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

Pre-configure the network video recorders as much as possible and familiarize yourself with the system design and the customer network setup to streamline the setup process.

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.
- Positioned and focused in the direction specified in the system design.
- Assigned a descriptive name.
- 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 using the Avigilon Camera Configuration Tool.

Refer to the device installation guide for more information.

Tip: For bulk configuration, use the Camera Configuration Tool available on **avigilon.com**. You can also use the device's web interface for configuration. If needed, use the Avigilon USB Wifi Adapter System to access the camera interface through a wifi network.

Video Recorders

Install the video recorders. An ACC system can feature network video recorders (NVRs), HD Video Appliances, ACC ES Recorders or Avigilon video analytics appliances. Each video recorder must be:

- Connected to the network — camera and corporate network as required.
- Configured for NTP time synchronization.
- Assigned a descriptive name.
- Assigned an IP address.
- 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.

ACC 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.

The ACC Analytics Service must be installed to use the Avigilon Appearance Search feature. Avigilon NVR 4 Premium and Standard servers come with the ACC Analytics Service pre-installed. If you are installing an analytics kit on an NVR 3 Value or third-party server, download and install the ACC Analytics Service software.

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

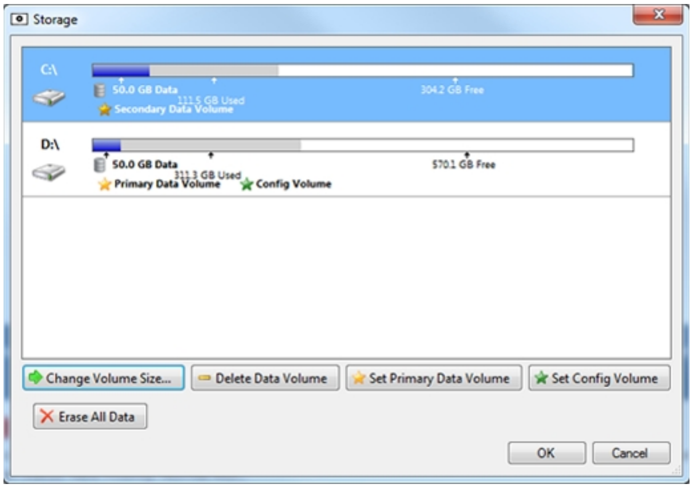
To ensure the anti-virus software does not interfere with the ACC software's ability to write video data and other important files, exclude the following locations from being scanned:

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`

Configure Sites and Servers

In the ACC software, a site can contain one or more servers depending on the license edition. Site settings control user access and system- wide events. Server settings control video and storage settings for devices connected to that server.

When there are multiple servers in a site, you can assign a failover connection to a backup server. This connection allows a device to continue recording if the primary server fails.

Multiple Server Sites

A site can contain multiple servers that share settings and tasks. For example, users and groups that are added to the site will automatically have access to all linked servers.

Tip: Plan how your system should be configured before connecting servers to sites to avoid reconfiguring settings each time a server is added.

Connecting Servers to a Site

Sites only have one server by default, but you can add multiple servers to a site and manage them together. All servers within a site share settings and are represented as one unit in the System Explorer.

When servers are installed a significant distance apart, they may only share users and group information. These sites can be joined into families. For more information, see *Site Families* on page 6.

Note:

- If you're using the Avigilon Artificial Intelligence (AI) Appliance, connect the appliance to an NVR server before connecting that server to your site.
- Servers must have the same version of the ACC software to be connected.
- Ensure ports 38880 to 3884 TCP/UDP are open across the network.
- Ensure servers have unique Windows hostnames.
- When a server joins a site, its site license must be reactivated.

1. In the New Task menu ☰, click **Site Setup**.
2. Click 🏢.

   The Site Management tab lists all accessible and connected sites and servers. If you can't find your site, you'll need to search for it.

3. Select your 🗄 server and drag it to a different site.

   Sites without any servers are automatically removed from the list.

4. Reactivate the site license.

After the server is connected to the site, settings are merged and the following rules are applied:

- Unique settings from the server are added to the site.
- When settings are identical, only the site version is kept.
- When a server setting and a site setting share the same name but are configured differently, the server setting is added to the site and renamed: <setting name> (server name), e.g. Email1 (Server2F).
- Site Views are combined.
  - Site organization settings override server settings when merged. Any unorganized elements from the server are listed at the bottom of the site View.
- All user groups are merged.
  - If groups have the same name, the site settings are used and users from both the site and the server are added to the group.
  - New groups to the site automatically receive access to all the devices in the site.
  - New groups to the added server automatically receive access to all the devices that are connected to the server.
- Users with the same name will share configured settings, 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.

Disconnecting Servers from a Site

When you disconnect a server from a site, it becomes a separate server under its own site.

Disconnected servers retain all settings from the site it was previously connected to.

1. In the New Task menu ☰, click **Site Setup**.
2. Click 🏢.The Site Management tab lists all the sites that you can access and all the servers that are connected to each site.
3. Select a server from the site and click **Disconnect from Site...**.
4. After the server is disconnected, you'll need to reactivate the site licenses.

You can purchase new licenses for a disconnected server or you can deactivate the required licenses from the previous site. Deactivated licenses can be activated for other sites.

Site Families

Independent sites can be connected to create a site family. User, rank, and group information is centrally managed by the parent site while the child sites can define local users and groups.

Connecting Site Families

Each parent site can have up to 1 Core site, 24 Standard sites, and unlimited Enterprise sites as child sites. Each site should be running the same version of ACC software.

1. In the New Task menu ☰, click **Site Setup**.
2. Click 🏢 and select the 🏢 site you want to connect as a child.
3. In the bottom-right corner, click **Connect to Parent Site**.

> **Note:** Selecting a ▤ server only allows you to Connect to Site....

4. In the **Connect to:** drop-down list, select a parent site.
5. In the **Rank:** drop-down list, assign a rank for the child site.
6. Click **OK**, then click **Yes**.

Disconnecting Site Families

You can dismantle a site family by removing the child from your Corporate Hierarchy. Removed sites function independently, or can be connected to another parent site.

To remove a parent site from a child:

1. Under Site Management, select the child site you want to disconnect.
2. In the bottom-right corner, click **Disconnect from Parent Site...**.
3. Click **OK**.

> **Note:** Network issues may require revoking access from the parent site.

To remove a child site from a parent:

1. Under Site Management, select the parent site you want to disconnect.
2. In the bottom-right corner, click **Disconnect Child Site...**.
3. Use the drop-down list to select the child site to disconnect.
4. Click **OK**.

Naming a Site or Server

Give sites and servers meaningful names to easily identify them in the System Explorer.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a site or server, then click ⚙.
3. Enter a name, then click **OK**.

Editing the Site View

You can change your site organization in the View tab to reflect how your system is set up.

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

The site cannot be moved or re-organized.

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

1. In the New Task menu ☰, click **Site Setup**.
2. Click 📹.
3. Edit your layout.
   - To add a folder, click +. Folders are only visible in the View tab.

     Double-click the folder to change its name.
   - Click and drag items to move their location.
   - Use ↑ ↓ to move one element at a time.
   - To sort the layout alphabetically, click ≡↓. To sort a single folder, select an element within the folder then click ≡↓.
   - To delete a folder, select the folder and click —. The elements inside the folder will move to

the bottom of the layout.

- Expanded or collapsed folders will appear that way when users log in to the site. Users can still collapse or expand folders in the System Explorer.

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

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

Activate Site Licenses

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

You can activate a 30-day demo license or a purchased license. Purchased licenses do not expire, and allow you to join multiple servers to form larger sites in Enterprise systems.

Activating a Demo License

Activate a demo license to begin a 30-day trial of the ACC Client software.

> **Tip:** Finish organizing your multi-server site before activating a license to avoid reactivating the site license each time a new server is added.

1. In the New Task menu ☰, click **Site Setup**.
2. Select your new site, then click 🔑.
3. Click **Request Demo License...**.
4. Select the preferred license edition, then click **Activate Now**.

Activating a License

Once your license is activated, you can immediately use the new licensed features.

> **Tip:** Finish organizing your multi-server site before activating a license to avoid reactivating the site license each time a new server is added.

Online Activation

If you have internet access, use online activation. However, if your site is large and contains hundreds of licenses, the server may time out. Use *Offline Activation* on the next page instead.

1. In the New Task menu ☰, click **Site Setup**.
2. Select your new site, then click 🔑.
3. Click **Add License...**.
4. Enter your product keys.

   If you copy and paste more than one comma-separated product key, the system will format it automatically.

   - To remove the last product key, click **Remove Last Key**.
   - To clear all the product keys, click **Clear**.
5. Click **Activate Now**.
6. Click **OK**.

Offline Activation

Note: You need a licensing.avigilon.com account. Contact Avigilon Order Management for access.

Offline licensing involves transferring files between a computer running the ACC Client software and a computer with internet access.

In the ACC Client:

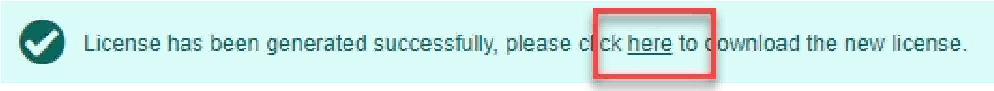
1. In the New Task menu ☰, click **Site Setup**.
2. Select your new site, then click 🔑.
3. Click **Add License...**.
4. Select the **Manual** tab.
5. Enter your product keys.

   If you copy and paste more than one comma-separated product key, the system will format it automatically.

   - To remove the last product key, click **Remove Last Key**.
   - To clear all the product keys, click **Clear**.
6. Click **Save File...** and choose where you want to save the `.key` file. You can rename the file as required.
7. Copy the `.key` file to a computer with internet access.

In a browser:

1. Go to licensing.avigilon.com/activate and log in.
2. Select **Generate License**, then click **Choose File**.
3. Select the `.key` file, then click **Upload**.
4. In the success message, click **here** to download the license file `capabilityResponse.bin`.



License has been generated successfully, please click here to download the new license.

5. Copy the `.bin` file to a computer running the ACC Client software.

In the ACC Client:

1. In the License Management dialog box, click **Apply...**.
2. Select the `.bin` file and click **Open**.
3. Click **OK** to confirm your changes.

Configure Devices

After the site and servers have been configured and licensed, 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 only available if the site has the required license, and if you have the required user permissions.

To access a device, it must be connected to a server within your site. After a device has been discovered on the network, it can be connected to the server.

1. In the New Task menu ☰, click **Site Setup**.
2. Click 📹.
3. In the Discovered Devices area, select the devices and click **Connect...**.

> **Tip:** You can also drag devices to a server in the Connected Devices area.

4. Select which server will connect to the device.

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

5. Connect third-party devices using their native drivers. In the **Device Type:** drop-down list, select the device's brand name. The system may only support one type of driver from the device.
6. If the camera supports a secure connection, the **Device Control:** drop-down list is displayed. Select one of the following options:
   - **Secure** — This default protects and secures the camera configuration and login details.
   - **Unsecure** — The camera configuration and login details may be accessible to users with unauthorized access.

     Cameras with a secure connection are identified with the 🔒 icon.
7. In the **Network Type:** drop-down list, select **LAN** or **WAN**.

   Select the WAN network type to connect cameras on your local network if the Internet Control Message Protocol (ICMP) is blocked or disabled.
8. In the Site View Editor, choose where to display your device in the System Explorer. If it is not displayed, click ⌄.
   - If your site includes folders, select a location for the device in the left pane.
   - In the right pane, drag devices to set where they are displayed.
   - If you are connecting multiple devices at the same time, the devices must be assigned to the same location.

   > **Tip:** If your preferred site is not listed, temporarily connect the device to a different server that is connected to the site you want.

9. Click **OK**.
10. If the device is password protected, enter the device's username and password, then click **OK**.

Configure Video Analytics

If the connected device supports video analytics, enable and configure the video analytic capabilities to trigger video recording and alarms.

If the system you are installing will use the Avigilon Appearance Search™ feature, enable each required camera to support this feature.

Enabling Server-Based Analytics

Server-based analytics enables Classified Object video analytics for cameras without analytics capabilities. To use this feature, you need an Avigilon video analytics appliance.

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

   Only cameras without the Classified Object video analytics mode enabled are displayed.

   If you do not have access rights for a camera, it will not be shown in this list.
3. To enable Classified Object 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. You cannot exceed a Total Analytic Load of 100%.
4. Click **OK**.

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

Enabling the Avigilon Appearance Search™ Feature

Note: Avigilon Appearance Search feature requires at least one of the following:

- An NVR with a GPU for use with cameras that support the Avigilon Appearance Search feature.
- An NVR connected to an Avigilon AI Appliance for use with cameras without Classified Object video analytics.

With the Avigilon Appearance Search feature, operators can find all instances of a person or vehicle across their site.

Avigilon AI Appliances automatically enable the Avigilon Appearance Search feature when server-based analytics are enabled for a camera. For more information, see *Enabling Server-Based Analytics* above.

1. In the server Setup tab, click 👤🔍.
2. Select the camera you want to enable. The Load for each camera is proportional to the amount of activity in the camera's field of view.

   The Total Appearance Search Load bar displays an estimate of the server's analytics service load based on the amount of data that each enabled camera may generate. When the load exceeds 100%, search results might be missed.

   You can view the status of your analytics service in the Site Health tab.
3. Click **Apply**.

Tip: You can also enable and disable the Avigilon Appearance Search feature for an individual camera in the device's Analytics settings.

Analytics Mode

If your device supports self-learning, you can select an analytics mode to use.

Tip: If you have an ACC ES Analytics Appliance, you can enable both analytics modes simultaneously. In the device Setup tab enable Unusual Motion mode. In the server Setup tab enable server-based analytics. For more information, see *Enabling Server-Based Analytics* on the previous page.

Enabling an Analytics Mode

Enable Classified Object or Unusual Motion mode for a video analytics device.

1. In the device Setup tab, click ⚙.
2. In the Video Analytics Mode: drop-down list, select one of the following:
    - **Classified Object** — Detect and classify people or vehicles.
    - **Unusual Motion** — Compare the speed and direction of movement against the scene, displaying irregularities as opposed to traditional movement.
    - **None** — Do not use analytic capabilities.
3. Click **OK**.

Configuring Analytics Settings

Cameras with Classified Object Detection video analytics and cameras connected to Avigilon analytics appliances can be configured to improve classified object detection accuracy.

Tip: You can configure these settings for multiple cameras using the Avigilon Camera Configuration Tool available on **avigilon.com**.

Note: Certain options are only available if supported by the device.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a camera, then click 🏃 .
3. Edit the analytics settings. Each setting is described below.
4. Click **Apply**.

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

Analytic Settings

Setting	Description
Camera Type:	Select the type of camera that has been connected. • **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.
Analytics Scene Mode:	Select the location that best describes where the camera is installed. • **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. This option may 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.
Enable Noise Filter	Select the check box if the camera is too sensitive and falsely detects motion as classified objects.
Display Classified Objects	Select the check box to display bounding boxes around classified objects in recorded video.
Sensitivity:	Enter a value between 1-10 to select how sensitive a camera is to tampering

Setting	Description
	events. Tampering is 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.
Trigger Delay:	Enter a value between 2-30 to define how many seconds the camera will wait before sending tampering events. The default value is 8. 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.
Enable Self Learning	Select the check box to enable self-learning. If you clear this check box, more classified objects may be falsely detected.

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, ensure the cameras are physically connected to each camera channel before connecting the appliance 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.

1. In the New Task menu ☰, click **Site Setup**.
2. Select the appliance, then click 🏃 .
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 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. Configure the available analytics settings. For more information, see *Configuring Analytics Settings* on page 13.

5. If you'll enable self-learning or configure video analytic events, skip this step.
6. Click **Apply** to save your settings.
7. If you are prompted, allow the device to reboot.

Setting a Device's Identity

In a device's General settings, you can give the device a name, describe the location, and give the device a Logical ID. Logical IDs allow easier keyboard and joystick control.

> **Note:** Certain options are only available if supported by the device.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a device and click ⚙.
3. In the **Device Name:** field, enter a meaningful name to easily identify it. By default, the device name is its model number.
4. In the **Device Location:** field, describe the device location.
5. In the **Logical ID:** field, enter a unique number to allow the ACC 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 Logical IDs** is enabled in ACC Client Settings, the device's Logical ID will appear beside the device's name in the System Explorer.

6. To disable the LEDs on a camera, select the **Disable device status LEDs** check box. This may be required if the camera is installed in a covert location.
7. Click **OK**.

Zooming and Focusing the Camera Lens

If the camera has remote zoom and focus capabilities, they can be controlled through the Image and Display settings.

1. In the camera Setup tab, click 🖥.
2. If the camera has a built-in auto-focus feature, choose one of the following:
   - **Continuous Focus** — The camera will automatically focus itself whenever the scene changes. Skip the remaining steps.
   - **Manual Focus** — You can manually focus the camera through the Focus: buttons.
3. While you watch the preview in the image panel, complete the following steps to zoom and focus the camera:
   a. Use the **Zoom:** buttons to zoom in to the distance you want to focus.

4. In the **Iris:** drop-down list, select **Open**. When the iris is fully open, the camera's depth of field is the shortest.
5. Use the **Focus:** buttons until the image becomes clear.

Button	Description
Auto Focus	The camera will automatically focus one time.
0	The camera will focus as close to zero as possible.
«	Large step toward zero.
‹	Small step toward zero.
›	Small step toward infinity.
»	Large step toward infinity.
∞	Infinity.

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

Image and Display Settings

Note: Certain options are only available if supported by the device.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a camera, then click 🖥.
3. Use the focus controls to focus the camera. For more information, see *Zooming and Focusing the Camera Lens* on the previous page.
4. Click ☼ to toggle the Auto Contrast Adjustment. This change does not affect recorded video or video displayed in other views. By default, Auto Contrast Adjustment is off.

5. If the camera supports day/night control, select one of the following options from the **Day/Night Mode:** drop-down list:

   - **Automatic** — The camera controls the infrared (IR) 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.

6. 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: Maximum Exposure:**, **Maximum Gain:**, and **Priority:** control low light behavior.

Option	Description
Synchronize Image Settings with All Heads	Apply the same image settings to all camera heads. Zoom and focus settings must be set individually.
Exposure:	Let the camera control the exposure by selecting **Automatic**, or set a specific exposure rate. Increasing the manual exposure time may affect the image rate.
Iris:	Let the camera control the iris by selecting **Automatic**, or manually set it to **Open** or **Closed**.
Maximum Exposure:	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:	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:	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.

Option	Description
Priority:	Select **Image Rate** or **Exposure** as the priority. When set to **Image Rate**, the camera maintains 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 maintains the exposure setting as the priority and overrides 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, reduce the effects by setting the **Flicker Control:** to the same frequency as your lights. Generally, Europe is **50 Hz** 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 check box to enable automatic color adjustments through 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 check box to enable automatic IR adjustments through Adaptive IR Compensation. This allows the camera to automatically adjust the video image for saturation caused by IR illumination.
Saturation:	Move the slider to adjust the video's color intensity until the video image meets your requirements.
Sharpening:	Move the slider to adjust the video sharpness to make the edges of objects more visible.
Image Rotation:	Change the rotation of captured video by 90, 180, or 270 degrees clockwise.
White Balance	Control white balance settings to adjust for differences in light. Let the camera to control the white balance by selecting **Automatic White Balance**, or select **Custom White Balance** to manually set the **Red:** and **Blue:** settings.

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

7. Click **OK**.

Compression and Image Rate

Use the camera Compression and Image Rate settings to modify the camera's frame rate and image quality sent over the network.

Note: Certain options are only available if supported by the device.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a camera, then click IPS.

   Total Camera Bandwidth: gives an estimate of the bandwidth used by the camera with the current settings.

   Note: For cameras capable of maintaining multiple streams, these settings only affect the primary stream.

3. In the **Format:** drop-down, select the preferred streaming format.
4. Move the **Image Rate:** slider to select the number of images per second (ips) you want the camera to stream.

   For H.265 and H.264 cameras and encoders, the image rate 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.

5. 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**.
6. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in kilobits per second (kbps).
7. In the **Resolution:** drop-down list, select the preferred image resolution.
   For thermal cameras, use the default resolution for enhanced video quality.
8. In the **Keyframe Interval:** drop-down list, enter the preferred number of frames between each keyframe. It is recommended to have at least one keyframe per second.

   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.

9. If your camera supports multiple video streams, 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™ technology feature to enhance bandwidth and storage efficiencies.

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

Motion Detection Events

You can configure the system to generate motion events that can be used when searching video or to trigger notifications and rules.

There are two types of motion detection available:

- **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.
- **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.

Setting Up Pixel Motion Detection

Set up pixel motion detection to define motion events. Motion events can be used when searching recorded video, or to trigger notifications and rules.

1. In the New Task menu ≡, click **Site Setup**.
2. Select a camera, then click 🏃.
3. In the **Pixel Motion Detection** tab, define the region of interest (ROI) where motion is detected. A motion event is generated for changes in any pixel within this ROI.

> **Tip:** The motion detection area should avoid reas 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 and drag to add a new pixel motion detection area. You can draw multiple overlays to define the pixel motion detection area.
- ⊟ — click and drag to exclude areas from the pixel motion detection area.
- ✎ — manually draw pixel motion detection areas.
- ⤢ — select the entire image panel for pixel motion detection.
- ☒ — clear the image panel of all pixel motion detection areas.

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

   - **Sensitivity:** — adjust how much each pixel must change before it is considered in motion.

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

   - **Threshold:** — adjust how many pixels must change before the image is considered to have pixel motion.

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

     > **Tip:** The **Motion** indicator above the Threshold: slider indicates how much motion is occurring in the current scene. The camera will only detect pixel motion if the Motion indicator moves to the right of the Threshold: marker.

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

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

Setting Up Classified Object Motion Detection

Set up classified object motion detection to define classified object motion events. Motion events can be used when searching recorded video, or to trigger notifications and rules.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a camera, then click 🏃.
3. In the **Classified Object Motion Detection** tab, configure the green overlay to define the region of interest (ROI) where motion is detected.

   > **Note:** Motion events are only triggered if the bottom center of the detected object's bounding box is in the ROI.

   - To change the shape or size of the overlay, click and drag the markers on the border. Extra markers are automatically added to help you fine tune the shape of the overlay.
   - To move the overlay, click and drag.
   - To add an exclusion area, click ⊞. The red exclusion area is added inside the overlay.

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

        - 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.
        - To delete the exclusion area, select an exclusion area then click ☒.
    - To restore the green overlay, click ⊟.
4. Define the objects that are detected by the system.
    - **Object Types:** — select whether the motion event applies to people or vehicles or both.
    - **Sensitivity:** — move the slider to adjust how likely the system is to generate a motion event.

      If you set the slider to the left, the device will generate fewer motion events for objects detected with higher confidence. Use this setting for scenes with a high level of activity.

      If you set the slider to the right, the device will generate more motion events for objects detected with lower confidence. Use this setting for scenes with little activity.

      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 detections.
    - **Threshold Time:** — enter how long an object must move before a motion event is generated.
    - **Pre-Motion Record Time:** and **Post-Motion Record Time:** — enter how long video is recorded before and after a motion event.
5. Click **Apply** to save your settings.

Recording Schedule

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

Recording Schedule Templates

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

Adding a Template

1. In the New Task menu ☰, click **Site Setup**.
2. Select a server then, click ◉.
3. In the Templates: area, click **Add Template** .
4. Enter a name for the **New Template**.
5. Click the **Set Area** button, then click or drag the cursor across the **Recording Mode:** timeline to set the types of events cameras will record. Individual rectangles on the Recording Mode: timeline are colored when they have been selected.

   The **Recording Mode:** options include:

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

6. To disable recording in parts of the template, click **Clear Area**, then click or drag the cursor across the timeline to remove set recording periods.
7. 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 and set the time between each reference image.

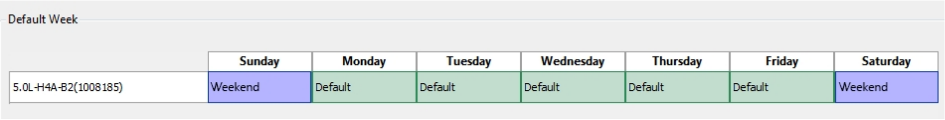
Editing and Deleting a Template

1. In the Setup tab, select the server you want to edit and click ◉.
2. 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**.

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 New Task menu ☰, click **Site Setup**.
2. Select a server, then click ◉.
3. Select a template from the Templates: list.
4. In Default Week, click the days your template will cover for each camera on your site.



Default Week

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
5.0L-H4A-B2(1008185)	Weekend	Default	Default	Default	Default	Default	Weekend

5. Click **OK**.

Recording and Bandwidth

While the Recording Schedule settings define what and when cameras record, the Recording and Bandwidth settings define how long recorded video is stored. This affects Tier 1 storage, and is referred to as Data Aging. Data aging only occurs when the storage is 100% full.

In Recording and Bandwidth 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 cameras connected.

- For JPEG2000 or JPEG compression cameras, data aging is available at three rates:
  - **High Bandwidth** — Records at original quality.
  - **Half Image Rate** — Records half of the data to make room for new recordings.
  - **Quarter Image Rate** — Records a quarter of the original data, allowing you to still view older video.
- H.265 and H.264 cameras that support data aging, are available at two rates:
  - **High Bandwidth** — Keep the original high quality video and a secondary low resolution stream.
  - **Low Bandwidth** — Only keep the secondary stream of low resolution video.

    > **Note:** Data aging only occurs when the secondary stream is enabled.
- For H.265 and 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 you'll find 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.

Configuring Data Aging

> **Note:** When setting up data aging to work with Storage Management Continuous Archive, make a note of the lowest data aging setting. Your lowest setting must be greater than what you entered for Archive video older than:. This ensures that archiving starts before data is deleted on the local ACC Server.

1. In the New Task menu ☰, click **Site Setup**.
2. Select a server, then click ⏲.

   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.

3. In the Data Aging column, move the sliders to adjust the amount of video that 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.
4. 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 Total Record Time is significantly shorter than the Max. Record Time, the camera's actual recording time will be closer to the Total Record Time estimate. The total recording time assumes continuous recording, and will increase with a Recording Schedule.

5. Click **OK**.

Add Users and Groups

Add users and different permission groups for accessing the system.

Adding a User

Add additional users with their own access.

1. In the New Task menu ☰, click **Site Setup**.
2. Click 👥.
3. Click **Add User**.
4. Complete the User Information area.
5. Select the **Disable user** check box to create a profile, but prevent access.
6. 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.
7. Select the **Member Of** tab to assign the user to a group.
   a. Select access group check boxes to assign the user to that group.

      > **Tip:** Clicking on each access group displays the relevant group privileges and access.

   b. Return to the **General** tab.

8. In the Password area, complete the following fields:
    - **Password:** — The password the user will use to gain access.
    - **Confirm Password:** — Re-enter the password.

      The password must meet the minimum strength requirements, defined by how easy it is for an unauthorized user to guess.

      > **Tip:** 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** — The user must replace the password after the first login.
    - **Password Expiry (Days):** — The number of days before the password must be changed.
    - **Password never expires** — The password will never need to be changed.
9. Click **OK**.

Adding Groups

Groups define which features users can access. You can further define privileges by assigning each group a rank, and setting rules on what a group can access.

1. In the New Task menu ☰, click **Site Setup**.
2. Click 👥.
3. Select the **Groups** tab, then click **Add Group**.
4. Select an existing group to use as a template for your new group, then click **OK**.
5. Add the following details in Edit Group:
    a. Enter a group name.
    b. Select a rank from **Rank:**. To edit or view the entire Corporate Hierarchy, click ✎.
    c. Move the **Min Password Strength:** slider to define how strong each user's password must be.
    d. To enable Two-Factor Authentication, select the **Required** check box.

       Users will need an authenticator app on their mobile device to scan a QR code before they can log into a site.

       Ensure your servers sync to a real-time source. If the time on the user's device does not match, they will not be able to log in. Verfication codes are only valid within 5 minutes.

       > **Note:** The default administrator will be able to log in to a site without Two-Factor

> Authentication, even if it is enabled for their group.

> **Important:** Users with Two-Factor Authentication enabled will not be able to use the ACC Mobile 3 app or the ACC Virtual Matrix software.

6. Click **Enable Dual Authorization** to configure Dual Authorization settings. When enabled, users cannot review recorded video without permission from the authorizing group.
    a. Click the toggle to enable Dual Authorization. Click again to disable Dual Authorization.
    b. Select which groups can authorize users.
    c. Click **OK**.
7. In the **Members** tab, add users to the group.

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

    a. Click **Add User**.
    b. Select the users from this site to include in this group or use Search... to refine results.
    c. Click **Add**. The users are added to the Members list.
8. Click **OK** to save the new group.

Customize Video Monitoring Setup

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

Saving Views

After you've customized a View, you can save and share it with users across your site. Saved Views appear in the System Explorer.

Saving a View

1. In the toolbar, click 💾 > **Save As New View**.
2. Select the site you'll add the view to, assign a name, and then add a unique number as the Logical ID

to mark the view in your site.

> **Tip:** Click ⌄ to choose where to display the View in the System Explorer.

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

Editing a Saved View

1. Open a saved View.
2. Make any required changes to the View tab.
3. In the toolbar, select 💾 > **Update Saved View**.

Renaming a View

1. In the System Explorer, right-click ▦ and select **Edit** or **Delete**.
2. Update the Name or Logical ID.
3. Click **OK** to update the View.

Deleting a Saved View

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

Maps

You can create and manage maps that can be monitored in the View tab. Operators can interact with video or alarms from cameras on the map.

Adding a Map

You can add a JPEG, BMP, PNG, or GIF as a layout of your site.

> **Tip:** Maps should be smaller than 3000 x 3000 pixels.

1. In the System Explorer, right-click on your site and select **New Map**.
2. Add a name and click **Change Image...** to upload your map.
3. Select the location of the map in your site hierarchy.
4. Click **OK**.

After a map has been added, you can add camera locations and their view.

Adding Cameras to a Map

After you've uploaded a map, add cameras and highlight their field of view.

1. In the System Explorer, right-click on your map and select **Edit**.
2. Click and drag a camera from the System Explorer to add it on the map.
3. Customize the appearance, direction, and size of the camera.
    - **Size** — How large the icon is in relation to the map.
    - **Show As:** — Display the camera as an icon or shape.
    - **Icon, Shape & Cone Color** — The color of the camera con or shape.
    - **Preferences** — Display the field of view, name, or camera region.
    - **Delete from Map** — Remove the camera from the map.
4. In the toolbar, click **Save**.

Editing and Deleting Maps

You can update a map or delete an old map anytime.

- In the System Explorer, right-click 📍 then select one of the following:
    - To edit the map, select **Edit...**.
    - To delete the map, select **Delete**. When the confirmation dialog box appears, click **Yes**.

Joystick Settings

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

Use the Joystick settings to 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 ACC 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 ACC Client, select ⚙ > **Client Settings** > **Joystick**.

    If the keyboard is not automatically detected, an error message is displayed. Click **Scan for Joysticks...**.
3. 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.
2. In the top-right corner of the ACC Client, select ⚙ > **Client Settings** > **Joystick**.
3. If the joystick is not automatically detected, an error message will appear. Click **Scan for Joysticks...**.
4. 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.
5. 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.

Email Notifications

You can automatically email individuals and groups when events occur.

1. In the New Task menu ☰, click **Site Setup**.
2. Click **External Notifications** ✉.

Configuring the Email Server

When generating email notifications, the ACC Client must have access to an email server.

1. In the Email Server tab, configure the following.
   - **Sender Name:** — The name that will be displayed in each email.
   - **Sender Email Address:** — The email address that will be displayed in each email.
   - **Subject Line:** — The subject displayed in each email.
   - **SMTP Server:** — The server address used by the site.
   - **Port:** — The SMTP port number.
   - **Timeout (seconds):** — The maximum time a server will spend trying to send an email.
2. If the email server uses encryption, select the **Use secure connection (TLS/SSL)** check box. For servers that use STARTTLS encryption, select the **Use STARTTLS** check box.
3. If the email account has a username and password, select **Server requires authentication** check box

and enter the credentials.

4. Click **OK**.

Adding Recipients

1. In the **Email Notifications** tab, click **Add**.
2. Name the new email group and add the recipient information.
   - **Add Email** — Manually add a single email.
   - **Add User/Group** — Include a user or group's email.
3. Select the Email Trigger and customize which cameras, devices, or transactions will be included.
4. Select a schedule and enter a limit on email frequency.
5. Click **OK**.

Editing Email Notifications

1. In the New Task menu ☰, click **Site Setup**.
2. Select your site and click **External Notifications** ✉.
3. Select an email group and makes your changes, or click **Remove** ▬ to delete the group.
4. Click **OK**.

Central Station Monitoring

If you use a third-party monitoring company, you can automatically send notifications for events using the Rules engine.

Note: Notifications are supported as XML through SMTP, or SIA through IP. Check with your monitoring service for their preferred method.

1. In the New Task menu ☰, click **Site Setup**.
2. Select your site and click **External Notifications**✉.
3. In the **Central Station Monitoring** tab, enable central station monitoring and select the method for your notification.
4. Add the email or account information for the monitoring company.
5. Set the **Minimum Heartbeat Interval:** to the frequency your monitoring company recommends. This message confirms that your site is communicating with their network.

   Tip: Click **Send Test Message** to make sure that you've correctly entered all contact information.

6. Click **Apply** then **OK**.

Avigilon Corporation
avigilon.com

PDF-ACC7INSTALLWFLW-A

Revision: 1 - EN

20190604

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. □ Ensure each server has a unique Windows hostname.
4. □ Network switches with enough ports and PoE budget for all camera and server connections.
5. □ Ensure servers are connected to an uninterruptible power supply (UPS) that is powerful enough to provide surge protection and uninterrupted backup power to the system. Configure the UPS connected to servers to shut down Windows during a power outage when there is a certain percentage or time of battery power left (for example, 25% or 15 minutes).
6. □ Ensure switches are also connected to a UPS.
7. □ 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.

8. □ 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.
9. □ IP addresses for the system.

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

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

    avigilon.com/support-and-downloads

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

a Motorola Solutions Company

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 2.

   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.
   - NVR or HD Video Appliance
     a. □ Complete initial Windows setup.
     b. □ Set date and time.
     c. □ Set a unique Windows hostname.
     d. □ Set new password for local administrator account.
     e. □ Activate site license according to system design. See *Activate Site Licenses* on page 8.
   - ACC ES Recorder or Avigilon video analytics appliance
     a. □ Assign password to administrator account in the web interface.
     b. □ Set date and time.
     c. □ Set a unique 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 3.

6. Configure sites and servers:

    a. □ (Enterprise systems only) Merge multiple servers into a single site as required. See *Multiple Server Sites* on page 4.

    - □ Activate licenses for the new site. See *Activate Site Licenses* on page 8.

    b. □ Configure the Site View. See *Editing the Site View* on page 7.

    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.

7. Configure devices:

    a. □ Assign a Logical ID to the camera. See *Setting a Device's Identity* on page 16.

    b. □ Adjust camera focus. See*Zooming and Focusing the Camera Lens* on page 16.

    c. □ Adjust video image and display. See *Image and Display Settings* on page 17.

    d. Set compression and image rate. See *Compression and Image Rate* on page 19.

    - □ Image rate.
    - □ Quality level.
    - □ Keyframe interval.

    e. □ Configure video analytics. See *Configure Video Analytics* on page 11.

    f. Configure motion detection areas.

    - Pixel Motion. See *Setting Up Pixel Motion Detection* on page 21.
        - □ Green motion detection area.
        - □ Sensitivity.
        - □ Threshold.
    - Classified Object Motion. See *Setting Up Classified Object Motion Detection* on page 22.
        - □ Green motion detection area.
        - □ Object Type.
        - □ Sensitivity.
        - □ Threshold.

    g. □ Recording schedule. See *Recording Schedule* on page 23.

    h. □ 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 *Saving Views* on page 28.
    - □ Add maps. See *Maps* on page 29.
    - □ Configure joysticks. See *Joystick Settings* on page 30.
11. □ Configure external notifications. See *External Notifications* on page 31.
12. Configure ACC Mobile 3 access.
    - □ Install the ACC Web Endpoint software. This software is pre-installed on ES and HDVA appliances (RPA, RPO, ENVR1, AS1).
    - □ Download the ACC Mobile 3 application from the App Store or Google Play™ store.
    - □ In the app, configure the site address to point to an ACC IP address.
13. □ Verify setup — Log in as different users to check interface and permissions.