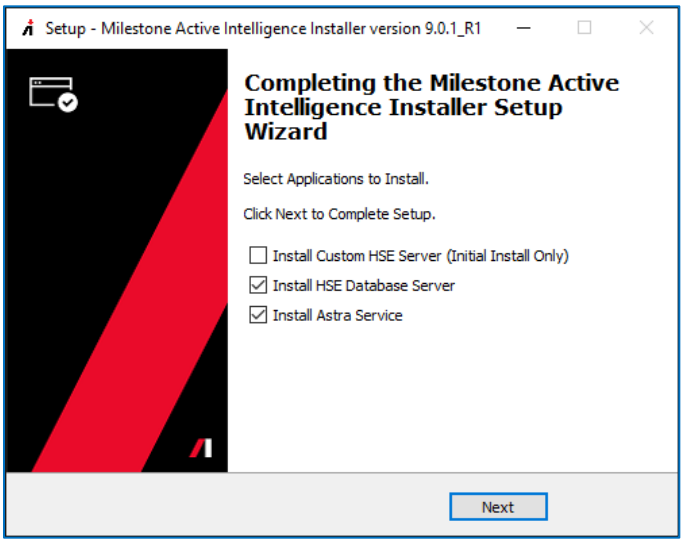
   a. Typical required components to check and install are:

      i. "Install HSE Database Server" and "Install Active Intelligence Service"

      ii. Select "Install Custom HSE Server" only to install those service on a separate server.

Note: If no boxes are check and "Next" is selected, setup will exit.

9. Once selections are made, select “Next” to continue.

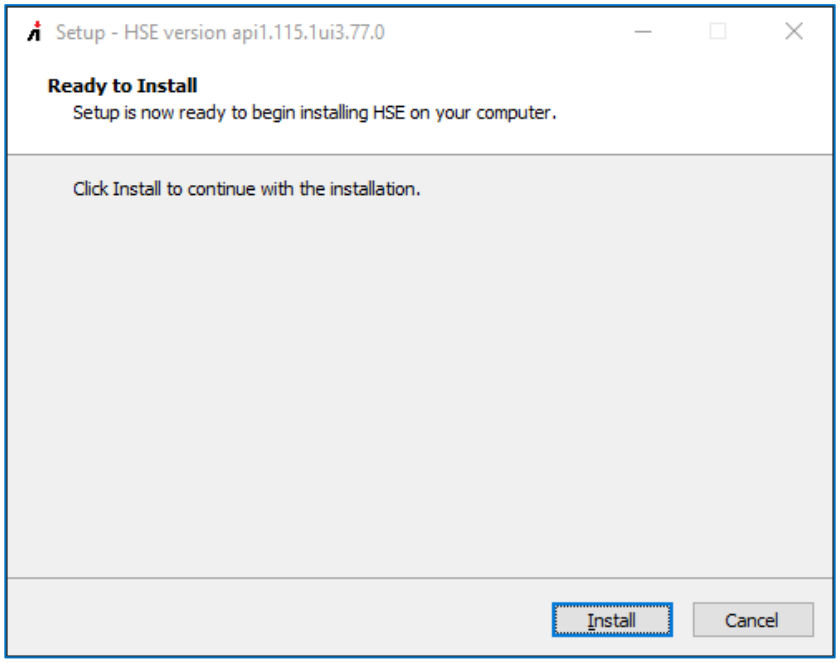


Note 1: If prompted during the installation process, allow Microsoft .Net to be installed.

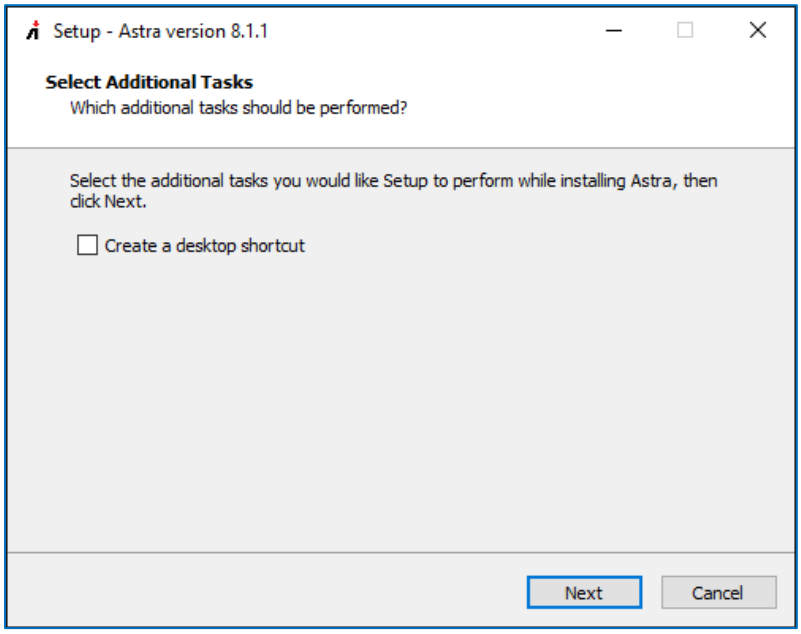
Note 2: When prompted, allow desktop icons to be installed, then delete them if they are not needed after the setup and testing of the fresh install is completed.

10. Setup will create the program shortcuts in the following start menu folder, “Active Intelligence”.

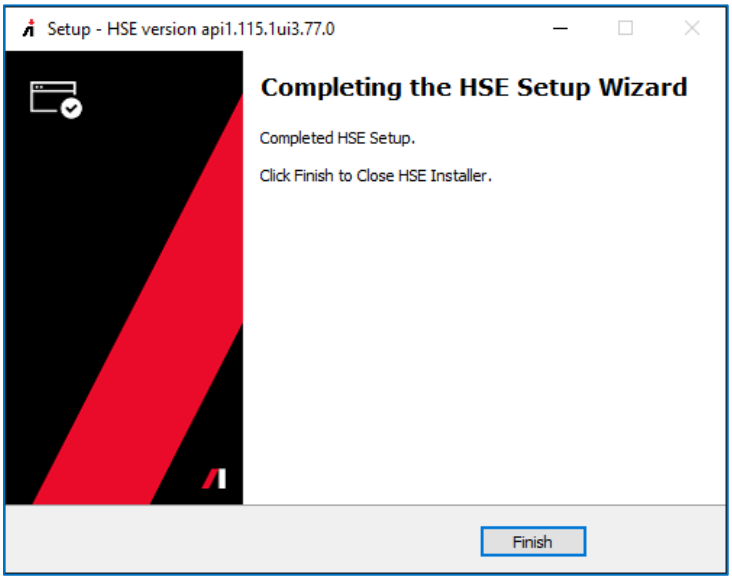
11. The HSE “Ready to Install” screen will display. Select “Install” to continue with the installation or “Cancel to quit.



12. Select “Create a desktop shortcut” to place a check mark in the box, then select “Next”.

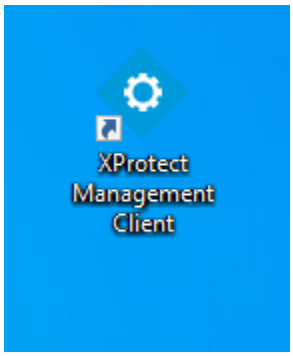


13. Once the install has completed, select “Finish”.



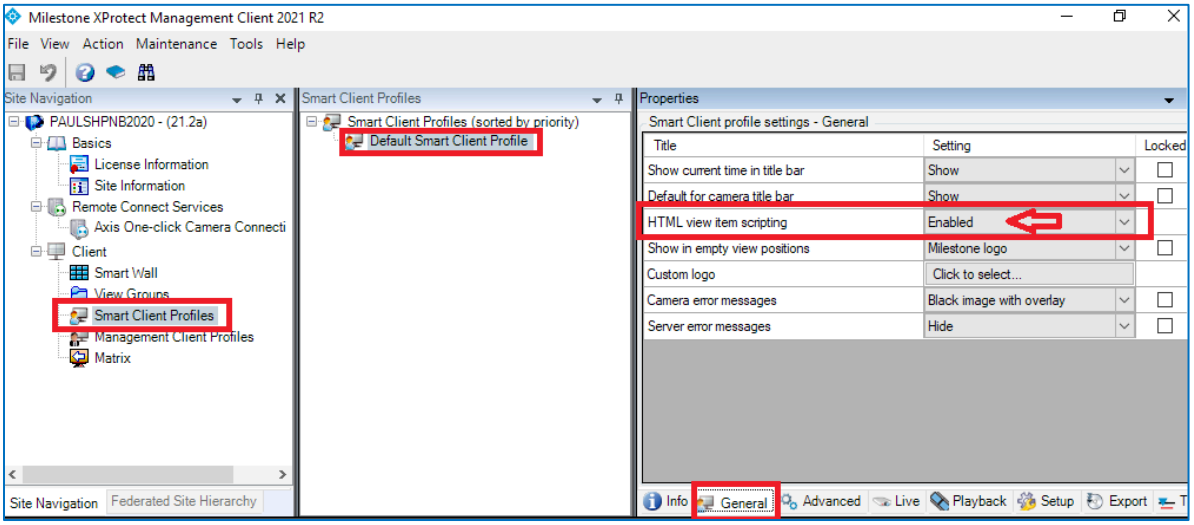
Enable Scripting in the Milestone XProtect Management Client.

Open the Milestone XProtect Management Client.



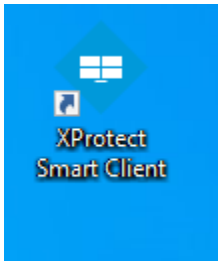
Navigate to the Client > Smart Client Profiles > Default Smart Client Profile.

Make sure the “General” tab is selected and set the “HTML view item scripting” to Enabled.

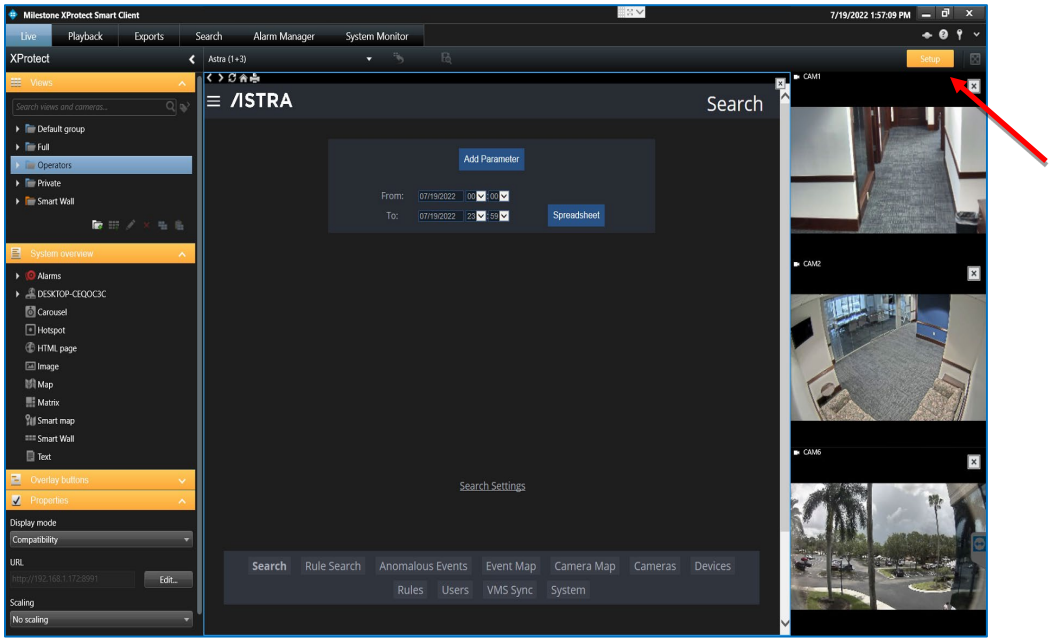


XProtect Smart Client view setup for ASTRA integration

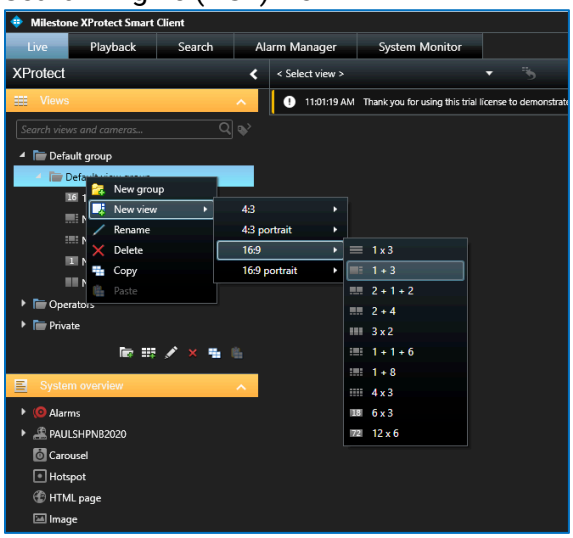
Open the Milestone Smart Client



Create a new view in the XProtect Smart Client by selecting “Setup” in the top banner on the right.

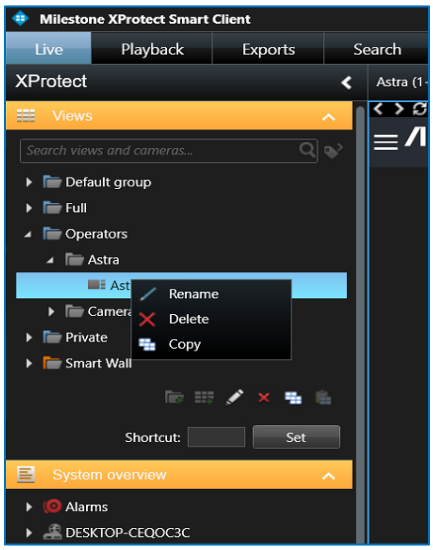


ASTRA uses a common XProtect Smart Client view for all integrations.
The ASTRA view is a 1 + 3 with the Hypermedia Search Engine (HSE) being in the “1” view area and the “3” corresponds to the 3 camera views that are to the immediate right of the Hypermedia Search Engine (HSE) view.

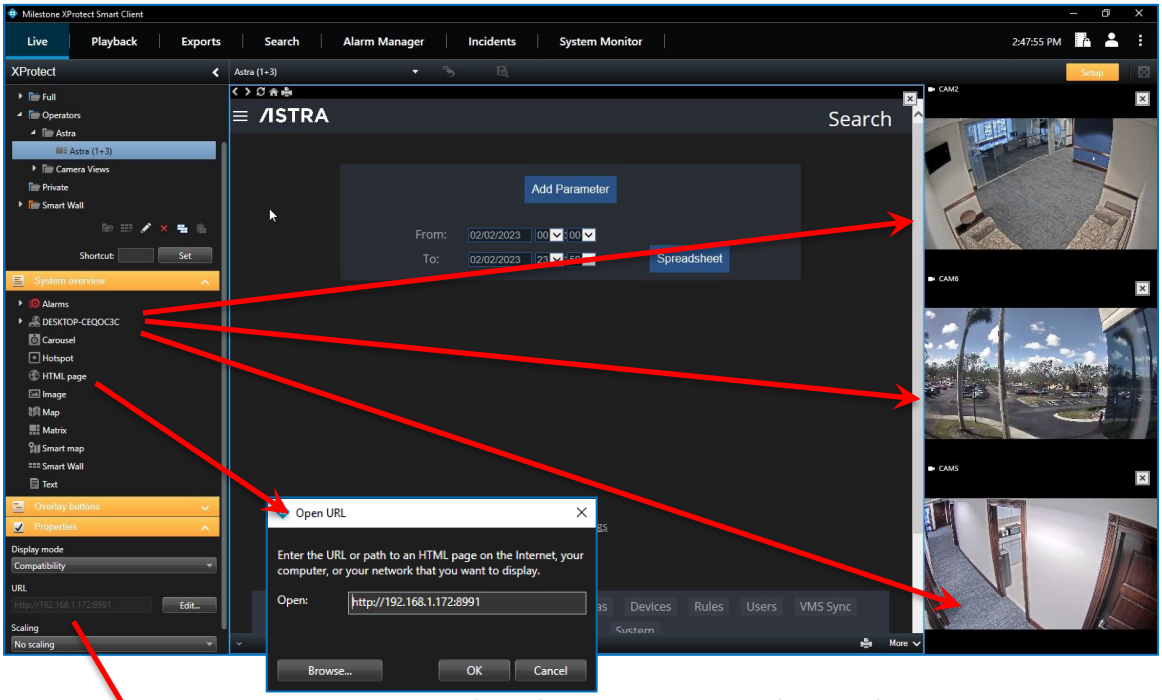


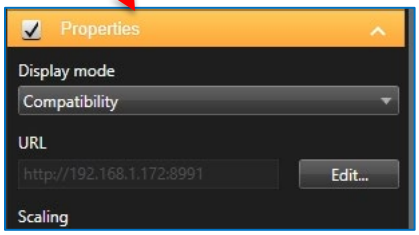
To get to the XProtect Smart Client view, select “Default Group” > “New View” > “16:9” > “1 + 3”.

Once the blank 1+3 view appears, it can be renamed by right clicking on the view and selecting “rename”.



The Hypermedia Search Engine (HSE) uses the Web portal for its view.





Select the HTML page and enter the URL.

The URL used is = http://IPAddress:8991 where IPAddress is the IP address of the machine hosting the Hypermedia Search Engine (HSE).

Make sure the Display mode is set to Compatibility mode.

Populate the camera views by simply dragging and dropping the cameras into the view spaces.

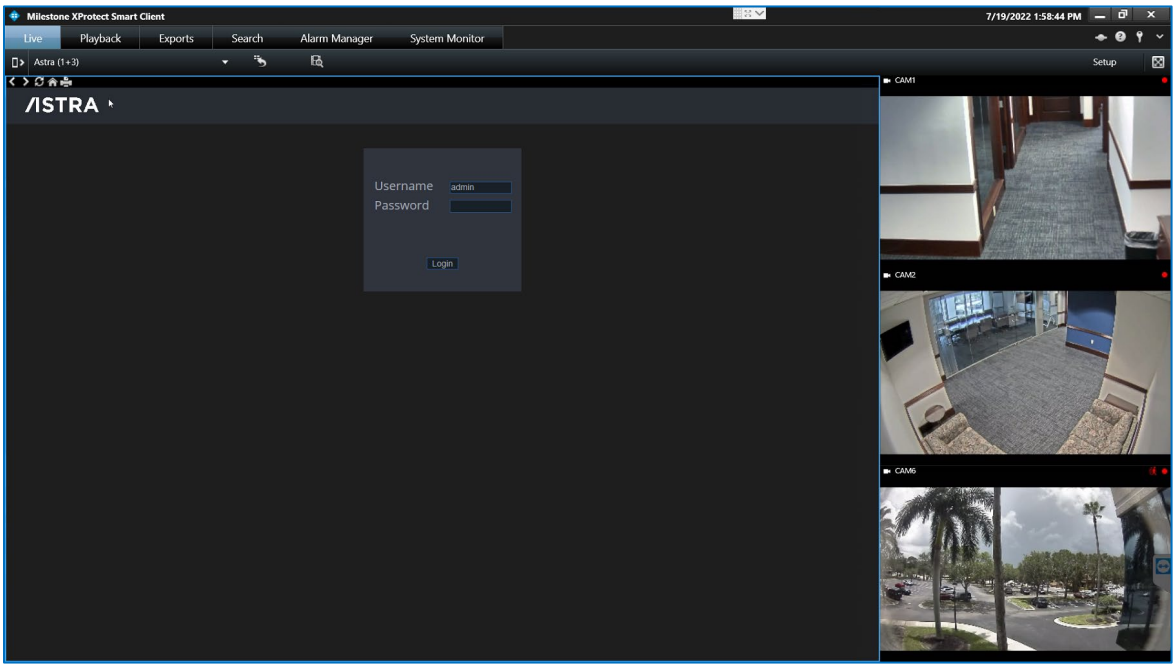
When completed select the Setup button in the top right corner to save.

ASTRA Milestone XProtect Smart Client Configuration

Select the 1 + 3 view created in the previous steps. Log in to ASTRA.

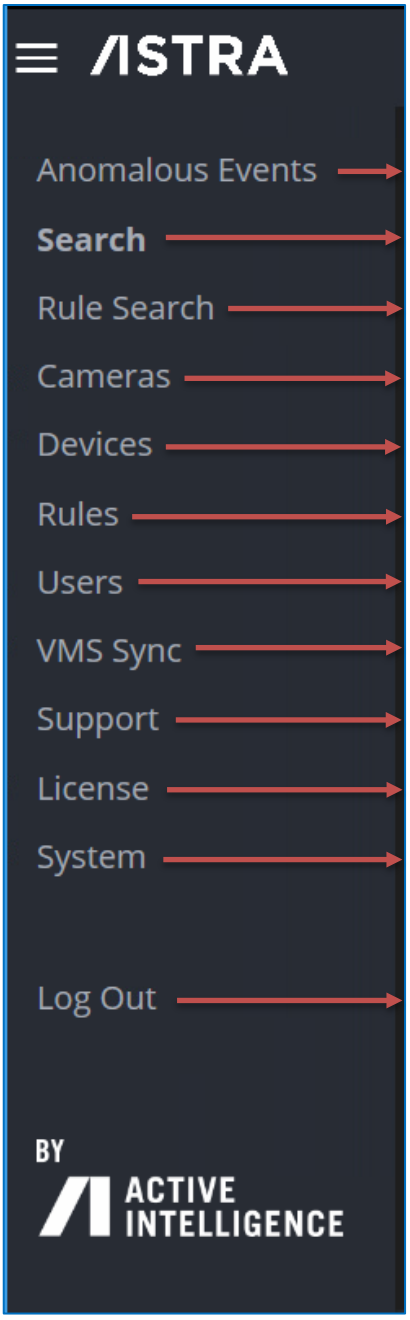
After saving, log in to the Hypermedia Search Engine (HSE) with the default credentials.

Username *"admin"*
Password – *"Password1"*



The ASTRA dropdown menu is in the upper left corner of the ASTRA screen within the XProtect Smart Client and is used to configure the ASTRA interface with Milestone XProtect.

Each menu item is described below:



Brings up tabulated summary of Live Anomalous Events

Brings up the HSE search engine for forensic investigations

Provides drop down menus of rules to select for viewing

Assigns name, identifier

Assigns device name, identifier, type of device, cameras, can be related

Sets up criteria and action to take using key words

Sets up Usernames, passwords, and roles of users

Login credentials used to establish connection to VMS

Displays Active Intelligence Support contact information

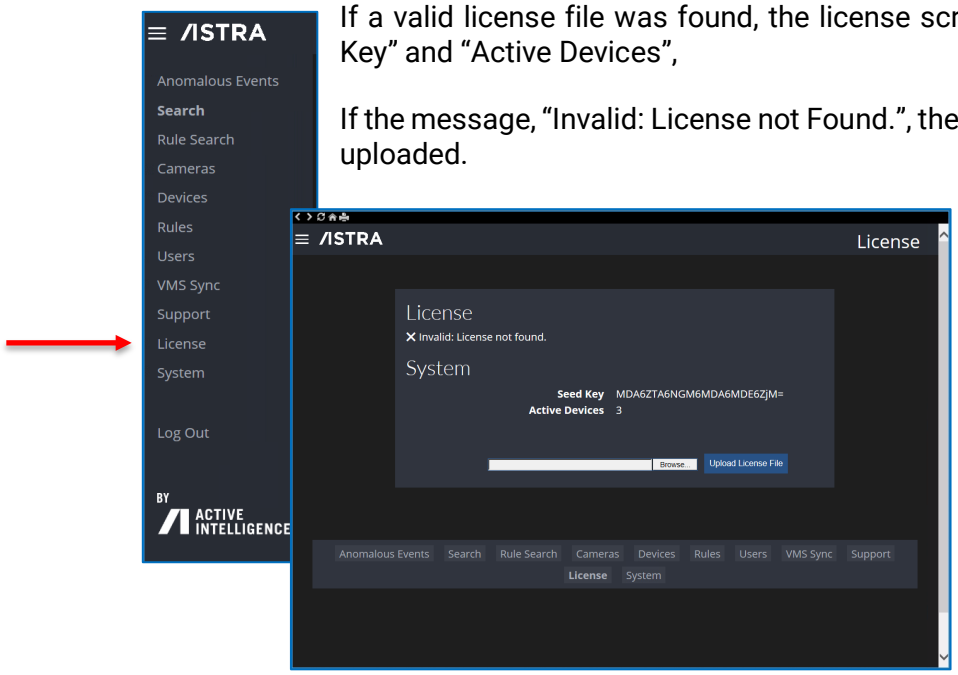
Displays Current License information

System information shows time zone and version of ASTRA Software release

Logs out of the ASTRA software, but leaves the XProtect Smart Client logged in

ASTRA LICENSE

Select License under the dropdown menu ≡ to verify that a valid license file has been installed.



If a valid license file was found, the license screen displays showing the “Seed Key” and “Active Devices”,

If the message, “Invalid: License not Found.”, then a valid license file has not been uploaded.

To obtain a “New” ASTRA License, select the “Seed Key”, then copy and paste the seed key text into an email.

***DO NOT* send a screenshot**

Email the seed key along with the Purchase Order, client’s name, contact information and number of cameras streams to become activated in ASTRA to:

Support@Activeintelcorp.com

When the ASTRA license file is received, save it to the server. Then select “Browse”, go to the location the license file was saved, select the .lic file and “Open”.

Select “Upload License” and the system will display “New license file successfully installed”.

The following information is now visible on the License page - license expiration date and time, days remaining on current license, total camera licenses available, total cameras enabled, total licenses in use, failover enabled / disabled status, total licensed cameras offline, and AMCS Watchdog status.

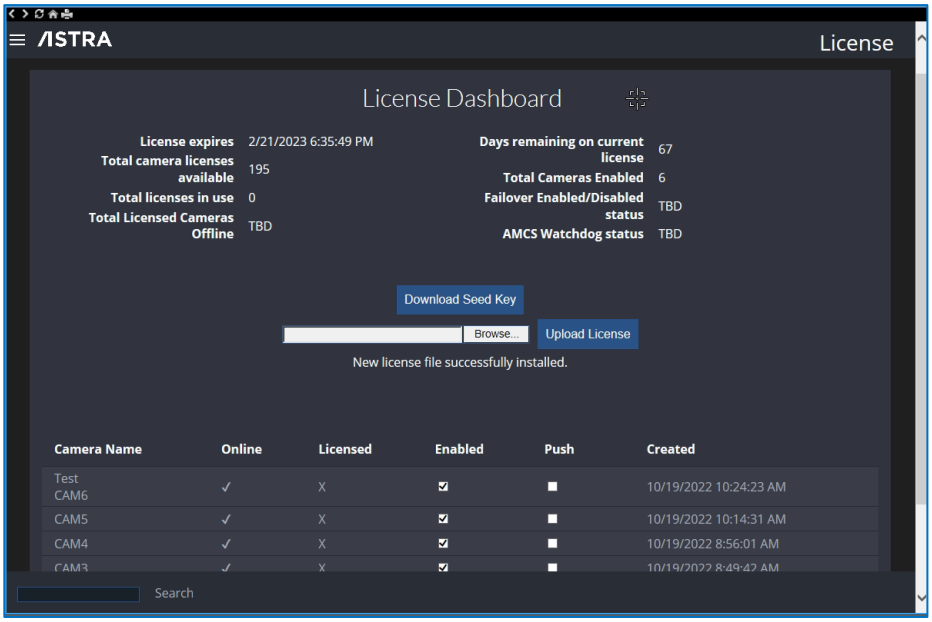
The camera names listed are determined by the account login in the VMS Sync fields. Any cameras that the user has permission to view on the VMS will be displayed within ASTRA.

The License dashboard has six columns:

- ***Camera Name*** – presents as it appears in the VMS
- ***Online*** – camera status; a check mark appears when a camera is online, nothing is shown in the column when the camera is offline. This information comes from the VMS.
- ***Licensed*** – *Future*
- ***Enabled*** – defines where ASTRA has been enabled for that camera's stream. Cameras can be enabled/disabled by selecting the check box.

Note: If a camera stream has been enabled and has learned the scene in the field of view (FOV) and is then disabled, by removing the check mark, the cameras stream will cease reporting of ASTRA anomalies. The ASTRA system storage may store the learned scene for a short period. If reenabled quickly, the two-week leaning period may / may not have been retained. The exact storage retention time is system dependent. Plan for the two-week learning mode.

- ***Push*** – triggers a generic event, which can be used by the VMS to trigger additional actions and events
- ***Created*** –is the date that the camera was imported via VMS sync

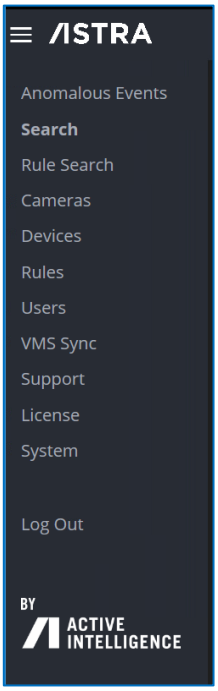


VMS Sync

A new install will require synchronizing the ASTRA framework with the VMS.

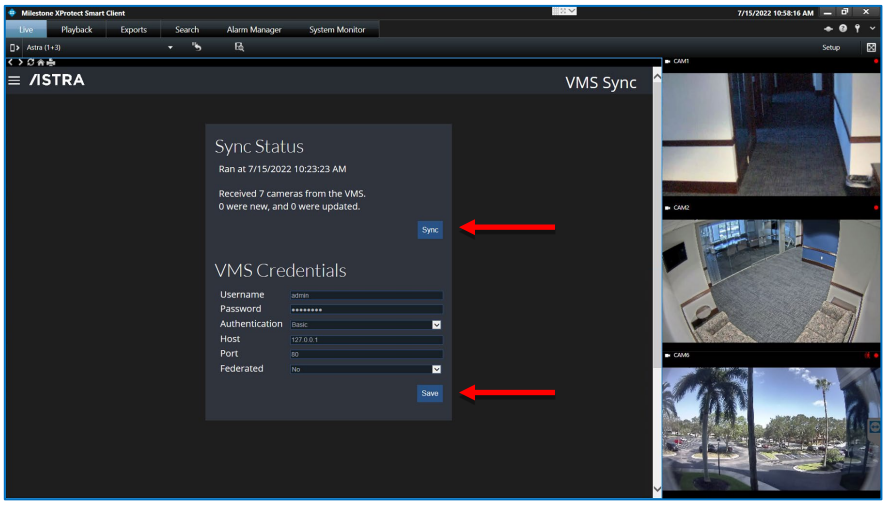
From the drop-down menu ≡, select “VMS Sync” to establish a connection with the VMS.

The VMS user credentials are required for this step (the username and password were established in the installation process of the VMS).



The user that logs in to the system must have access to all the cameras that are being utilized by ASTRA to detect anomalies. The “Sync” status window will change and show the current date and time, the number of cameras received from the VMS, and the number of new and updated cameras associated with this Sync.

“Sync” must be run every time cameras are added and/or updated to start anomaly detection.



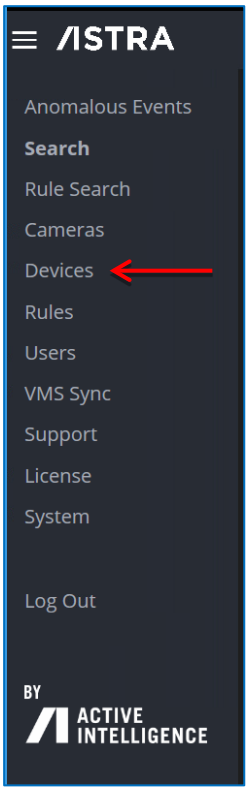
Enter the authentication credentials, which are either the Windows login or the VMS Basic login. These login credentials should have access to the cameras within the VMS that you would like to process with Astra.

Once logged into VMS Sync, the Sync Status will show the date and time “Sync” was last ran, the number of cameras received from the VMS, and number of updated cameras.

To Sync ASTRA with the VMS, select “Save” then select “Sync”.

Device Manager

Go to “Devices” in the ASTRA dropdown menu ≡.



In the Device Manager, cameras streams can be associated to each camera view in the Device Manager List. These cameras are used for video review when the “Show” button is selected within any anomaly.

Note: The first camera stream added should be the camera stream in which the anomaly was detected.

Once enrolled, each camera stream must be configured in the Device Manager.

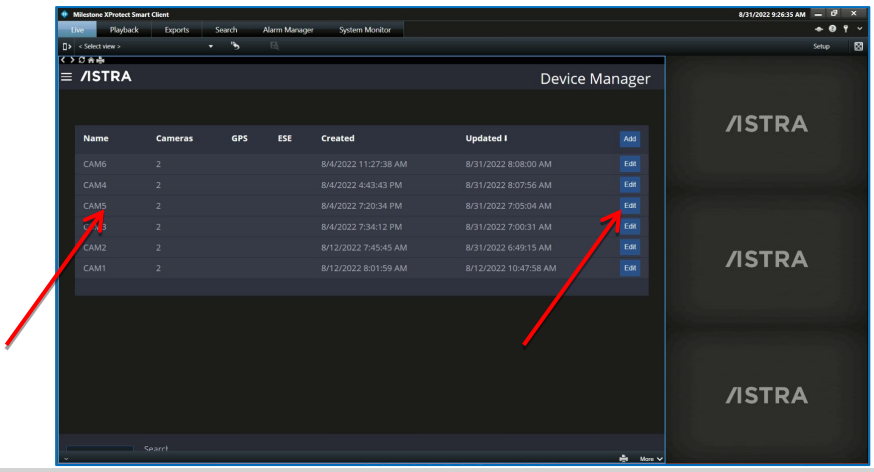
Example: ASTRA detected an event on the lobby camera, what other camera views would the operator like to view in real-time? One might be the exit door camera, or the hallway camera. These views would then display anytime the lobby camera has an event: Lobby Camera where anomaly was detected, exit door, and hallway cameras.

The association must be completed for each camera stream individually.

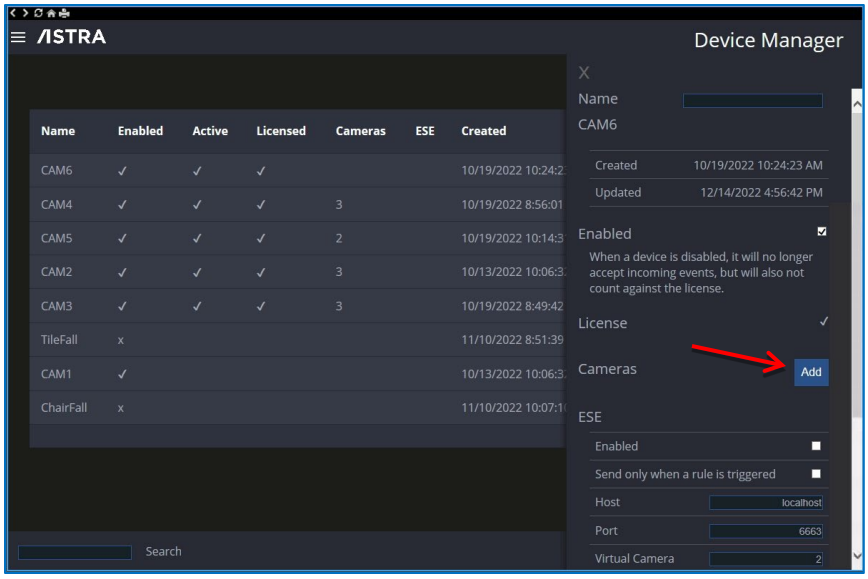
Note: The camera names displayed are the camera names used as the descriptors when the VMS was setup.

The suggested defaults of the physical camera can also be added at the discretion of the user.

Below, ASTRA sent a camera stream’s anomaly event to the ASTRA Management System. By doing so, the VMS attached camera streams associated with the anomaly - CAM1 was automatically enrolled. From Device Manager, select “Edit” on the camera to edit the associated camera(s).

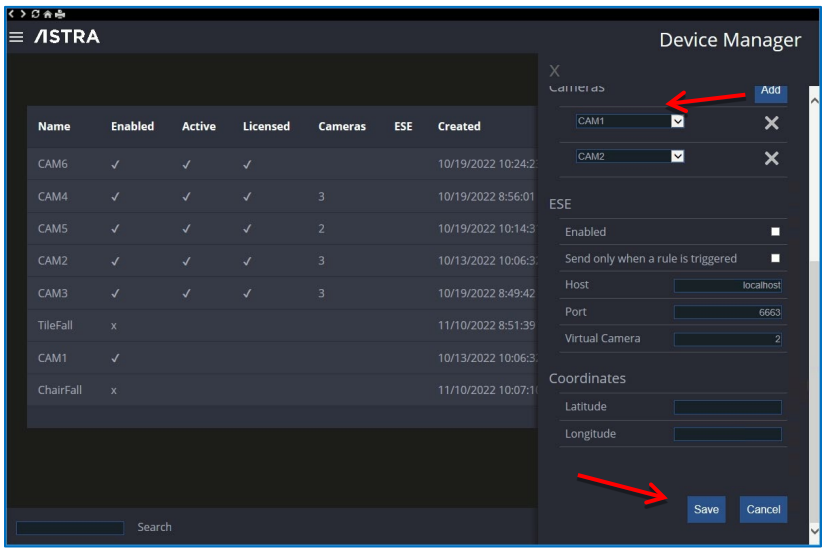


Note: The Device table will be empty until an Anomaly event is received from the ASTRA Engine



The side bar window will open, as shown. Within the side bar window, at the bottom of the screen select Edit.

Within the side bar window, under the Cameras heading, select “Add”, then select the camera from the drop-down menu. Complete this process for each camera stream to be associated. More than three cameras can be associated, however, only the top three will display.



To remove the association between the cameras, use the “X” to the right of the drop-down menu to remove.

After completing the assigning of camera streams to be associated, scroll to the bottom, and select “Save”.

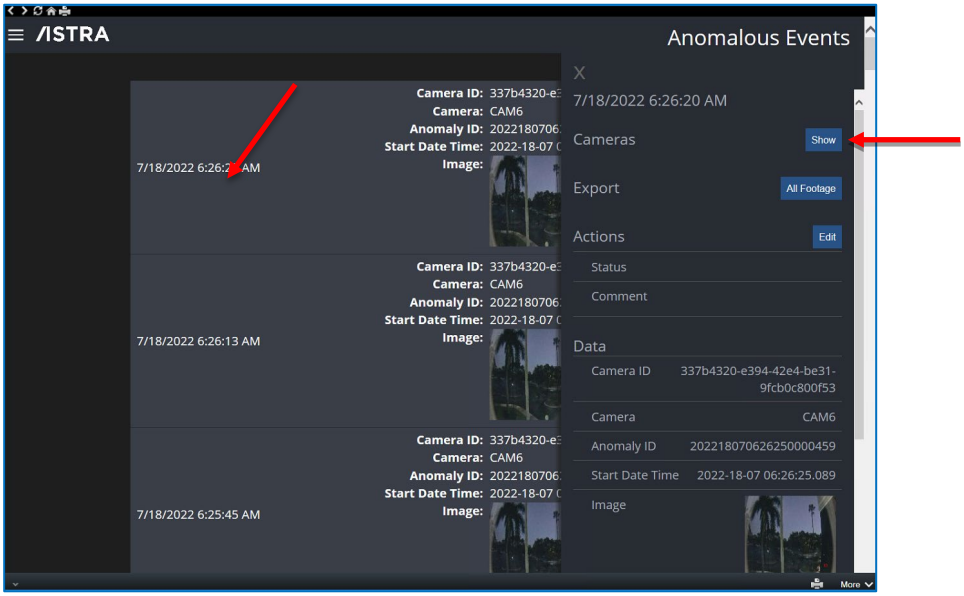
Once the Camera’s steams in Device Manager have been configured, the system is ready to fully process ASTRA anomaly events.

Note: As ASTRA sends anomaly data, each new camera stream that the ASTRA integration has not received data from previously, will be enrolled automatically. Anomaly data from these new cameras streams will be stored in the HSE database. These events can be viewed using the Search or Anomalous Events pages within the HSE. The camera playback features in the Search and Real-time pages will not function until the playback cameras are associated on the Devices page.

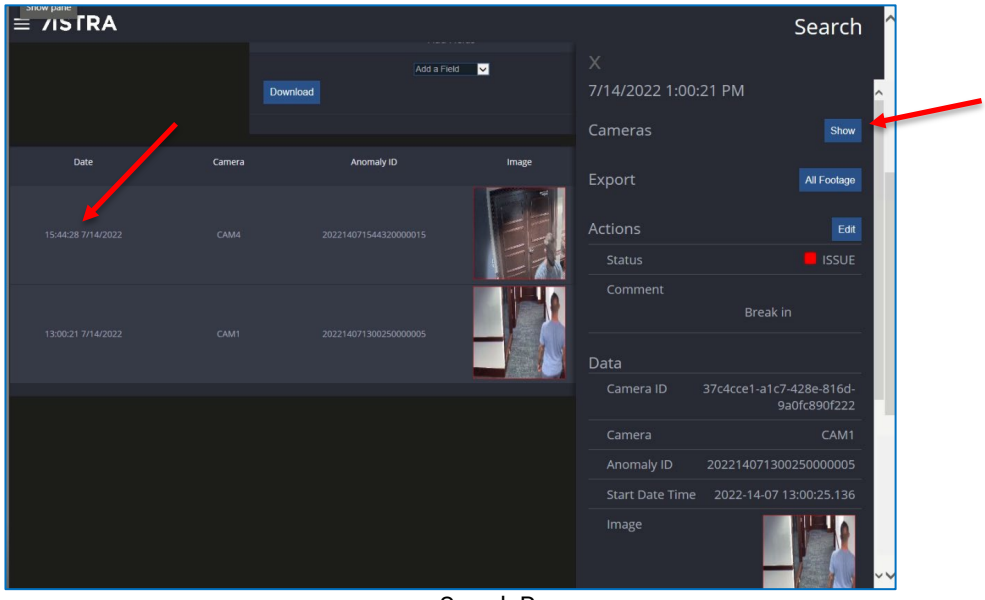
Viewing and Labeling Anomalous Events

When finished adding cameras streams in the device manager, evaluate the integration using the “Anomalous Events” or Search Pages.

To get to the side bar, select any anomaly event and the side bar will appear. Then select “Show”.



Anomalous Event Page



Search Page

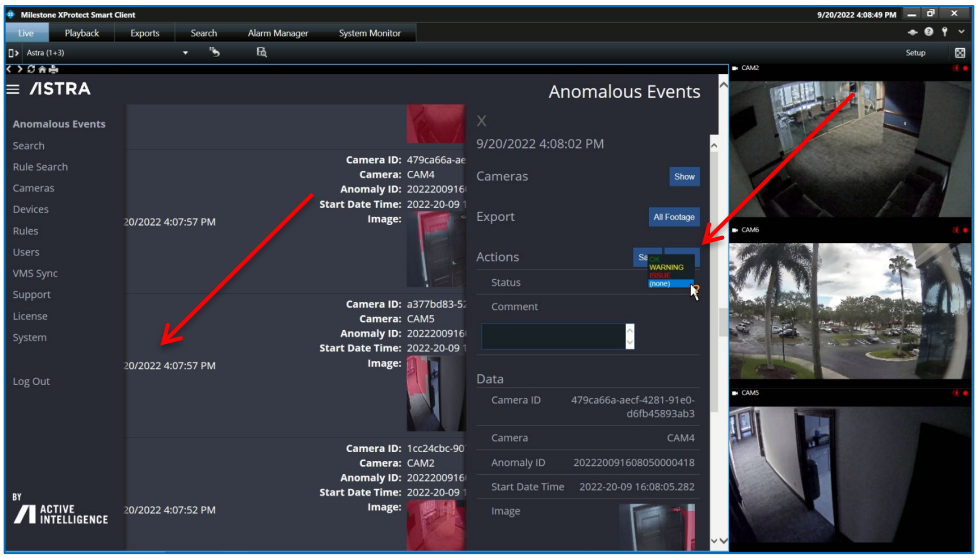
Note: A camera stream must be associated in the device page for the anomaly event, otherwise the “show” button will not be displayed.

Select any event to open the side window. Select the Edit button, then “status”, the drop-down menu provides three default options: “OK”, “Warning”, and “Issue”.

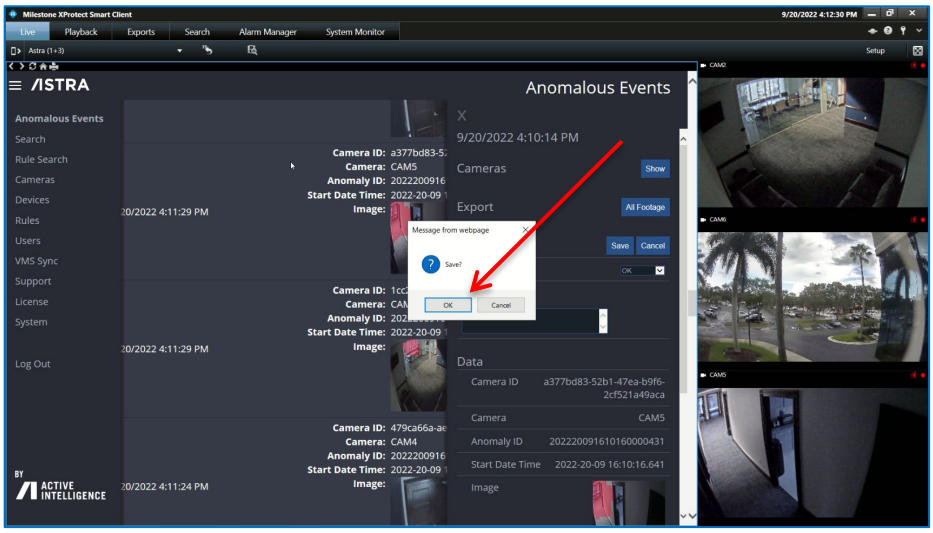
Note: The client will be able to add to the list as needed in future versions.

Select one of the options based on the event severity

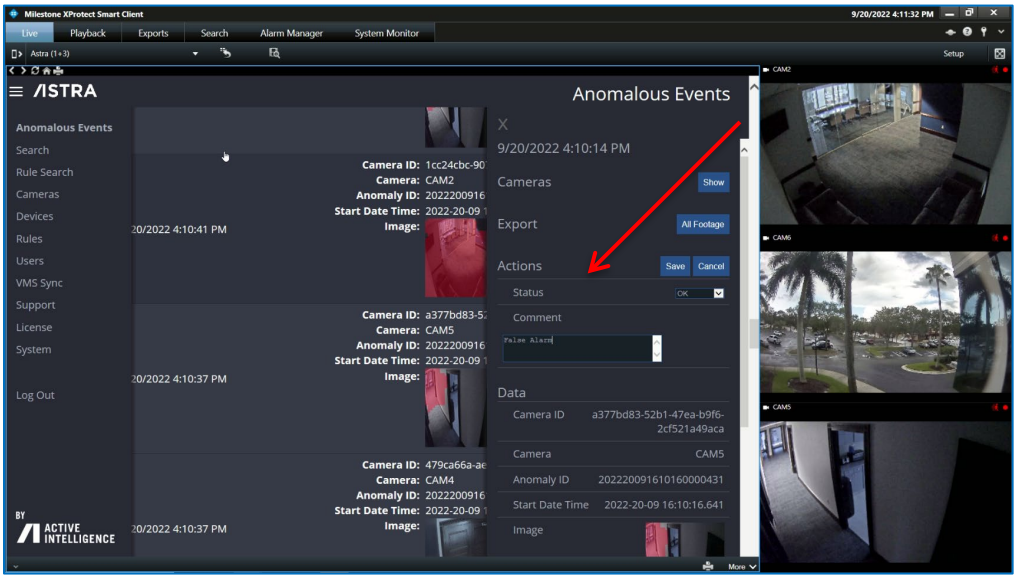
OK −−−−−−− Non-actionable events.
Warning −−− Of concern or notable
Issue −−−−− To be reviewed



A pop-up Save window will appear - select “OK”.



Select the comments box and enter the details of the event to coincide with the status (for example, Slip and fall, Fight, etc.). In this case, it was “OK” because it was a false alarm. These all become searchable elements.



Push Event

See the License page to set Push notifications for generic events. Push events are activated on a per-camera basis.

Push will send a generic event to the VMS for each camera that is enabled.

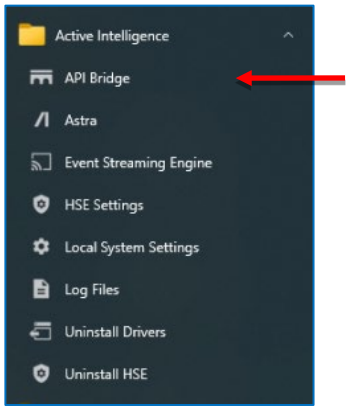
Generic Events for ASTRA can be added as a function of the VMS (not ASTRA) as necessary for the end-user's operations from the Management Client:

Generic events allow the system to trigger actions in the "event server". Some examples include:

- External events – User-defined events
- System Monitor events
- Trigger Alarms
- Send an Email or Text
- Events from add-on products and integrations

Reference the VMS manual for instructions on creating rules and alerts based on Generic Events.

Generic Events are sent automatically when the API Bridge receives an event from the ASTRA engine IF the "Push" checkbox is selected for the Camera that is sending the Generic Event on the License Page.

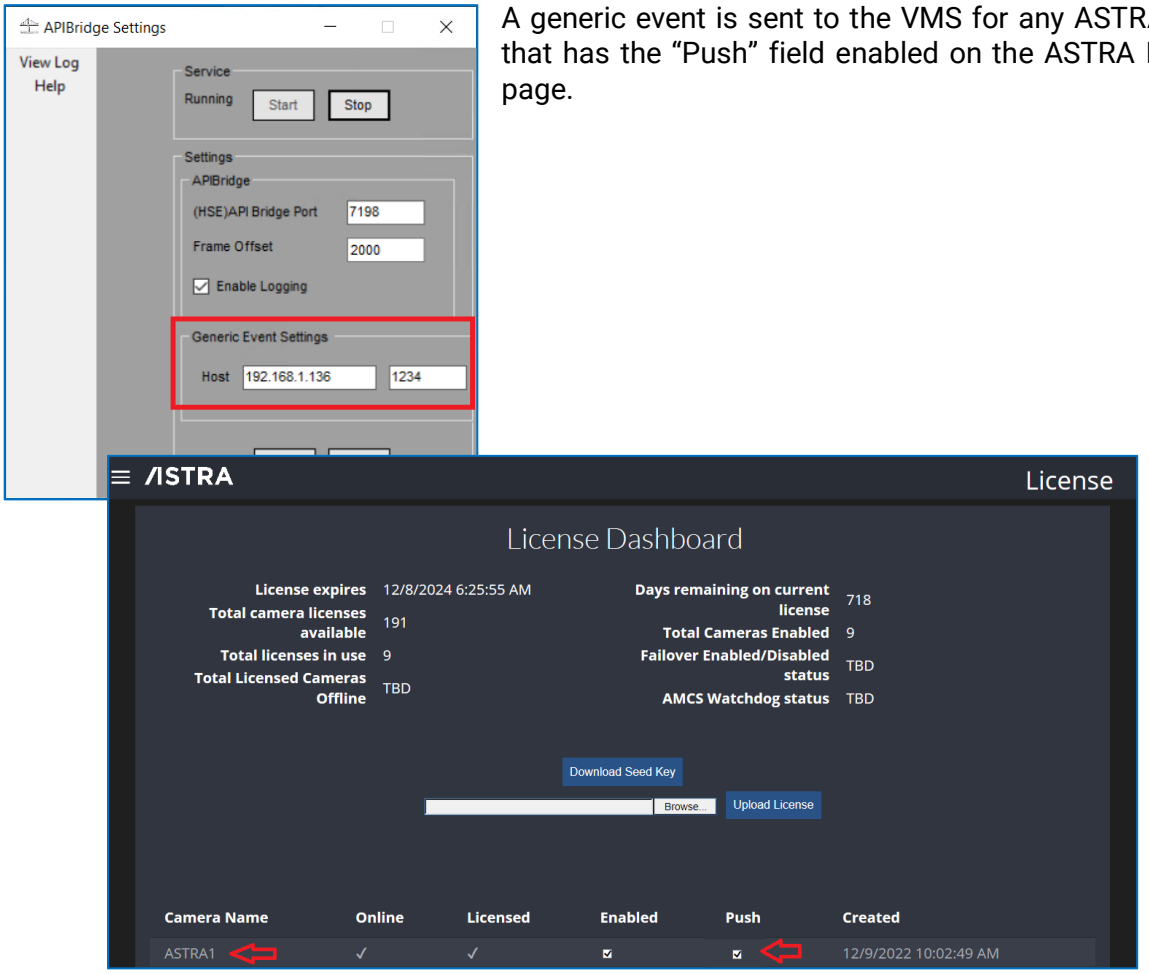


The API Bridge is what sends the Generic events to the VMS. The API Bridge is installed on the machine that has the ASTRA service installed. Open the API Bridge Settings from:

Windows Start menu > Active Intelligence

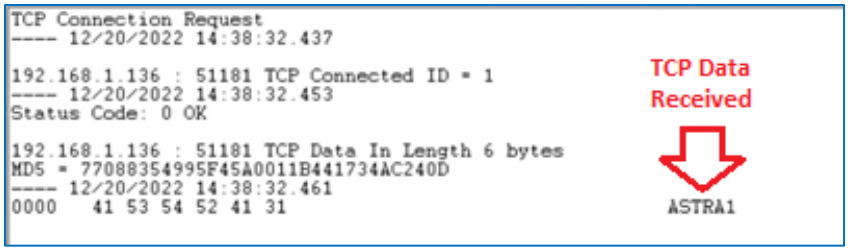
Go to the Generic Events section and change the IP address to be the IP address of the machine hosting the VMS Generic Events listener and set the port number to be what the VMS is listening on for Generic Events.

Once this is done, be sure to restart the APIBridge service using the controls in the APIBridge GUI.



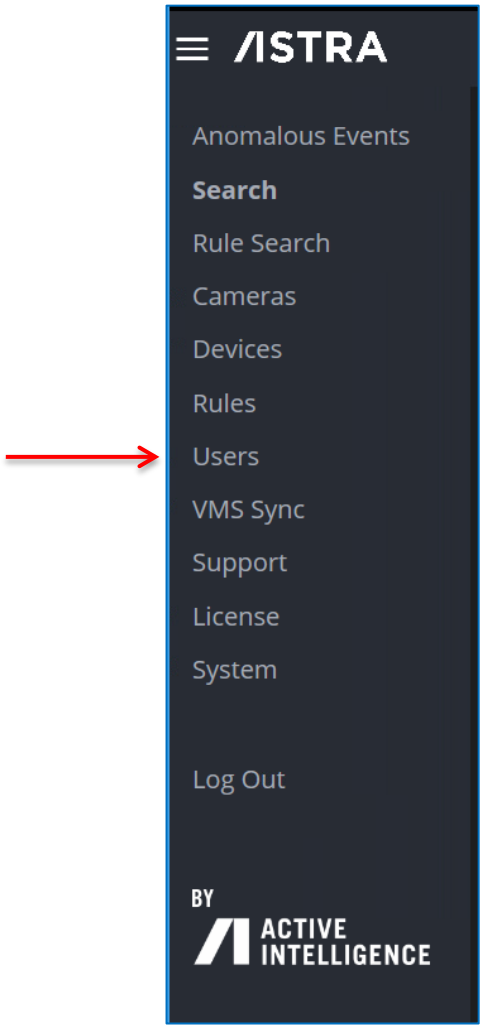
A generic event is sent to the VMS for any ASTRA event that has the “Push” field enabled on the ASTRA License page.

Note: The camera stream must be Online, Licensed, and Enabled before it can generate a Generic Event. The TCP listener example below shows the actual TCP data that was sent. In this case the camera name was ASTRA1.



ASTRA License Page User Manager

To get to the User Manager select the dropdown menu ≡ and select “Users”.

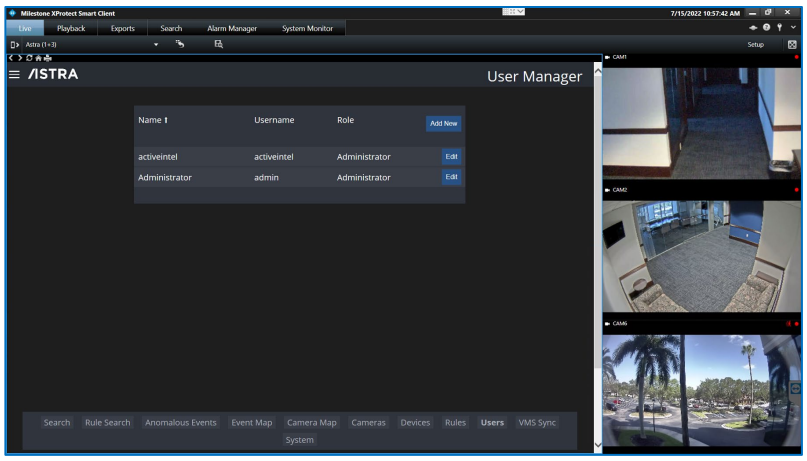


This is where the administrator can add or delete accounts and assign permission levels for all accounts.

There are three levels of authorizations:

- Administrator
  - Administrator can add /remove users, change passwords, authorization levels and make changes within the pages of the HSE.
- Manager
  - Managers have the same rights as the administrators, but they cannot add / delete users or change authorizations levels.
- User
  - Users can only view pages in the HSE. They cannot make any changes to the pages.

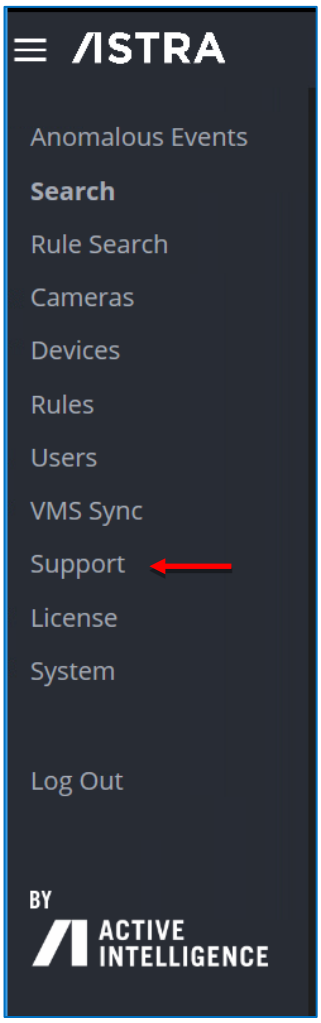
This page allows the administrator to change login passwords.

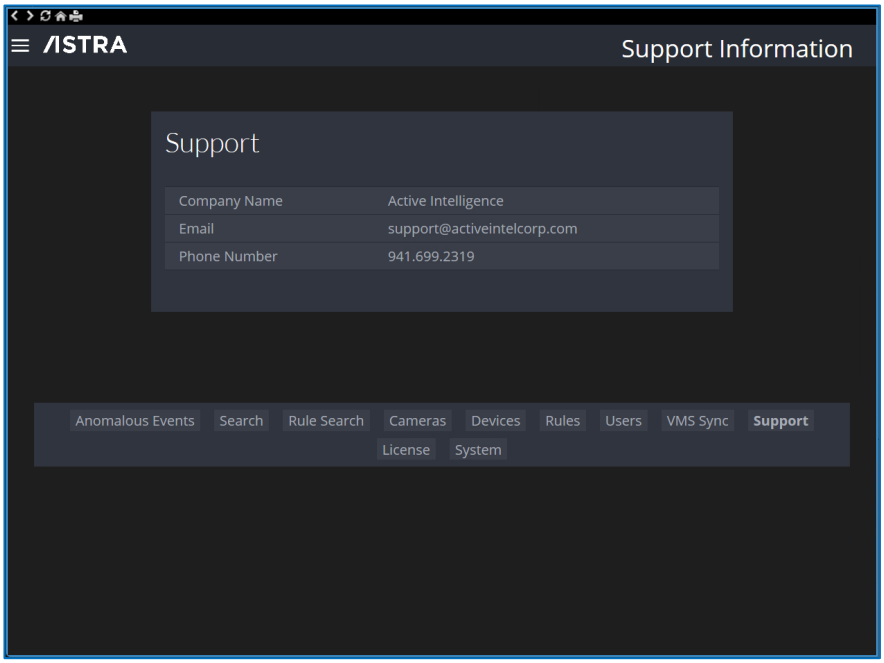


Support

To get to the Support page select the dropdown menu ≡ and select “Support”.

The support tab provides quick access to the ASTRA Technical Support team contact information.

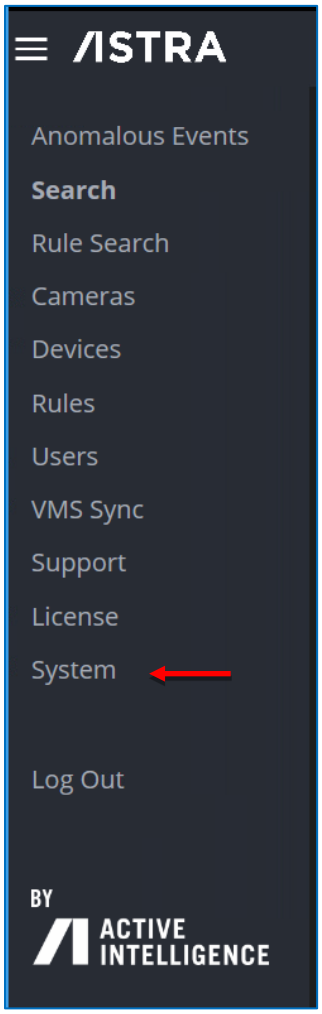


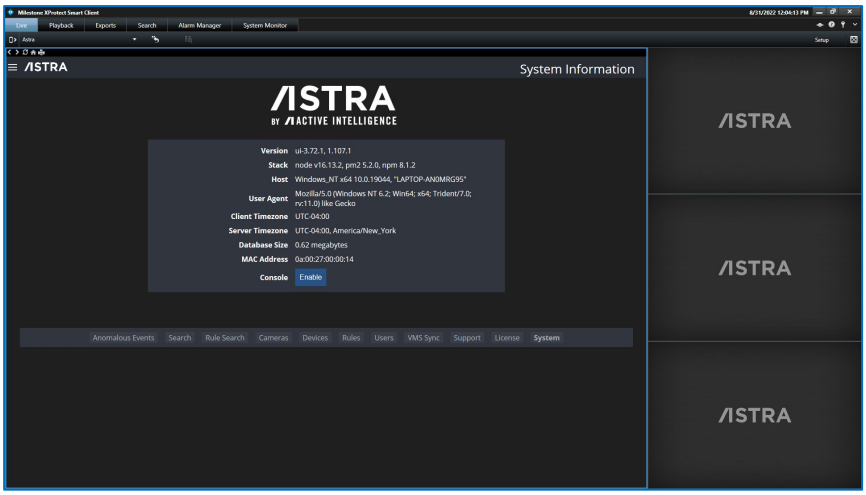


System

To get to the System Information page, select the dropdown menu ≡ and select “System”.

The System Information page shows information that may be requested by technical support during troubleshooting, like version, host, MAC addresses, and more.

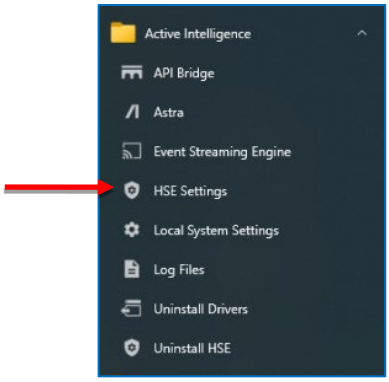




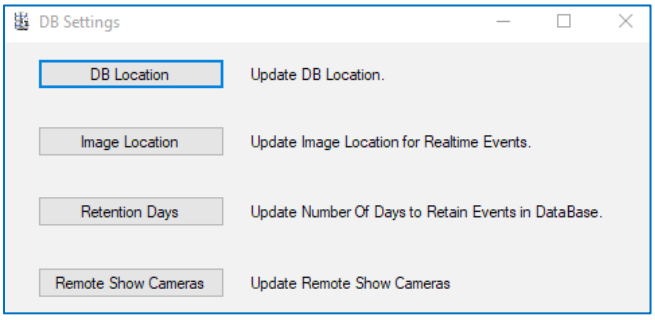
HSE Settings

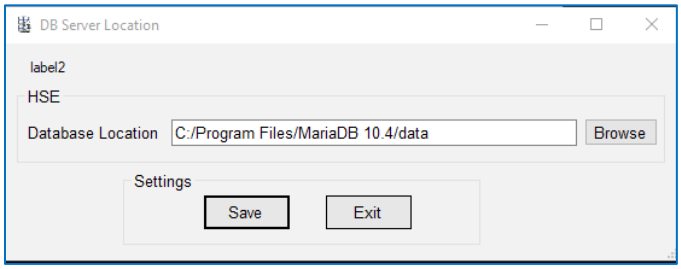
To bring up the HSE database (DB) settings table go to:

Windows Start > Active Intelligence > HSE settings



This is used to see the HSE database location, where the snapshots are stored for Anomalous Events, and how many days the HSE data is retained.

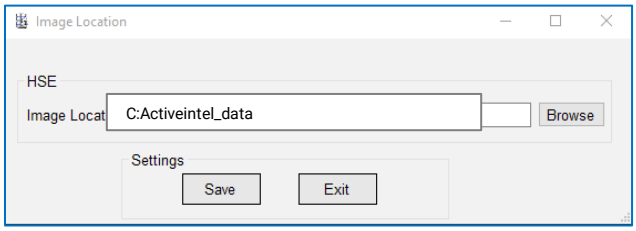




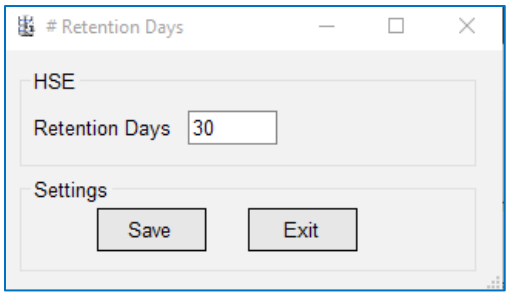
Note: To verify that data is being sent to the HSE database, go to the "Search" or "Anomalous Events" page in the HSE, or go to the HSE Log file found in the folder ConvergenceTP > Logs > DB Log.

“Image Location” sets the location for all ASTRA Anomaly Events that have been received to be saved as JPEG images.

The default folder is C:/Activeintel/data, however, this location can be changed if desired.



Use the Retention Days field to change the HSE database retention time from the default 30 days to another value. If changed, make sure to select the save button before continuing.



Note: The HSE Retention Days MUST be set at the same number of days as the VMS retention storage time(minimum). This will prevent the instance of anomalies without associated video.

TCP Ports Used

Windows firewall exceptions need to be made for the ports listed.

1234 – _Milestone Generic Event Server Default Port
7250 – _ASTRA ASTRA interface module
7341 – _ASTRA License Server
8990 – _ASTRA HSE API port
8991 – _ASTRA HSE web interface

Reports

The ASTRA server stores incident reports that are created and retrieved using its Anomaly Information Management System via the search function.

Several reports can be generated with the drop-down menus.

The first drop-down menu has selection options for:

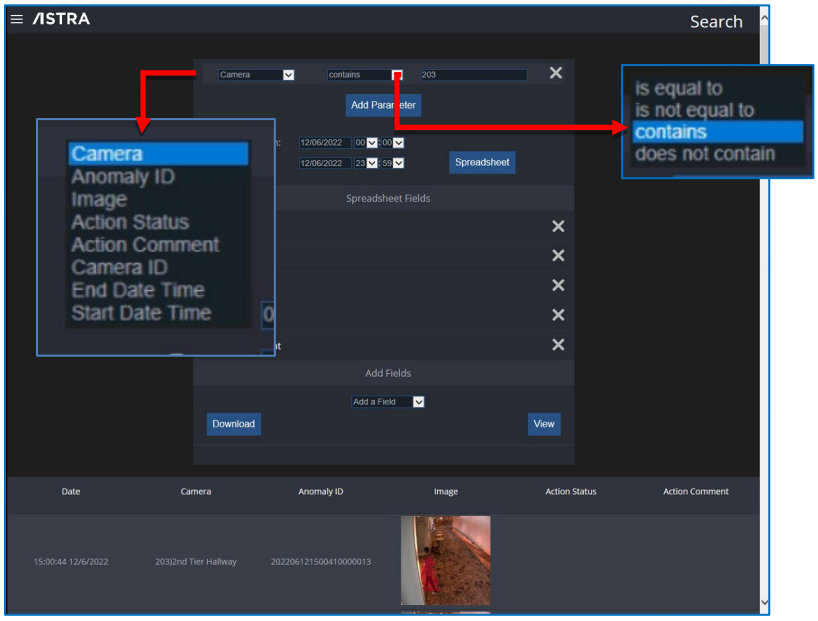
- Camera,
- Anomaly ID
- Image
- Action Status
- Action Comment
- Camera ID
- End date
- Time
- Start Date Time.

The second drop-down menu has selection options for:

- is equal to
- is not equal to
- contains
- does not contain.

The third box is a mandatory text field where the text of what is sought is entered.

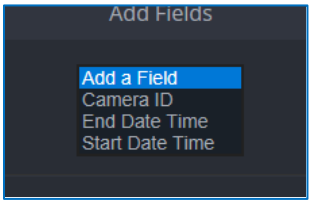
A report can also be generated by start / end date and start / end time.



Additional items seen in the camera drop-down list can be selected via “Add Parameters”. By selecting “Add Parameters”, all the items shown in the drop-down list are displayed. Here, the items not desired can be removed from the report by using the “X on the right.

When the “Spreadsheet” button is selected the following options: “Add Fields”, “Download” and “View” are displayed.

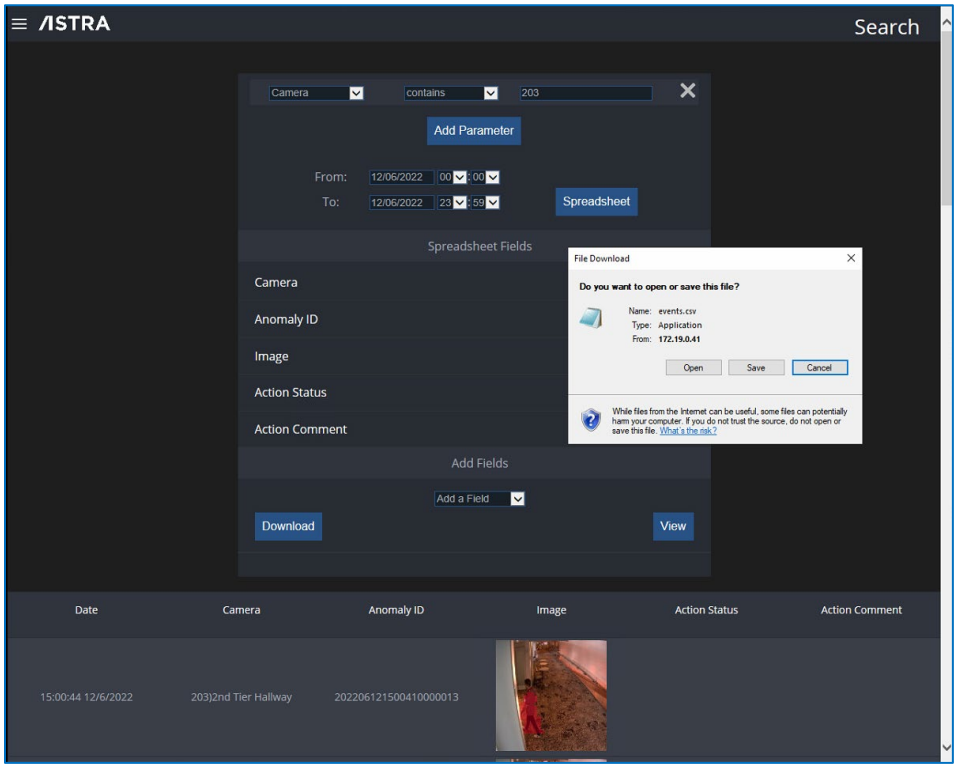
The “Add Field” drop-down menu allows “Camera ID”, “End Date Time”, or “Start Date Time” to be added. Any or all items in the drop-down menu can be added.



To view the report there are two options:

“Download” creates a .csv file that can be opened or saved.

“View” allows the user to review the report to ensure the necessary information is included. This can then be saved or closed.



Search results are displayed in the bottom field with the columns that were selected in the drop-down menus.

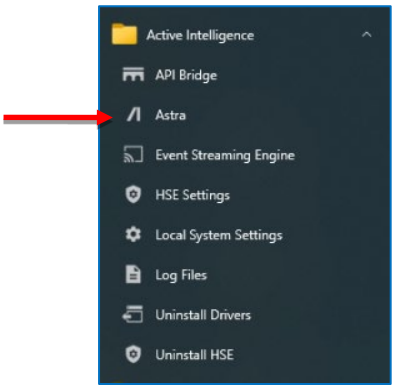
Settings

ASTRA program settings can be launched from the desktop icon:

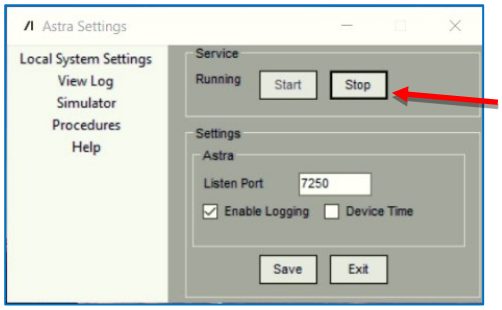
ASTRA

Or by going to the Windows menu:

Windows Start Menu > Active Intelligence > ASTRA

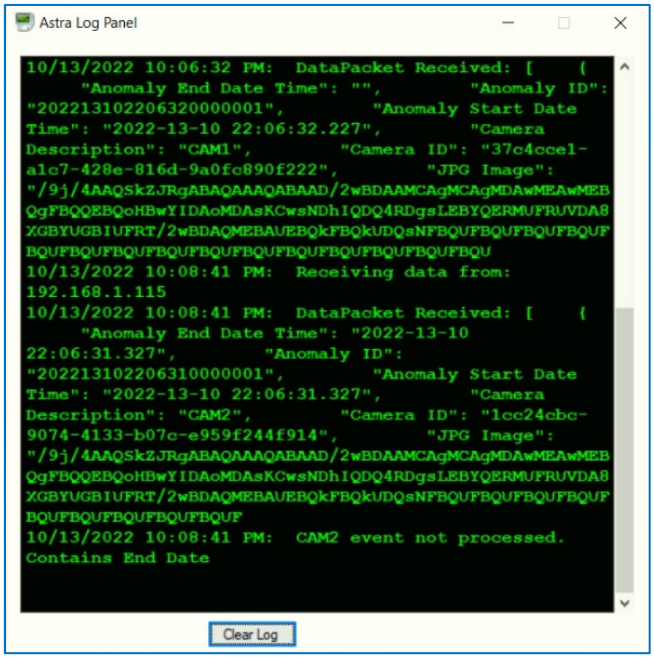


Whenever any changes are made and saved in the ASTRA Settings, the ASTRA Service must be “Stopped” and “Started” for the changes to be applied. This is done using the Service Stop and Start buttons shown below. After the service is started, select “Save and Exit” from ASTRA Settings.



The ASTRA Log File can be extremely useful for testing all the components in the ASTRA integration.

Select “View Log” on the left side of the ASTRA Settings menu screen.



Professional Services

Active Intelligence offers a full range of Professional Services to Authorized Channel Partners and their clients.

These services include:

- Installation And Migration Services
- Upgrade Services
- System Audits and Configuration Services
- System Troubleshooting Services
- Technical Consultation Services
- Technical Training
- Annual Maintenance Plans

Consult the Professional Services documentation for descriptions and pricing information.

How to get Support

The Active Intelligence Authorized Channel Partners are the first level of support to their customers. Therefore, customers should first contact the Authorized Channel Partners for assistance with questions.

Active Intelligence Technical Support is typically available **Monday – Friday, 9:00 am – 5:00 pm Eastern Time Zone**, excluding most Holidays.

Technical issues that can be resolved by email and phone are handled at no additional charge. If the problem cannot be resolved by email and over the phone, Professional Services are required. This is a paid service – contact your Active Intelligence Technical Support Representative for pricing information.

Active Intelligence Authorized Channel Partners can contact support in three ways:

Email: support@activeintelcorp.com

Phone: 941-699-2300, option 1

Web: www.activeintelligencecorp.com/support

Email Support:

Use the subject line to concisely describe the issue your client is facing. If the email is a follow-up with an existing ticket number, include the ticket number in the subject line.

In the message body, please include the following information:

- Contact information including full name and phone numbers
- Authorized Channel Partner name (contact information, phone number/email address)
- End User name
- License information

Provide as much detailed information as possible, including versions of ASTRA, the VMS software, system information, model numbers, and any screenshots showing the issue or errors messages.

The more detailed information provided in the support request, the faster our team can get started resolving the issue at hand.

Phone Support

When telephone support is required, call: ***941-699-2300,*** then press the extension for Support (option 1). When available, a support representative will answer your call. If the support team is on another call, yours will be placed into the queue and the next available support representative will answer the call in the order it was received.

Please be patient as each support issue is unique and no time limit is placed on our quality of service (QoS) to solve the issues. If you hang up, you will lose your place in the queue.

Additional resources:

Sales: sales@activeintelcorp.com; 941-699-2300, option 2

Sales Engineering: saleseng@activeintelcorp.com; 941-699-2300, option 4

Active Intelligence Website: www.activeintelligencecorp.com

ASTRA Documentation: www.activeintelligencecorp.com/resources

18501 MURDOCK CIRCLE
SUITE 602
PORT CHARLOTTE,
FL 33948
ACTIVEINTELLIGENCECORP.COM