Initial ACC™ System Setup and Workflow Guide

If you are setting up an Avigilon Control Center (ACC) system for the first time, complete the following recommended setup procedures. Other features can be set up and adjusted as required.

For an overview of the procedures that should be performed before you arrive at site, see *Pre-Site Checklist* on page A.

For an overview of the procedures that should be performed at site, see *System Setup Checklist* on page C.

More detailed information about each of the procedures in this guide is available in the *Avigilon Control Center Client User Guide*.

Before Arriving On-Site

To make system setup more efficient, it is highly recommended that you pre-configure the network video recorders as much as possible, be familiar with the system design and the customer network setup.

For more information, see *Pre-Site Checklist* on page A.

Install Hardware and Software

Cameras and Devices

Install the cameras and devices according to the system design. Each device must:

- Be connected to the network.
- Be aimed and focused in the direction specified in the system design.
- Be assigned a descriptive name.
- Be assigned an IP address (static or dynamic depending on network policy).

Before a camera is connected to the ACC system, it can be configured from the camera web interface or from the Camera Configuration Tool.

Refer to the device's installation guide for more information.

Video Recorders

Install the video recorders. An ACC system can feature network video recorders (NVRs), HD Video Appliances, ACC ES HD Recorder or ACC ES Analytics Appliance. Each video recorder must:

- Be connected to the network — camera and corporate network as required.
- Be configured for NTP time synchronization.
    - Set the date and time.
- Be assigned a descriptive name.
- Be assigned an IP address.
- Be assigned a new password for the administrator account on the NVR.

Refer to the recorder installation guide for more information. If you are installing a Windows based NVR system, see the Windows help files for more information.

Avigilon Control Center™ Software

If you have an Avigilon NVR installed in your system, the ACC software is pre-installed. When you start the NVR, complete the initial ACC configuration wizard.

NOTE: The ACC analytics service is not pre-installed and is required for Avigilon Appearance Search feature applications.

If you installed a third-party NVR in your system, download and install the ACC Server software and ACC Client software. The software can be downloaded from the Avigilon website: **avigilon.com/support-and-downloads/**.

Configure Anti-Virus Settings

When anti-virus software runs an automated scan on a heavily utilized Avigilon server or workstation, it may prevent video data from being written. Some anti-virus software packages are equipped with live process scanning and incorporated firewalls. These features may cause communication failures between cameras and servers or between servers and clients.

You may need to set up exceptions in the anti-virus software running on servers, workstations or clients within the ACC system. For more information on how to exclude locations and applications from being scanned, see your anti-virus software manual.

Preventing Data Write Issues

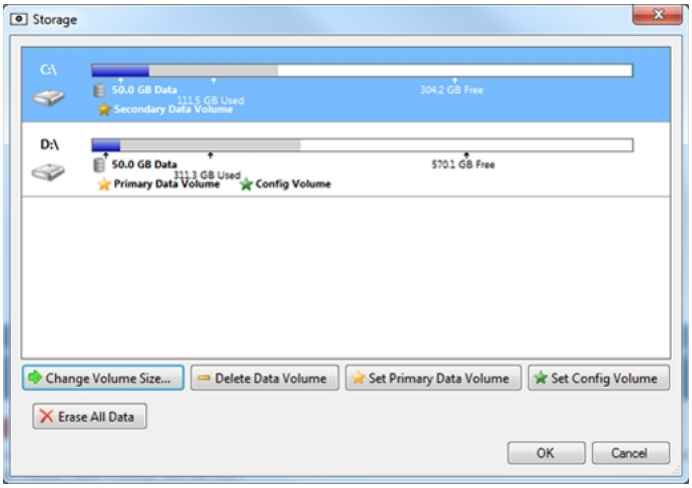
To ensure the anti-virus software does not interfere with the ACC software's ability to write video data and other important files, exclude the following locations from being scanned:

AvigilonData	Located on each of the Primary and Secondary Data Volumes.*
AvigilonConfig	Located on each of the Config Volumes.*
Avigilon Program Files	Located at `C:\Program Files\Avigilon`.

*To see which drives are configured as the Primary and Secondary Data Volumes and Config Volumes, use the ACC Admin Tool.

- In the Admin Tool, click **Settings > Storage**.

  The Primary and Secondary Data Volumes and Config Volumes are displayed.



Preventing Network Communication Failure

To prevent communication failure, exclude the following from having their network traffic scanned or analyzed:

- ACC Server Applications:
  - `C:\Program Files\Avigilon\Avigilon Control Center Server\VmsAdminPanel.exe`
  - `C:\Program Files\Avigilon\Avigilon Control Center Server\VmsAdminPanelLauncher.exe`
  - `C:\Program Files\Avigilon\Avigilon Control Center Server\VmsDaemonService.exe`
- ACC Client Applications:
  - `C:\Program Files\Avigilon\Avigilon Control Center Client\VmsClientApp.exe`
- Avigilon Data folder
  - `C:\AvigilonData`

Activate Site Licenses

After you install all the physical components in your ACC system, you must activate a site license to use all the application features.

You have the option of activating a demo license to evaluate the system feature set, or activating a full license that you have already purchased.

Activating a License for the First Time

If you just installed an ACC Server, you can choose to activate a demo license to test Avigilon Control Center features, or activate a purchased license to begin using your ACC system for normal operations.

Demo licenses allow you to use ACC software for a limited amount of time to evaluate the software. Once the demo period ends, the license expires and you will no longer be able to use the ACC software until a formal license is activated.

NOTE: Be aware that a demo license is automatically removed when you activate a formal license, or join a server with a demo license to a new site.

Purchased licenses do not expire, and allow you to join multiple servers to form larger sites in Enterprise systems.

Tip: Join multiple servers to form a site before activating your licenses to avoid the need to reactivate your license each time a different server is joined into the site.

1. At the top-left corner of the application window, click  to open the New Task menu then click  .
2. In the Setup tab, select your new site then click  .

   The License Management dialog box is displayed.

To...	Do this...
Activate a demo license	a. Click **Request Demo License...**. b. In the following dialog box, select the preferred license edition.
Activate a purchased license	a. Click **Add License...**. b. In the following dialog box, enter the product key. A check mark will appear if the product key is valid.

   - If you have internet access, select the **Automatic** tab.

     To complete activating the license through this tab, see *Automatic Licensing* on the next page.
   - If you do not have internet access, select the **Manual** tab.

     To complete activating the license through this tab, see *Manual Licensing* on the next page.

Automatic Licensing

NOTE: You must have internet access to use this method.

1. Open the License Management dialog box then initiate the licensing task that you want to perform.
2. At the top of the following dialog box, select the **Automatic** tab.
3. If you are activating a license, you will be prompted to enter a license key or select the preferred demo license edition.
4. Click the button that will immediately apply your license changes.

Manual Licensing

1. Open the License Management dialog box then initiate the licensing task that you want to perform.
2. At the top of the following dialog box, select the **Manual** tab.
3. If you are activating a license, you will be prompted to enter a license key or select the preferred demo license edition.
4. Click **Save File...** .
5. From the Save As window, choose where you want to save the `.key` file that is generated by the system. You can rename the file as required.
6. Click **Save**.
7. Copy the `.key` file to a computer with internet access.
8. Open a web browser and go to **http://activate.avigilon.com**.

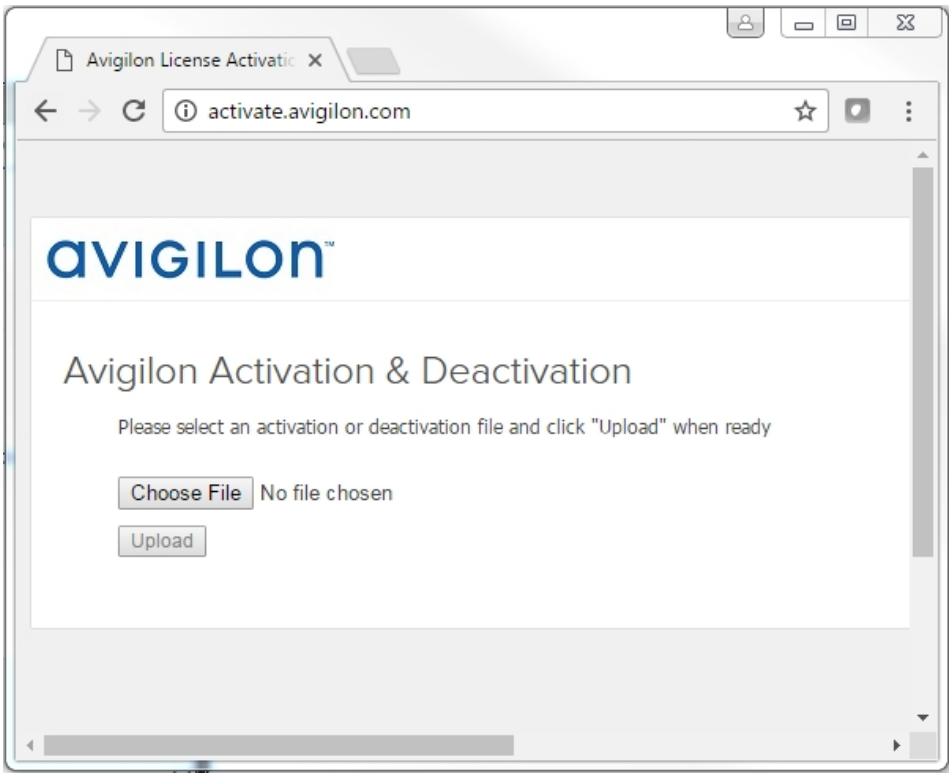


Figure 1: The Avigilon License Activation web page

9. Browse to the location of the `.key` file then click **Upload**.

   The generated license file (`.lic`) should download automatically. If it does not, allow the download to occur when you are prompted.

10. Copy the downloaded `.lic` file to a location that would be accessible to the ACC Client software.
11. Complete the product registration page to receive product updates from Avigilon, then click **Register**.

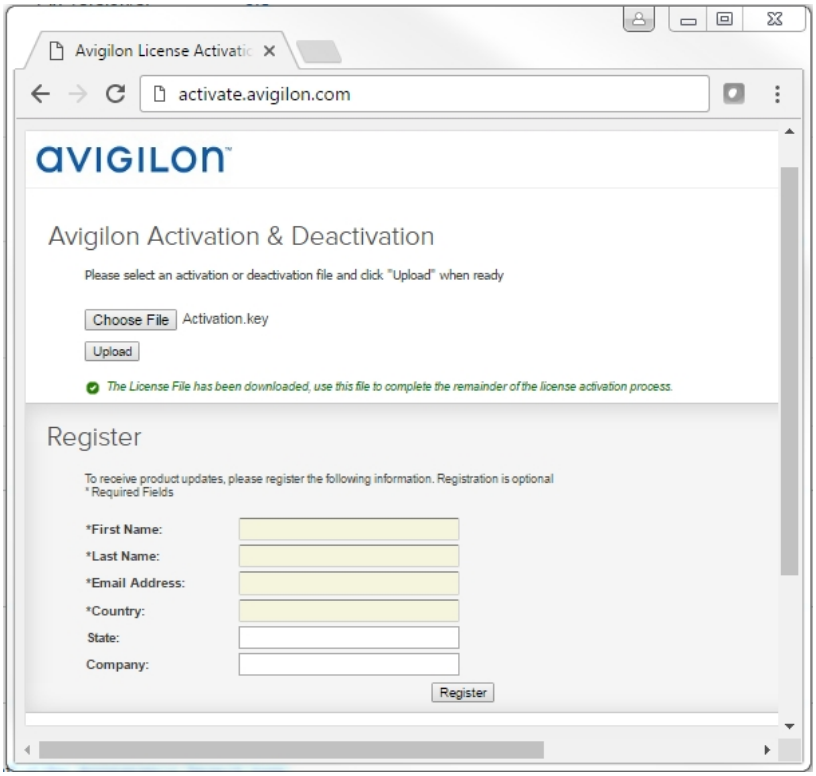


Figure 2: The product registration web page

12. Return to the ACC Client and click **Apply...**.
13. Locate the downloaded `.lic` file and click **Open**.
14. When the Confirm Licenses dialog box is displayed, click **OK**.

Configure Sites and Servers

In the Avigilon Control Center software, servers are organized in clusters called sites. By organizing the system into clusters, you are able to control user access and system wide events through the site settings. Site settings are stored on the server, or across all servers in a multi-server system.

Depending on your system and license edition, you may have multiple servers in a site. When there are multiple servers in a site, the site is able to distribute tasks and system data between the servers so that the system can continue running even if a server fails.

Within a site, each individual server is responsible for managing the devices that are connected to it. Specifically, the server controls video recording. Through the server settings, you control when video is recorded, how long it is stored, and how much bandwidth is used to stream video.

Start configuring and managing sites and servers by completing the following procedures.

Connecting Servers to Sites

By default, each site only has one server but you can add multiple servers to a site so that they can be managed together. All servers within the site share settings and are represented as one unit in the System Explorer.

Tip: It is recommended that you only add new servers to an existing site to avoid managing a large number of duplicate settings, and more easily configure device connections across the combined site.

This procedure is primarily for grouping a number of servers in the same local area network to work together and share settings.

If the servers are installed a wide distance apart but only need to share users and group information — you can join the sites together into a site family instead. For more information, see *Connecting Site Families* on the next page.

1. In the site Setup tab, click  .

   The Site Management tab lists all the sites that you can access and all the servers that are connected to each site.

   If you do not see the site or server you want to configure, you may need to add the site.

2. When you select a  server, you will see the available options at the bottom of the application window.
3. To move a server:
   - Select the  server and drag it to a different site.
   - Or, select the  server then click **Connect to Site...** at the bottom-right corner of the tab. In the following dialog box, select the site you want the server to connect to.

   NOTE: Sites without any servers are automatically removed from the list.
4. After the server has joined the new site, reactivate the site licenses.

Once the server is connected to the site, the settings are merged.

- Unique settings from the server are added to the site.
- If the settings are identical, only the site version is kept.
- If a server setting and a site setting have the same name but are configured differently, the server setting is added to the site and renamed in this format: *<setting name> (server name),* e.g. Email1 (Server2F).
  - In the rules engine, the *Notify users (default)* rule is always added and renamed, even if the settings are the same. The site version remains enabled but the added rule is disabled by default.
- The two site Views are combined.
  - The site settings take precedence.

    For example, a map from the site was copied to the server in the past. In the server, the map was placed at the top of the site View. But in the site, the same map is placed at the bottom. After the server is connected to the site, the map takes the position used by the site at the bottom.
  - New, unorganized elements from the server are listed at the bottom of the site View.
- User permission groups are merged.

    - If groups have the same name, the site settings are used and the users from both the site and the server are added to the group.
    - Groups that are new to the site automatically get access to all the devices in the site.
    - Groups that are new to the server automatically get access to all the devices that are connected to the server.
- Users with the same name will use the settings configured in the site (including passwords), and gain group permissions from the server.
- If the site is connected to a Windows Active Directory, the server must be connected to the same Active Directory domain or the connection will fail.

Connecting Site Families

Site families are sites that are connected together into a hierarchy. Sites are still managed independently, but user and group information is centrally managed by the parent site.

Child sites are connected to a parent site to create a site family. Once set up, all ranked user and group privileges on the parent site are applied to the child sites and controlled from the parent site. The child site can still define local users and groups.

NOTE: A parent site can have multiple child sites, but a child site can only have one parent site. You must be logged in to both potential parent and child sites before you can connect them.

Only Enterprise sites can be parent sites. Each parent site can have up to 1 Core site, 24 Standard sites and unlimited Enterprise sites as child sites.

1. In the site Setup tab, click  .

   The Site Management tab is displayed.
2. Select the  site you want to connect as a child site.
3. In the bottom-right corner of the tab, click **Connect to Parent Site**.

   Tip: If you selected a  server instead of a site in the previous step, you will only have the option to Connect to Site....
4. In the following dialog box, select the parent site from the **Connect to:** drop-down list.
5. In the **Rank:** drop-down list, select a rank for the child site. To edit or view the entire Corporate Hierarchy, click  .
6. Click **OK**.
7. In the confirmation dialog box, click **Yes**.

Naming a Site

Give the site a meaningful name so that it can be easily identified in the System Explorer. Otherwise, the site uses the name assigned to the server it was originally discovered with.

1. In the site Setup tab, click  .
2. In the following dialog box, enter a name for the site.
3. Click **OK**.

Naming a Server

Give the server a meaningful name so that it can be easily identified in the System Explorer. Otherwise, the server uses the name that is assigned by Windows.

1. In the server Setup tab, click  .
2. In the following dialog box, enter a name for the server.
3. Click **OK**.

Editing the Site View

You can edit the way your site is organized in the View tab so that it reflects how your system is set up.

By default, all cameras are listed in alphabetical order by site in the System Explorer. Through the Site View Editor, you can organize the System Explorer to display cameras by location and group items for convenience, or hide cameras that are not relevant to an ongoing investigation.

NOTE: These settings only affect the System Explorer in the View tab.

1. In the site Setup tab, click  .

   The Site View Editor dialog box is displayed.

   NOTE: The site name is not displayed because it cannot be moved or re-organized. In the System Explorer, the site is always displayed at the top.

2. Change the site View layout as required.
   - Click to add a New Folder. The New Folder is displayed with a icon for organizational purposes only and is only visible from the View tab.

     Double-click the New Folder field to change the name.
   - To move one element, select the listed element then use the green arrows to move it up and down the list, or move it under a folder.
   - To move multiple elements, select more than one element then drag them up and down the list together, or under the same folder.

- To show or hide the elements under a folder, click the arrow on the left to expand or collapse the folder.

  This setting determines what users see each time they log in to the site. The user can still collapse or expand folders in the System Explorer.

- To sort a folder, select an element then click to sort that folder level into alphabetical order.
- To delete a folder, select the folder then click .

3. Click **OK** to save your changes.

When you open a new View tab, the System Explorer displays your latest changes.

Configure Devices

After the site and servers have been configured, connect cameras and other devices to the system. Once connected, you can adjust the camera's image quality, video analytics and other video recording settings.

Connecting a Device to a Server

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

To access a device from a site, it must be connected to a server within the site. The server manages and stores the camera's recorded video, while the site manages the events that are generated by a connected device (such as an Avigilon Presence Detector sensor) or from the camera's video .

After a device has been discovered on the network, it can be connected to the server.

1. In the site Setup tab, click .

   The Connect/Disconnect Devices... tab is displayed.

2. In the Discovered Devices area, select one or more devices then click **Connect...**.

   Tip: You can also drag the device to a server on the Connected Devices list.

3. In the Connect Device dialog box, select the server you want the device to connect to.

   NOTE: If you are connecting multiple devices, all the cameras must use the same connection settings.

4. If you are connecting a third-party device, you may choose to connect the device by its native driver. In the **Device Type:** drop-down list, select the device's brand name. If there is only one option in the drop-down list, the system only supports one type of driver from the device.
5. If the camera supports a secure connection, the **Device Control:** drop-down list is displayed. Select one of the following options:

   NOTE: The setting may not be displayed if the camera only supports one of the options.

- **Secure** — The system will protect and secure the camera's configuration and login details. This option is selected by default.
- **Unsecure** — The camera's configuration and login details will not be secured and may be accessible to users with unauthorized access.

  Cameras with a secure connection are identified with the icon in the Status column.

6. If it is not displayed, click to display the Site View Editor and choose where the device appears in the System Explorer.
   - In the site directory, drag devices up and down the right pane to set where it is displayed.
   - If your site includes folders, select a location for the device in the left pane. The right pane updates to show what is stored in that directory.
   - If you are connecting multiple devices at the same time, the selected devices must be assigned to the same location.

   Tip: If the site you want is not listed, you may need to connect the device to a different server. Make sure the selected server is connected to the site you want.
7. Click **OK**.
8. If the device is password protected, the Device Authentication dialog box appears. Enter the device's username and password, then click **OK**.

Configure Video Analytics

If the connected device supports video analytics, enable and configure cameras to perform classified object detections.

After you enable video analytics, you will need to configure classified object motion detection and video analytic events before the system can trigger video recording and alarms based on the video analytics. If the system you are installing will be using the Avigilon Appearance Search™ feature, remember to enable each required camera to support this feature.

Enabling Server-Based Analytics

Server analytics is an ACC ES Analytics Appliance feature that allows video analytics to be performed for cameras without self-learning video analytics capabilities.

1. In the server Setup tab, click  .
2. In the following dialog box, a list of connected cameras are displayed.

   Only cameras without video analytics capabilities are displayed.

   If you do not have access rights for a camera, it will not be shown in this list.
3. To enable video analytics, select the check box beside the connected camera.

   The Total Analytic Load bar displays the appliance's video analytics capacity. The percentage is based on the enabled camera's current Compression and Image Rate settings.

4. Click **OK**.

   Your settings are now saved.

Video analytic events can now be set up for the enabled cameras from the camera's Setup tab.

Configuring Classified Object Detection

Cameras with Classified Object Detection video analytics and cameras connected to ACC ES Analytics Appliances can be configured to better understand the scene where they are installed and improve classified object detection accuracy. This allows cameras to learn their surroundings and detect specific events.

To configure Classified Object Motion Detection for a video analytics camera, see *Setting Up Classified Object Motion Detection* on page 21.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the device Setup tab, click  .

   The Settings dialog box opens.

2. From the **Analytics Scene Mode:** drop-down list, select the location that best describes where the camera is installed.

   The Analytics Scene Mode: setting helps the camera identify what it should be looking for.

   - **Outdoor** — this option is suitable for most outdoor environments. This setting optimizes the camera to identify vehicles and people.
   - **Outdoor High Sensitivity** — only use this option if you require the system to be more sensitive than the Outdoor setting. This option is optimized to run with higher sensitivity for detecting people and vehicles in challenging outdoor scenes. Be aware that this option will generate more false positives.
   - **Large Indoor Area** — this option only detects people and is optimized to detect people around obstructions, like chairs and desks, if the head and torso are visible.
   - **Indoor Overhead** — this option is optimized for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera FoV. Any movement is assumed to be human. It can be used in areas with limited space but with high ceilings, or to monitor doors. It should not be used with the Avigilon Appearance Search feature, or to detect people traveling against the crowd.

   NOTE: If you change the Analytics Scene Mode: setting after it has been set, the system will delete any data the device may have learned.

3. Select the **Display Classified Objects** check box to display bounding boxes around classified objects in live and recorded video.

4. In the Self Learning section:
    1. Check the **Enable Self Learning** box to enable self-learning.
    2. Clear the check box to disable self-learning. After self-learning is disabled, the camera stops self-learning and no longer utilizes any learned information.

       NOTE: Disabling self-learning may result in more classified objects being falsely detected.
    3. The Progress: status in the dialog box tells you the progress made so far.
    4. To reset self-learning, click **Reset**.
        - In the confirmation dialog box that appears, click **Yes**.

       NOTE: When self-learning is reset, all previous self-learning data for the device is deleted.
5. In the **Camera Type:** drop-down list, select the type of camera that has been connected to this camera channel.

   This helps the video analytics determine what type of image it should expect from the camera.

    - **Day and Night** — select this option if the camera can stream video in color or black and white. This type of camera typically displays color video during the day and black and white video at night to capture as much detail as it can of the scene.
    - **Color** — select this option if the camera can only stream video in color.
    - **Black and White** — select this option if the camera can only stream video in black and white.
    - **Thermal** — select this option if the camera can stream forward looking infrared (FLIR) video.
6. Move the **Sensitivity:** slider to define how sensitive the camera is to sudden changes in the scene.

   Tampering is defined as a sudden change in the camera field of view, usually caused by someone unexpectedly moving the camera. Lower the setting if small changes in the scene, like moving shadows, cause tampering events. If the camera is installed indoors and the scene is unlikely to change, you can increase the setting to capture more unusual events.
7. Select the **Trigger Delay:** value to define how long the camera will wait for tampering events to be sent.

   Trigger delay is defined as a temporary change in the camera field of view that may generate a tampering event due to a change in the scene. If the tampering ends before the trigger delay time has elapsed, no tampering events will be sent. If the time elapses but the tampering has not stopped, the events will be sent by the camera. The default setting is **8** and is a value in seconds from **2** and **30**.
8. Select the **Enable Appearance Search** check box if you want to use this camera with the Avigilon Appearance Search feature.

   NOTE: This option is only displayed if the camera is connected to a network video recorder that supports the Avigilon Appearance Search feature.
9. If the camera is too sensitive and falsely detects motion as classified objects, select the **Enable Noise Filter** check box .

   Disable this option if the camera is not sensitive enough.
10. Click **Apply** to save your settings.

Next, you can enable self-learning and configure analytics events. .

Configuring Rialto™ Video Analytics Appliances

To use a Rialto video analytics appliance, configure each connected camera channel for video analytics detection.

If you are configuring an analog video analytics appliance, the cameras are physically connected to each camera channel before the appliance is connected to the system.

If you are configuring an IP video analytics appliance, any camera on the network can be digitally connected to the appliance camera channels. Before you complete this procedure, connect the required cameras first.

NOTE: Rialto video analytics appliances do not support the Avigilon Appearance Search feature. Cameras connected to Rialto appliances do not have the option to be enabled for the feature.

1. Open the Setup tab, then select one of the appliance camera channels.
2. In the device Setup tab, click  .

   The Analytic Events dialog box opens.
3. Assign a camera to the channel.

   Skip this step if you are configuring an analog appliance.

   - From the **Linked Camera:** drop-down list, select a camera for this camera channel.

     Only cameras connected to the same server are listed.

     NOTE: If the camera you link to has a resolution higher than 2.0 MP, the video analytics appliance will use the camera's secondary video stream. This does not affect the resolution of recorded video.

     After you select the camera, the dialog box expands to display the video analytic event settings.
4. From the **Analytics Scene Mode:** drop-down list, select the location that best describes where the camera is installed.

   The Analytics Scene Mode: setting helps the camera identify what it should be looking for.

   - **Outdoor**— this option is suitable for most outdoor environments. This setting enhances the camera to identify vehicles and people.
   - **Large Indoor Area** — this option only detects people and is enhanced to detect people around obstructions, like chairs and desks, if the head and torso are visible.
   - **Indoor Overhead** — this option has enhanced value for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera FoV. Any movement is assumed to be human. It can be used in areas with limited space but with high ceilings, or to monitor doors.
   - **Outdoor High Sensitivity** — only use this option if you require the system to be more sensitive than the Outdoor setting. This option is enhanced to run with higher sensitivity for detecting people and vehicles in challenging outdoor scenes. Be aware that this option will generate more false positives.

   NOTE: If you change the Analytics Scene Mode: setting after it has been set, the system will delete any data the device may have learned.

5. In the **Camera Type:** drop-down list, select the type of camera that has been connected to this camera channel.

   This helps the video analytics appliance determine what type of image it should expect from the camera.

   - **Color** — select this option if the camera can only stream video in color.
   - **Black and White** — select this option if the camera can only stream video in black and white.
   - **Day and Night** — select this option if the camera can stream video in color or black and white. This type of camera typically displays color video during the day and black and white video at night to capture as much detail as it can of the scene.
   - **Thermal** — select this option if the camera can stream forward looking infrared (FLIR) video.
6. Check the **Enable Noise Filter** box if the camera is too sensitive and falsely detects motion as classified objects. Disable this option if the camera is not sensitive enough.
7. If you plan to enable self-learning or configure video analytic events, apply your changes now.

   Tip: Each time you choose to save or apply your settings, you may be prompted to reboot. To save time, enter all your video analytic settings before you click Apply or OK.
8. Click **Apply** to save your settings.
9. If you are prompted, allow the device to reboot.

Enabling Self-Learning

The Video Analytics Configuration dialog box allows you to enable or disable self-learning in video analytics devices.

1. In the device Setup tab, click  .

   The Analytic Events dialog box opens.
2. To enable self-learning, check the **Enable Self Learning** box.
3. To disable self-learning, clear the **Enable Self Learning** check box.

   NOTE: Disabling self-learning may result in more classified objects being falsely detected.

   Once disabled, the camera stops self-learning and no longer utilizes any learned information.
4. To reset self-learning, click **Reset**.
   - In the confirmation dialog box that appears, click **Yes**.

   NOTE: When self-learning is reset, all previous self-learning data for the device is deleted.
5. Click **OK** to save your changes.

Setting a Device's Identity

In a device's General dialog box, you can give the device a name, describe the device's location and give the device a logical ID. The logical ID is needed to control the device through keyboard and joystick commands.

1. In the device Setup tab, click  .

   The General dialog box is displayed.

   NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

2. In the **Device Name:** field, give the device a meaningful name to help you identify it. By default, the device model number is used as the device's name.
3. In the **Device Location:** field, describe the device's location.
4. In the **Logical ID:** field, enter a unique number to allow the Client software and integrations to identify this device. By default, the device's Logical ID: is not set and must be manually added.

   Tip: If **Display LogicalIDs** is enabled in Client Settings, the device's Logical ID will appear beside the device's name in the System Explorer.

5. (Cameras only) To disable the LEDs on a device, select the **Disable device status LEDs**. This may be required if the device is installed in a covert location.
6. Click **OK**.

Changing Image and Display Settings

1. In the camera Setup tab, click  .

   The Image and Display dialog box is displayed.

   NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

2. Use the focus controls to focus the camera.
3. Click  to toggle the Auto Contrast Adjustment.

   This setting changes the contrast of the video displayed in this dialog box. It does not affect recorded video or video displayed in other views. By default, Auto Contrast Adjustment is off.

4. If the camera supports day/night control, select one of the following options from the **Day/Night Mode:** drop-down list:
   - **Automatic** — allow the camera to control the infrared cut filter based on the amount of light in the scene.

     If available, move the **Day/Night Threshold:** slider to set the exposure value (EV) when the camera changes from day to night mode.

   - **Day Mode** — the camera will only stream in color and the IR cut filter is disabled.
   - **Night Mode** — the camera will only stream in monochrome and the IR cut filter is enabled.

5. Adjust the camera's image settings to best capture the scene. A preview of your changes are displayed in the image panel and the histogram.

   Tip: Use the **Maximum Exposure:**, **Maximum Gain:**, and **Priority:** options to control low light behavior.

Option	Description
Synchronize Image Settings with All Heads (Avigilon HD Multisensor Dome Cameras Only)	You can apply the same image settings to all camera heads by selecting this check box. **NOTE:** Zoom and focus settings must be set individually.
Exposure:	You can allow the camera to control the exposure by selecting **Automatic**, or you can set a specific exposure rate. **NOTE:** Increasing the manual exposure time may affect the image rate.
Iris:	You can allow the camera to control the iris by selecting **Automatic**, or you can manually set it to **Open** or **Closed**.
Maximum Exposure:	You can limit the automatic exposure setting by selecting a **Maximum Exposure:** level. By setting a **Maximum Exposure:** level for low light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images.
Maximum Gain:	You can limit the automatic gain setting by selecting a **Maximum Gain:** level. By setting a **Maximum Gain:** level for low light situations, you can maximize the detail of an image without creating excessive noise in the images.
Color Palette:	You can change how information captured from thermal cameras is represented by selecting a **Color Palette:**. **WhiteHot** – Grayscale. White represents hot, black represents cold. **BlackHot** – Grayscale. Black represents hot, white represents cold. **Rainbow** – Multicolor. Red represents hot, blue represents cold.
Priority:	You can select **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera will maintain the set image rate as the priority, and will not adjust the exposure beyond what can be recorded for the set image rate. When set to **Exposure,** the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible.
Flicker Control:	If your video image flickers because of the fluorescent lights around the camera, you can reduce the effects of the flicker by setting the **Flicker Control:** to the same frequency as your lights. Generally, Europe is **50 Hz**

Option	Description
	and North America is **60 Hz**.
Backlight Compensation:	If your scene has areas of intense light that cause the overall image to be too dark, move the **Backlight Compensation:** slider until you achieve a well exposed image.
Enable Wide Dynamic Range	Select this box to enable automatic color adjustments through Wide Dynamic Range (WDR). This allows the camera to adjust the video image to accommodate scenes where bright light and dark shadow are clearly visible.
Enable Adaptive IR Compensation	Select this box to enable automatic infrared adjustments through Adaptive IR Compensation. This allows the camera to automatically adjust the video image for saturation caused by IR illumination.
Saturation:	You can adjust the video's color intensity by moving the **Saturation:** slider until the video image meets your requirements.
Sharpening:	You can adjust the video sharpness to make the edges of objects more visible. Move the **Sharpening:** slider until the video image meets your requirements.
Image Rotation:	You can change the rotation of captured video. You can rotate the video 90, 180, or 270 degrees clockwise.
White Balance	You can control white balance settings to adjust for differences in light. You can allow the camera to control the white balance by selecting **Automatic White Balance**, or select **Custom White Balance** and manually set the **Red:** and **Blue:** settings.

Click **Apply to Devices...** to apply the same settings to other cameras of the same model.

6. Click **OK**.

Compression and Image Rate

Use the camera Compression and Image Rate dialog box to modify the camera's frame rate and image quality settings for sending image data over the network.

NOTE: The dialog box may appear differently depending on the device. Options that are not supported by the device will not be available.

1. In the camera Setup tab, click 

.

   The Compression and Image Rate dialog box is displayed.

   The Total Camera Bandwidth: area gives an estimate of the bandwidth used by the camera with the current settings. Adjust the settings as required.

NOTE: For cameras capable of maintaining multiple streams, the settings in this dialog box only affect the primary stream.

2. In the **Format:** drop-down list, select the preferred streaming format.
3. In the **Image Rate:** bar, move the slider to select the number of images per second (ips) you want the camera to stream over the network.

   For H.264 cameras and encoders, the image rate setting must be divisible by the maximum image rate. If you set the slider between two image rate settings, the application will round to the closest whole number.

4. In the **Image Quality:** drop-down list, select an image quality setting. An image quality setting of **1** will produce the highest quality video and require the most bandwidth. The default setting is **6**.
5. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in kilobits per second (kbps).
6. In the **Resolution:** drop-down list, select the preferred image resolution.
   NOTE: For thermal cameras, use the default resolution for enhanced video quality.
7. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe.

   To help you determine how frequently keyframes are recorded, the Keyframe Period: area tells you the amount of time that passes between each recorded keyframe.

   It is recommended that you have at least one keyframe per second.

8. If your camera supports multiple video streams, you can select the **Enable Low Bandwidth Stream** check box. Depending on your version of the software, the check box may also be called "Enable secondary stream".

   When enabled, the lower resolution video stream is used by the HDSM feature to enhance bandwidth and storage efficiencies.

9. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
10. Click **OK**.

Motion Detection

Depending on the type of camera you are configuring, there may be two types of motion detection available: Pixel Motion Detection and Classified Object Motion Detection.

Pixel Motion Detection observes the video stream as a whole and considers any change in pixel as motion in the scene. This option is available to most cameras that are connected to the system.

Classified Object Motion Detection analyzes the video and only reports the motion of vehicles or persons. This option is only available to Avigilon self-learning video analytics devices.

Setting Up Pixel Motion Detection

In the Motion Detection dialog box, use the Pixel Motion Detection tab to set up pixel motion detection. This allows you to define when the system will acknowledge motion in the scene.

1. In the device Setup tab, click  .

   The Motion Detection dialog box is displayed.

2. In the **Pixel Motion Detection** tab, define the green motion detection area in the camera's field of view:

   NOTE: Pixel motion detection is ignored in the areas that are not highlighted in green.

   Tip: Refer to the red motion activity overlay to help you define the green motion detection area. The motion detection area should avoid areas prone to continuous pixel motion — like TVs, computer monitors, trees and moving shadows. These areas tend to trigger motion recording even though the motion activity may be insignificant.

   -  — Click this button then draw green rectangles to define the pixel motion detection areas. You can draw multiple rectangles to create your pixel motion detection area.
   -  — Click this button and draw rectangles to erase sections from the pixel motion detection area.
   -  — Click this button and manually draw pixel motion detection areas with your mouse. This tool allows you to be very specific and highlight unusual shapes.
   -  — Click this button to highlight the entire image panel for pixel motion detection.
   -  — Click this button to clear the image panel of all pixel motion detection areas.

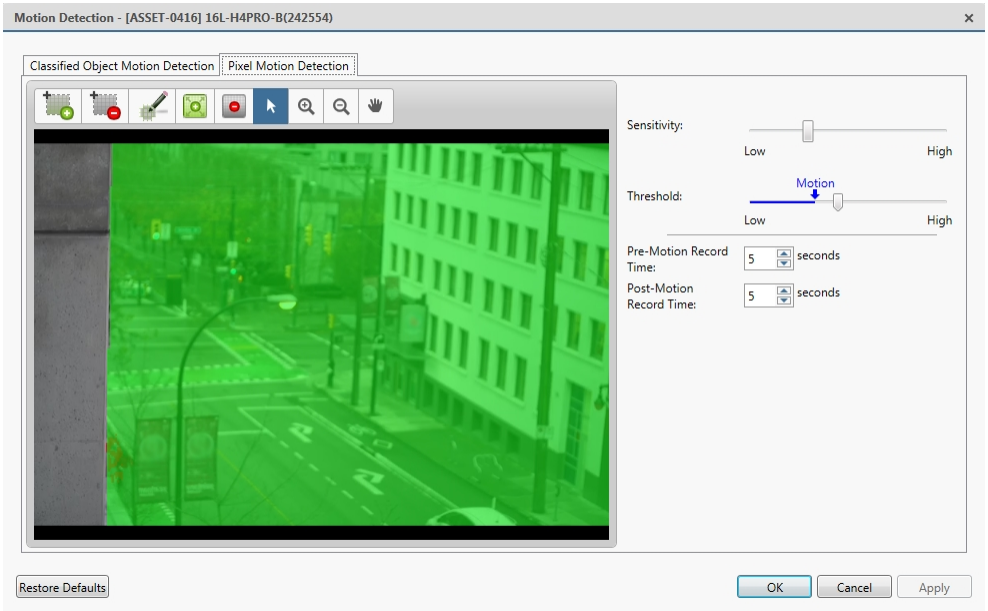


Figure 3: The Motion Detection dialog box: the Pixel Motion Detection tab

3. Define how sensitive the system should be to pixel motion.

    a. Move the **Sensitivity:** slider to adjust how much each pixel must change before it is considered in motion.

    When the sensitivity is High, even small movements are detected - like dust floating immediately before the camera lens.

    b. Move the **Threshold:** slider to adjust how many pixels must change before the image is considered to have pixel motion.

    When the threshold is High, only large motions are detected - like a truck driving across the scene.

    Tip: The **Motion** indicator above the Threshold: slider will move to indicate how much motion is occurring in the current scene. Only when the Motion indicator moves to the right of the Threshold: marker will the camera detect the pixel motion.

    c. In the **Pre-Motion Record Time:** and **Post-Motion Record Time:** fields, specify how long video is recorded before and after the pixel motion event.

4. Click **OK** to save your settings.

Setting Up Classified Object Motion Detection

In the Motion Detection dialog box, use the Classified Object Motion Detection tab to set up object motion detection. This allows you to define when the system will acknowledge a person or vehicle in the scene.

1. In the device Setup tab, click  .

   The Motion Detection dialog box is displayed.

2. In the **Classified Object Motion Detection** tab, define the green motion detection area in the camera's field of view:

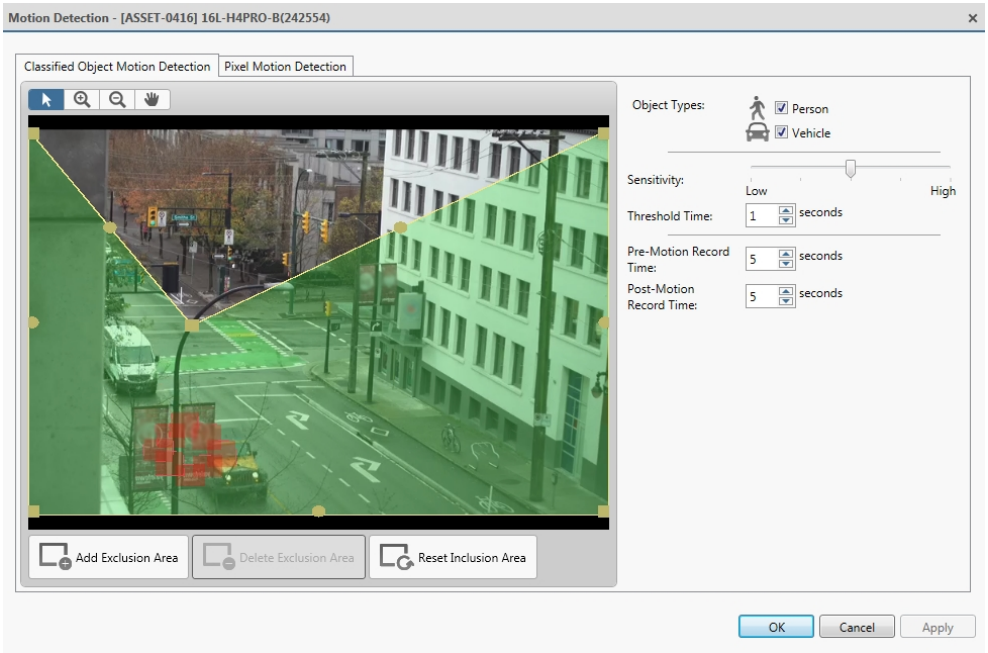


Figure 4: The Motion Detection dialog box: the Classified Object Motion Detection tab

- To change the shape or size of the green overlay, click and drag any of the yellow markers on the border. Extra markers are automatically added to help you fine tune the shape of the overlay.
- To move the green overlay, place the cursor over the green overlay until the cursor changes into a hand or the pan tool. Then, click and drag the green overlay to the desired location.
- Click  to add an exclusion area. The exclusion area is added inside the green overlay.

  Classified object motion is *not* detected in exclusion areas.

  - To set an exclusion area, move and resize the exclusion area as required then click anywhere on the green overlay.
  - To edit an exclusion area, double-click the exclusion area then modify as required.
- Select an exclusion area then click  to delete the exclusion area.
- Click  to restore the default green overlay.

3. Define the objects that are detected by the system.
    a. Check the **Person** box to detect people in the area.
    b. Check the **Vehicle** boxes to detect vehicles in the area.
    c. Move the **Sensitivity:** slider to adjust how sensitive the system is to the detection of classified objects.

        If you set the slider to **Low**, the video analytics device will detect fewer objects because the system must be highly confident that it has detected a person or vehicle before you are notified of an event.

        If you set the slider to **High**, the video analytics device will detect more objects because the system does not need to be as certain of the object classification before you are notified of a motion event.

        Be aware that if the slider is set too low, the system may miss classified object motion. If the slider is set too high, the system may generate a higher number of false classified object motion detections. Adjust the **Sensitivity:** slider to match the level of activity in the scene.

    d. In the **Threshold Time:** field, adjust how long an object must be moving before it is considered a moving object.
    e. In the **Pre-Motion Record Time:** and **Post-Motion Record Time:** fields, specify how long video is recorded before and after a classified object motion detection event.
4. Click **Apply** to save your settings.

Recording Schedule

The ACC system uses a recording schedule to set when each connected camera should be recording video. By default, the server is set to record motion and configured events when they occur.

Once the recording schedule is set, video is recorded automatically.

Adding and Editing a Recording Schedule Template

The recording schedule is set by using templates that tell cameras when and what to record. For example, you can create one recording schedule template for weekdays and another for weekends.

1. In the server Setup tab, click  . The Recording Schedule dialog box is displayed.
2. Click **Add Template** below the Templates: list.
3. Enter a name for the **New Template**.
4. Click the **Set Area** button, then click or drag the cursor across the **Recording Mode:** timeline to set the types of events that the cameras will record throughout the day. Individual rectangles on the Recording Mode: timeline are colored when they have been selected.

    The **Recording Mode:** options include:

    - **Continuous** — record video constantly.
    - **Motion** — only record video when motion is detected.

5. To disable recording in parts of the template, click the **Clear Area** button, then click or drag the cursor across the timeline to remove the set recording areas.
6. If cameras are *not* recording in Continuous mode all day, you can set cameras to record reference images between events in the recording schedule.
    - Select the **Record a reference image every:** check box, then set the time between each reference image.

Editing and Deleting a Template

1. In the Setup tab, select the server you want to edit then click  .
2. In the Recording Schedule dialog box, select a template from the Templates: pane and do one of the following:
    - To edit a template, modify the schedule.
    - To rename a template, click **Rename Template** and enter a new name.
    - To delete a template, click **Delete Template**.
3. Click **OK** to save your changes.

Setting Up a Weekly Recording Schedule

You can set up a weekly recording schedule by applying templates to cameras for each day of the week.

1. In the server Setup tab, click  . The Recording Schedule dialog box is displayed.
2. Select a template from the Templates: list.
3. In the Default Week area, click the days of the week this template applies to for each camera.

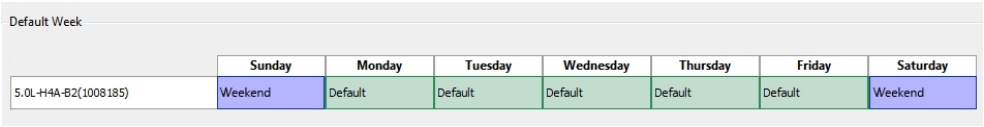


Figure 5: The Recording Schedule dialog box: Default Week

4. Click **OK**.

Recording and Bandwidth

While the Recording Schedule dialog box sets when and what cameras record, the Recording and Bandwidth dialog box sets how long recorded video is stored.

In the Recording and Bandwidth dialog box, you can change the data aging settings and set the maximum record time for each connected camera. The amount of data aging that is available depends on the camera that is connected to the system.

- For JPEG2000 or JPEG compression cameras, data aging is available at three rates:
  - **High Bandwidth** keeps recordings at their original quality.
  - **Half Image Rate** discards half of the recorded data to make room for new recordings.
  - **Quarter Image Rate** keeps 1/4 of the original recorded data so that you can still see older video.
- For H.264 cameras that support data aging, data aging is available at two rates:
  - **High Bandwidth** keeps the original high quality video and the secondary stream of low resolution video.
  - **Low Bandwidth** only keeps the secondary stream of low resolution video.

  NOTE: The data aging can only occur when the secondary stream is enabled.
- For H.264 cameras that *do not* support data aging, only the **High Bandwidth** video is kept.

By default, the system is set to keep recorded video for the maximum amount of time based on the available storage.

At the bottom of the Recording and Bandwidth dialog is the following statement:

Total record time estimate is based on constant recording

The retention time is determined by the **Max. Record Time** setting and the average camera data rate. Since the system can only provide an estimate of the data rate for the full retention period, the actual retention time may exceed the Max. Record Time setting by 5 minutes.

1. In the server Setup tab, click  .

   The Recording and Bandwidth dialog box is displayed.

   The Data Aging column shows an estimate of the recording time that is available at each image rate, given the amount of space on the recording device.
2. In the Data Aging column, move the sliders to adjust the amount of time video is stored at each image rate.
   - To change the data aging settings for all linked cameras, move the slider for one linked camera and all linked cameras will be updated.
   - To change the data aging setting for one camera, break the camera's link to other cameras by clicking the  icon to the left of its name, then make your changes.
3. In the **Max. Record Time** column, manually enter a maximum record time or select one of the options from the drop-down list for each camera.

   NOTE: If the time estimated in the Total Record Time column is significantly shorter than what is set in the Max. Record Time column, the camera's actual recording time will be closer to the Total Record Time estimate.
4. Click **OK**.

NOTE: If you are setting up data aging to work with the Storage Management Continuous Archive feature, keep note of the lowest data aging setting. To work together, the value of the data aging setting must be greater than the value configured for the Archive video older than: parameter on the Storage Management dialog box. This ensures that archiving starts before data is deleted on the local ACC Server.

Add Users and Groups

Add users and different permission groups for accessing the system.

Adding Groups

Groups define what features users have access to. Create new groups to change what users can access.

Groups can be given a rank in the Corporate Hierarchy to further define what the members of the group can access.

1. In the site Setup tab, click  .
2. In the following dialog box, select the Groups tab and click **Add Group**.
3. In the pop-up dialog box, select an existing group to use as a template for your new group, then click **OK**.
4. In the Edit Group dialog box, complete the following:
    a. Give the new group a name.
    b. Select a rank for the group from the **Rank:** drop-down list. To edit or view the entire Corporate Hierarchy, click  .
    c. Move the **Min Password Strength:** slider to define how strong the password used by each user in the group must be.

        The password strength is defined by an algorithm that anticipates how easy a password is to guess. There is no defined character minimum, but the stronger the setting, the harder it should be for an unauthorized user to crack the password.

        Tip: If users are expected to change their passwords frequently, you may want to select a weaker setting to ensure users do not have difficulty choosing new passwords.

    d. Select the required **Group Privileges:** and **Access Rights:** for the group. Clear the check box of any feature or device that you do not want the group to have access to.
5. Click **Edit Groups** to enable the Dual Authorization feature.

    When you enable Dual Authorization, users in this group cannot review recorded video without permission from a user in the authorizing group.

    a. In the following dialog box, select the groups that can grant authorization to users in this group.
    b. To disable the feature, click the toggle at the top of the dialog box.
    c. Click **OK**.

6. Select the Members tab to add users to the group.

   If a user is added to the group through the Add/Edit User dialog box, the user is automatically added to the group's Members list.

   a. Click  .
   b. Select the users that should be part of this new group. Only users that have been added to the site are displayed.

      Tip: Enter the name of a user in the **Search...** field to locate specific users.

   c. Click **Add**. The users are added to the Members list.
7. Click **OK** to save the new group.

Adding a User

1. In the site Setup tab, click  .
2. In the Users tab, click **Add User**.
3. When the Add/Edit User dialog box appears, complete the User Information area.
4. If you don't want this user to be active yet, select the **Disable user** check box. Disabled users are in the system but cannot access the site.
5. In the Login Timeout area, select the **Enable login timeout** check box to set the maximum amount of time the Avigilon Control Center Client software can be idle before the user is automatically logged out of the application.
6. Select the **Member Of** tab to assign the user to a group.
   a. Select the check box beside each access group the user belongs to.

      The other columns display the permissions that are included in the selected groups.

   b. Return to the **General** tab.
7. In the Password area, complete the following fields:
   - **Password:** — enter a password for the user.
   - **Confirm Password:** — re-enter the password.
   - **Strength:** — indicates the strength of the password. The strength is defined by the group the user is assigned to. If the user is a member of more than one group, the user must meet the strongest password requirement.

     The password must meet the minimum strength requirements.

     -  — password meets the strength requirements.
     -  — password does not meet the strength requirements, enter a new password.

     The password strength is defined by how easy it is for an unauthorized user to guess. If your password does not meet the strength requirements, try entering a series of words that is easy for you to remember but difficult for others to guess.

- **Require password change on next login** — select this check box if the user must replace the password after the first login.
- **Password Expiry (Days):** — specify the number of days before the password must be changed.
- **Password never expires** — select this check box if the password never needs to be changed.

8. Click **OK**. The user is added to the site.

Customize Video Monitoring Setup

To help make video monitoring more efficient, you can customize video displays, maps and setup joysticks shortcuts.

Saved Views

After you add videos to a View, adjust the layout to fit your preferences and zoom-in each video to the area of interest, you can save the View to share with other users in the site. A saved View remembers the current View layout, the cameras displayed in each image panel, and the image panel display settings.

Saving a New View

1. From the toolbar, select > **Save As New View**.
2. In the following dialog box, complete the following:
   a. Select the site that the View should be added to.
   b. Give the saved View a name.
   c. Assign a number to the saved View in the **Logical ID:** field. The logical ID is a unique number that is used to open the saved View through keyboard commands.
   d. If it is not displayed, click to display the Site View Editor and choose where the saved View appears in the System Explorer.
      - In the site directory, drag the saved View up and down the right pane to set where it is displayed.
      - If your site includes folders, select a location for the saved View in the left pane. The right pane updates to show what is stored in that directory.
   e. Click **OK**.

Your saved View is added to the System Explorer under the selected site. You can now manage the saved View as a part of your site.

Opening a Saved View

Do one of the following:

- In the System Explorer, double-click the saved View ().
- In the System Explorer, right-click and select **Open**.
- Drag from the System Explorer to the current View in the application or new window.
- On your keyboard, press `CTRL + G`. When you are prompted, enter the saved View's logical ID then press `Enter`.

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. From the tool bar, select > **Update Saved View**.

Renaming a Saved View

1. In the System Explorer, right-click and select **Edit...**.
2. In the Edit View dialog box, enter a new name or logical ID and click **OK**.

Deleting a Saved View

1. In the System Explorer, right-click and select **Delete**.
2. In the confirmation dialog box, click **Yes**.

Adding a Map

You can create a map from any image in JPEG, BMP, PNG, or GIF format. The image is used as the map background and cameras are added on top to show where they are located in your surveillance site.

NOTE: The recommended map image size should be no more than 3000 x 3000 px or 9 MP. Larger images may cause rendering issues.

1. In the System Explorer, right-click a site or site folder and select **New Map...**.
2. In the Map Properties dialog box, click **Change Image...** and locate your map image.
3. In the **Name:** field, enter a name for the map.
4. If it is not displayed, click to display the Site View Editor and choose where the map appears in the System Explorer. By default, the map is added to the site that you initially selected.
    - In the site directory, drag the map up and down the right pane to set where it is displayed.
    - If your site includes folders, select a location for the map in the left pane. The right pane updates to show what is stored in that directory.
5. Click **OK**.

    In the following Editing: Map tab, you can click **Edit Properties...** to open the Map Properties dialog box again.

6. Drag and place cameras from the System Explorer onto the map.

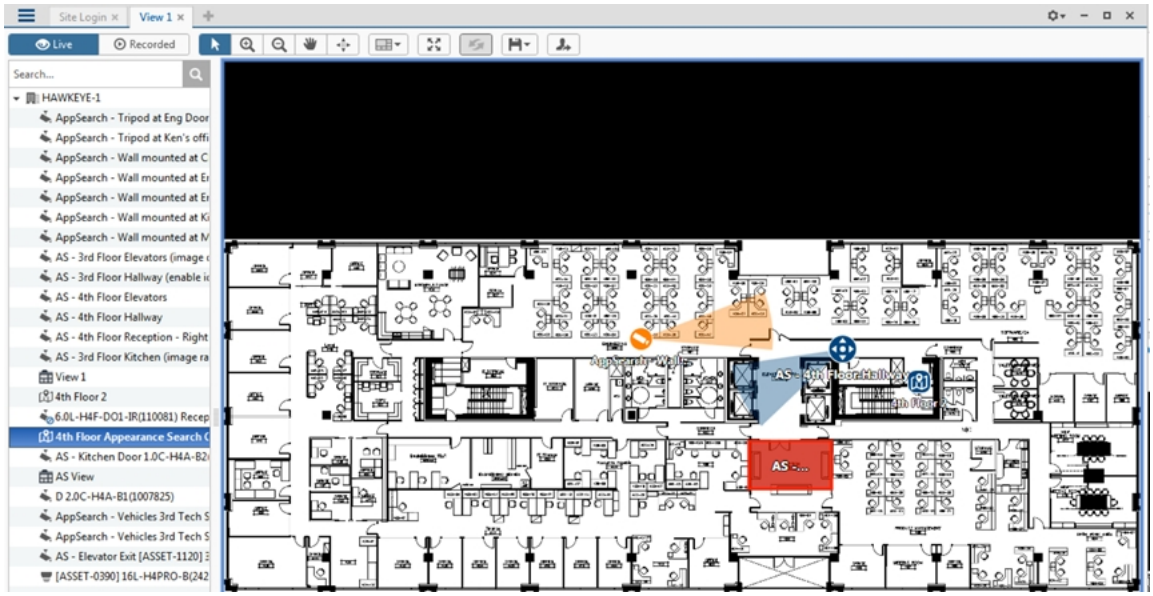


Figure 6: The Editing: Map tab

By default a camera is displayed as an icon with a yellow triangle to represent its field of view.

- Drag the black points at the end of the yellow field of view to re-size and position the camera angle.

7. Drag encoders, saved Views and other maps that you need from the System Explorer onto the map.
8. In the **Map Icon Properties** options, you can change the size and way icons or shapes are displayed on the map. Select any icon on the map then do the following:

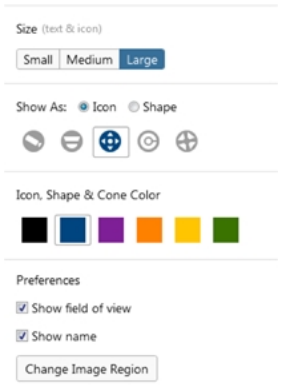


Figure 7: Map Icon Properties options

a. Select **Size** to display the text and icon.

b. To display an icon or shape, select one of the buttons in **Show As:**. Select the color of the icon, shape and cone to display on the map.

c. Select the **Show name** check box to display the object's name on the map.

d. Click **Delete from Map** to remove the object from the map.

e. (Cameras only) Select the **Show field of view** check box to display the camera's yellow field of view. This option is only available when the camera icon is used.

   Drag the corners of the yellow triangle to expand the field of view. Drag the black circle at the end of the triangle to rotate the field of view.

f. (Cameras only) Click **Change Image Region** to define the specific area that is displayed when you access the camera from the map.

   In the following dialog box, move and resize the green overlay to select the region you want to focus on, then click **OK**.

9. Click to save your new map.

Joystick Settings

There are two types of joysticks supported by the Client: standard Microsoft DirectX USB joysticks and the Avigilon USB Professional Joystick Keyboard.

Access the Joystick settings to install the required drivers and configure your joystick options.

Configuring an Avigilon USB Professional Joystick Keyboard For Left-Hand Use

The Avigilon USB Professional Joystick Keyboard is a USB add-on that contains a joystick for controlling zooming and panning within image panels, a jog shuttle for controlling the Timeline, and a keypad programmed with the Client software keyboard commands.

By default, the keyboard is installed in right-hand mode. Change the Joystick settings to configure it for left-hand mode.

1. Connect the keyboard.
2. In the top-right corner of the Client, select > **Client Settings** > **Joystick**.

   If the keyboard is not automatically detected, an error message is displayed. Click **Scan for Joysticks...**.
3. In the Joystick tab, select the **Enable left-hand mode** check box.
4. Click **OK**. The keyboard is now configured for left-hand mode.
5. Rotate the keyboard until the joystick is on the left and the jog shuttle is on the right. Reinstall the keypad cover with the View button labels at the top.

For more information about the Avigilon USB Professional Joystick Keyboard, see the installation guide that is included with the device.

Configuring a Standard USB Joystick

Use the Joystick settings to configure the buttons used in your standard Microsoft DirectX USB joystick.

1. Connect the joystick. In the top-right corner of the Client, select > **Client Settings** > **Joystick**.
2. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.
3. In the Joystick tab, choose an action for each button on the joystick:
    a. Press a button on the joystick to highlight its label in the dialog box.
    b. Select an action for the button from the drop-down list.

       Options include ways to control recorded video, Views, image panels, instant replay, audio, snapshots and PTZ.

    c. Repeat this procedure for each button on the joystick.
4. Click **OK**.

External Notifications

You can configure the site to send external notifications in response to specific events. You can set up an SMTP server for the site and choose what events require external notifications.

Setting Up the Email Server

To send email notifications, the site must be given access to an email server.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.
2. Select the Email Server tab.
3. In the Email Server Settings: area, complete the following:
    a. **Sender Name:** enter a name to represent the site in all email notifications.
    b. **Sender Email Address:** enter an email address for the site.
    c. **Subject Line:** enter a subject line for all emails sent from the site. The default subject is *Avigilon Control Center System Event*.
    d. **SMTP Server:** enter the SMTP server address used by the site.
    e. **Port:** enter the SMTP port.
    f. **Timeout (seconds):** enter the maximum amount of time the server will try to send an email before it quits.
4. (Optional) If the email server uses encryption, select the **Use secure connection (TLS/SSL)** check box.
5. (Optional) If the email account has a username and password, select the **Server requires authentication** check box.
    - Enter the **User Name:** and **Password:** for the email account.
6. Click **OK**.

Configuring Email Notifications

In the Email Notifications dialog box, you can create email notification groups to specify who will receive email notifications when certain events occur.

Be aware that you cannot send any email notifications until you've set up an email server for the site. For more information, see *Setting Up the Email Server* on the previous page.

NOTE: Some features are not available if the server does not have the required license, or if you do not have the required user permissions.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.

2. Make sure the Email Notifications tab is selected.
3. Click  .
4. Enter an **Email Group Name:**.
5. In the **Email Recipients:** area, add all the user, group and individual emails that are part of this email group. Do any of the following:

   - Click  to add a site user or access group. In the dialog box, select all the required users and groups then click **OK**.
   - Click  to add individual emails. In the dialog box, enter the email address then click **OK**.

   Tip: Make sure the site users in the Email Recipients: list have a valid email in their user account.

6. Click  to send a test email to everyone on the Email Recipients: list.
7. In the **Email Trigger:** area, select all the events that will trigger an email for this email group. Click the blue underlined text to define the event requirements.
8. To attach a snapshot of the email notification event, select the **Attach images from device(s) linked to the event** check box.

   NOTE: This option is disabled if *Motion Detect* is not selected because there are no images associated with system events, digital inputs, or POS transaction exceptions.

9. In the **Email Schedule:** area, select a schedule for the email notification.
10. To limit the number of emails sent, enter the minimum amount of time between each email in the **Send email at most every:** field.
11. Click **OK**.

The new email notification is saved and added to the Email Groups: list.

Central Station Monitoring

Central station monitoring notifications allow an ACC site to notify a third-party central monitoring company when an event of interest occurs. This feature works through the external notification feature and the rules engine. You need to enable the ACC site to send notifications, then create all the rules that would cause a notification to be sent to the central monitoring station.

Enabling Central Station Monitoring

If you use a central station monitoring service, you can set up the ACC site to communicate with your central monitoring service via:

- XML over SMTP notifications
- SIA over IP notifications

Consult with your central monitoring service for their preferred notification type.

1. In the site Setup tab, click  .

   The External Notifications dialog box is displayed.

2. In the Central Station Monitoring tab, select the **Enable Central Station Monitoring** check box.
3. In the Central Monitoring System: drop-down list, select which type of notification the ACC software should send:
   - **XML over SMTP** — external notifications will be sent to the central station monitoring service using SMTP.
   - **SIA over IP** — Security Industry Association (SIA) notifications will be sent to the central station monitoring service using IP.

You can now configure the notification options.

Configuring Notification Options

Consult with your central monitoring service for the correct settings for each field.

1. In the Options area, complete the fields with the information provided by your central monitoring service.
   - If you selected XML over SMTP notifications, the central monitoring service will typically provide you with a specific name, email address, and SMTP details to identify you in their system.
   - If you selected SIA over IP notifications, the central monitoring service will typically provide you with an Account Number, Site Receiver Numbe, primary and secondary server IP addresses and port numbers.
2. To periodically check the state of the connection to the central monitoring service, select a time interval from the **Minimum Heartbeat Interval:** drop-down list.
   - The selected amount of time must pass before a confirmation message is sent. The confirmation message is only sent if no other notifications are sent during the set time period.
   - This feature allows the system to automatically send a message to the central monitoring service to confirm that the systems are still connected and no issues have occurred.
   - If the central monitoring service requires the system to send a heartbeat test message at specific intervals, select the option that is equal to half the requested interval. For example, if the central monitoring service requires a confirmation message be sent once a day, assign the system to send a message every 12 hours.
3. Click **OK** to save your changes.

You can now create rules to send the central monitoring service notifications when specific events occur.

Create Central Station Monitoring Rules

Create rules that will notify the central monitoring service of specific events.

- On the Select Rule Action(s) page, make sure the **Send notification to Central Monitoring Station** option is selected. This ensures the central monitoring service is notified of the rule event.

  Tip: The system Email Notifications feature works separately from the Central Station Monitoring feature, but you can configure the rules to send you the same notifications as the central monitoring service. When you create rules for the central monitoring service, include the **Send email** option on the Select Rule Action(s) page. You can configure the rule to send you details that are not included in the central monitoring notification.

For XML over SMTP notifications only, you can customize the notification by clicking the blue link text in the rule description.

1. Click **no media** to select the type of attachment included with the notification.
   - In the Select Attachment dialog box, select the **Image** or **Video** check box.
   - For Video attachments, select the quality:

     low The attached video resolution is 4CIF with a fixed frame rate of 5 fps. The attached video size is typically under 1 MB.

     high The attached video resolution is 720p with a fixed frame rate of 10 fps. The attached video size is typically under 3 MB, depending on the camera's image and compression settings and the amount of motion in the scene.
2. Click **no media source** to select which cameras to export from.
   - In the Select Cameras dialog box, you can choose to include attachments from cameras linked to the trigger event or other cameras in the system.

     NOTE: Only select cameras that are connected to the same server as the triggering device. Attachments from other servers are not currently supported.

To arm or disarm event notifications from the site, the ACC software also supports rule conditions — the requirement that a condition be met before a rule is executed. Digital input device events can be used to condition a rule and effectively arm or disarm the rule.

Avigilon Corporation
avigilon.com

PDF-ACC-INSTALLWFLW-F

Revision: 1 - EN

20180517

Pre-Site Checklist

Installer: _____

Project Name:_____

Before you begin initial system setup, make sure the following requirements are met before you arrive at the installation site:

1. ☐ Avigilon Network Video Recorders (NVR).
    - ☐ Spare monitor for server configuration (VGA).
2. Client workstations
    - ☐ Avigilon Remote Monitoring Workstations, including monitors.
        - Some models come with a single display port and a single DVI connection per video card, plus a Display port to DVI adapter.
        - Some models come with HDMI ports and an HDMI to DVI adapter.
        - HDMI monitor cables must be purchased separately.
    - ☐ Customer provided workstation.
3. ☐ Network switches with enough ports and PoE budget for all camera and server connections.
4. ☐ Ensure switches and servers will be connected to a UPS that is powerful enough to provide surge protection and uninterrupted backup power to the system.
5. ☐ Avigilon camera channel licenses for each server.
    - ☐ For single-server sites, activate licenses on server at the office for faster setup.
    - ☐ For multi-server sites, activate licenses after merging multiple servers into a single site. May be easier to perform on-site.
6. ☐ System design of the site (see the person who sold the project).
    - Make sure the design includes the following:
        - ☐ List of all camera to server connections — video recording and redundancy.
        - ☐ Server and camera configuration settings — retention time, images per second, and any other settings required to obtain the best video retention results.
7. ☐ IP addresses for the system.

    This is provided by the IT group at the site if you are putting the system on their network.

8. Camera installation tools:
    - ☐ Laptop for running the Camera Configuration Tool.
    - ☐ USB Wi-Fi Adapter for H4 cameras
    - ☐ PoE splitter
9. Download a copy of the latest Avigilon software:

    avigilon.com/support-and-downloads/for-software/acc/downloads/

    - ☐ ACC Server software
    - ☐ ACC Client software
    - ☐ ACC Virtual Matrix software (if applicable)
    - ☐ ACC Gateway software (if applicable)
    - ☐ ACC Web Endpoint software (if applicable)
    - ☐ ACC Analytics Service software (required for Avigilon Appearance Search feature)

System Setup Checklist

Installer:_____

Project Name:_____

Install and configure the ACC system as follows:

Important: Always follow system design documentation and criteria for all device and server settings.

1. ☐ Install cameras and devices.

   For more information, see *Install Hardware and Software* on page 1.

   a. ☐ Connect devices to network.
   b. ☐ Aim and focus cameras.
   c. ☐ Assign a name and location for the camera or device.
   d. ☐ Assign a dynamic or static IP address to the camera or device.

2. ☐ Install the video recorder.
   - Windows based NVR — NVR3 or HD Video Appliance
     a. ☐ Complete initial Windows setup.
     b. ☐ Set date and time.
     c. ☐ Set computer name.
     d. ☐ Set new password for local administrator account.
     e. ☐ Activate site license according to system design. See *Activate Site Licenses* on page 4.
   - ACC ES Recorder or ACC ES Analytics Appliance
     a. ☐ Assign password to administrator account in the web interface.
     b. ☐ Assign a hostname for the recorder.
     c. ☐ Set date and time.
     d. ☐ Set a name for the recorder.
3. ☐ Configure NTP time synchronization.
4. ☐ Install and run ACC Client software on local workstation.
5. ☐ Configure anti-virus settings for servers and workstations. See *Configure Anti-Virus Settings* on page 2.

6. Configure sites and servers:
    a. ☐ (Enterprise systems only) Merge multiple servers into a single site as required. See *Connecting Servers to Sites* on page 7.
        - ☐ Activate licenses for the new site. See *Activating a License for the First Time* on page 4.
    b. ☐ Configure the Site View. See *Editing the Site View* on page 9.
    c. ☐ Connect cameras to the servers. See *Connecting a Device to a Server* on page 10.
    d. ☐ Enable analytics devices. See *Configure Video Analytics* on page 11.
        - ☐ Enable self-learning. See *Enabling Self-Learning* on page 15.
7. Configure devices:
    a. ☐ Assign a logical ID to the camera. See *Setting a Device's Identity* on page 15.
    b. ☐ Adjust video image and display. See *Changing Image and Display Settings* on page 16.
    c. Set compression and image rate. See *Compression and Image Rate* on page 18
        - ☐ Image rate.
        - ☐ Quality level.
        - ☐ Keyframe interval.
    d. Configure motion detection areas.
        - Pixel Motion. See *Setting Up Pixel Motion Detection* on page 19.
            - ☐ Green motion detection area.
            - ☐ Sensitivity.
            - ☐ Threshold.
        - Classified Object Motion. See *Setting Up Classified Object Motion Detection* on page 21.
            - ☐ Green motion detection area.
            - ☐ Type.
            - ☐ Sensitivity.
            - ☐ Threshold.
    e. ☐ Recording schedule. See *Recording Schedule* on page 23.
    f. ☐ Data aging settings. See *Recording and Bandwidth* on page 24.
8. ☐ Add users and groups. See *Add Users and Groups* on page 26.
9. ☐ Configure Avigilon Rules and Alarms as required to satisfy all system functionality per the system design documentation.
10. Customize video monitoring setup:
    - ☐ Add saved Views. See *Saved Views* on page 28.
    - ☐ Add maps. See *Adding a Map* on page 29.
    - ☐ Configure joysticks. See *Joystick Settings* on page 31.
11. ☐ Configure external notifications. See *External Notifications* on page 32.
12. Configure ACC Mobile access.
    - ☐ To run ACC Mobile 2.x, install and configure ACC Gateway software.
    - ☐ To run ACC Mobile 3.x, install ACC Web Endpoint software.

13. ☐ Verify setup — Log in as different users to check interface and permissions.
14. ☐ Download ACC Mobile from the App Store or Google Play™ store.
    - ☐ For ACC Mobile 2.x, configure the app to point to a Gateway IP address.
    - ☐ For ACC Mobile 3.x, configure site address to point to an ACC IP address.