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 on **help.avigilon.com/acc**.

Before Arriving On-Site

Important: If this is the user's first ACC 7 Server or if the server will be upgraded to ACC 7 software for the first time, see the *Avigilon Licensing Portal User Guide*. You may need to contact Avigilon Order Management to set up the user's Company account, Customer Administrator account, and Customer User accounts.

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.

Network Setup

For most systems using Avigilon-certified network video recorders (NVRs) and NVR workstations, no network configuration is required.

If your system uses zero-configuration networking (Zeroconf), follow the guidelines below to use a static IP address or DHCP enabled network instead.

IP Addressing

Plan the IP addressing scheme for server network ports, cameras, devices, and viewing stations.

1. Determine the number and type of network interface card (NIC) ports of the server.
2. Determine the quantity and location of the cameras and devices. Refer to the system design files to determine how many server NICs are required for inbound video traffic and group cameras and devices accordingly.
3. If the cameras and devices are grouped, assign each group to a unique IP subnet. Use a subnet mask that defines the required network scope (for example, networks with less than 250 devices generally use a 255.255.255.0 subnet mask).
4. Assign one server NIC port for outbound video traffic. Assign only one default network gateway to it. This will connect to the customer's network where the viewing stations are and also for Internet access.
5. Use the other server NICs for the camera network. These are for inbound video traffic.
    - Each NIC belongs to one unique IP subnet.
    - If using VLANs, one subnet should belong to one unique VLAN.
    - Do not assign any default network gateway to these NICs. Camera traffic should be as local as possible.
    - Assign one static private IP address to each NIC. If using DHCP, use IP address reservation so each NIC always gets the same unique IP address.
    - For the initial setup:

- If using Static IP addressing:
  - Assign a temporary second IP address to each NIC. This is a unique Zeroconf IP address of 169.254.x.x network with a 255.255.0.0 subnet mask. After the cameras and devices using the Zeroconf subnet are connected to the ACC Server, change their IP addresses to the private IP address subnet of the server NIC.

    For example, a server NIC has:

    IP address / subnet mask: 192.168.10.10 / 255.255.255.0
    Temporary IP address / subnet mask: 169.254.100.100 / 255.255.0.0

    After cameras (with IP addresses 169.254.x.x) are connected to the ACC Server, change the camera IP addresses to 192.168.x.x / 255.255.255.0 range.
  - After the initial setup, remove the server NIC's temporary 169.254.x.x IP addresses.
- If using a DHCP enabled network:
  - Consider the DHCP lease time configured on the DHCP server. When the lease time expires, the cameras will negotiate an IP address renewal and this may cause an interruption in the video streaming. This might appear as an abnormal camera restart.
  - Set the DHCP lease time to Forever, or long enough to minimize unnecessary camera IP address renewals.
  - If possible, set DHCP reservations so each camera always gets the same unique IP address.

Configuring Ports

Configure the network to allow servers, clients, services and devices to communicate. The following tables list ports that need to be opened for specific system components.

ACC Client

Port	Port Type	Protocol	Services	Network Scope	Direction	Encrypted	Optional
38880	TCP	HTTPS	API	ACC Server	Outbound	Yes	No
38881	TCP	HTTPS	API, Media	ACC Server	Outbound	Yes	No
38883	UDP Multicast 239.255.255.0	Custom	Server Discovery	ACC Server	Inbound	No	Yes
51000 to 55000	UDP	RTP/RTCP	Media	ACC Server	Both	No	Yes
443	TCP	HTTPS	Avigilon Cloud Services	Internet (ACS)	Outbound	Yes	Yes

Port	Port Type	Protocol	Services	Network Scope	Direction	Encrypted	Optional
443	TCP	HTTPS	Usage Analytics	Internet (Revulytics)	Outbound	Yes	Yes
443	TCP	HTTPS	Usage Analytics	Internet (Google)	Outbound	Yes	Yes
443	TCP	HTTPS	Licensing (Online)	Internet (Flexera)	Outbound	Yes	Yes

ACC Server

Port	Port Type	Protocol	Services	Network Scope	Direction	Encrypted	Optional
38880	TCP	HTTPS	API	ACC Server	Both	Yes	No
38881	TCP	HTTPS	API, Media	ACC Server	Both	Yes	No
38882	UDP	Custom	Avigilon Cloud Services	Internet (ACS)	Both	Yes	No
38883	UDP Multicast 239.255.255.0	Custom	Usage Analytics	Internet (Revulytics)	Both	No	Yes
38884	UDP	NTP	Usage Analytics	Internet (Google)	Inbound	No	Yes
38980	TCP	Postgres	Database Replication	ACC Server	Both	Yes	No
38981	TCP	Postgres	Database	ACC Server	Both	Yes	No
38982	TCP	HTTPS	Clustering (Gossip)	ACC Server	Both	Yes	No
38983	TCP	MQTT	Clustering (MQTT)	ACC Server	Both	Yes	No
3702	TCP	WS-Discovery	Onvif Device Discovery	ACC Server	Both	No	Yes
51000 to 55000	UDP	RTP/RTCP	Media	ACC Server	Both	No	Yes
59595	UDP Multicast	HTTP	Pelco device	Pelco	Inbound	No	Yes

Port	Port Type	Protocol	Services	Network Scope	Direction	Encrypted	Optional
	239.255.255.0		driver (SOAP)	Cameras			
8443	TCP	HTTPS	Web Endpoint REST API (Windows Only)	Integration, ACC Mobile, Browser Clients	Inbound	No	Yes
443	TCP	HTTPS	Web Endpoint REST API, Administrative Web UI (Appliance Only)	Integration, ACC Mobile, Browser Clients	Inbound	No	Yes
1900	UDP Multicast 239.255.255.250	SSDP	Web Endpoint (Appliance Only)	SSDP Clients	Both	No	Yes
49152	TCP	SSDP	Web Endpoint (Windows Only)	SSDP Clients	Inbound	No	Yes
5353	UDP	MDNS	Web Endpoint	MDNS (Bonjour) Clients	Both	No	Yes
443	TCP	HTTPS, AMQP	Avigilon Cloud Services	Internet (ACS), WebRTC Signalling (Ably, Pubnub)	Outbound	Yes	Yes

Avigilon Cloud Services

For a list of communication ports for ACS, see the ACS **Port Configuration**.

Network Connectivity

Ensure each server NIC is connected to a network switch port that is 1 Gbps or higher.

The server NIC connected to the customer's network can have a 100 Mbps connection if the expected outbound traffic is low.

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 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 NVRs, HD Video Appliances, or Avigilon Hardened OS appliances. Each video recorder must be:

- Connected to the network — camera and corporate network as required.
- Assigned an IP address.
- Assigned a new password for the administrator account.
- Assigned a CA-signed certificate. Refer to your **video infrastructure documentation** for details.
- *Windows systems only*:
    - Assigned a unique name.
    - Connected to an uninterruptible power supply (UPS). Refer to your **video infrastructure documentation** for details.
    - Configured for NTP time synchronization. Refer to your **video infrastructure documentation** for details.

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

Important: Upgrade to the latest version of ACC™ 5 software before upgrading to ACC 7 software to avoid losing data.

If you're using version 5.4, upgrade to version 5.6.2.28 first, and then to the latest version of 5.10 software.

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

If you installed a third-party NVR:

- Download and install the latest ACC Server software and ACC Client software from **avigilon.com**.
- Install the ACC Analytics Service to use the Avigilon Appearance Search feature and Face Recognition.

Install the ACC Web Endpoint Service to use Avigilon Cloud Services, the ACC Mobile 3 app and web-based integrations.

Logging In

To open the ACC Client software:

- Double-click the desktop shortcut icon  .
- In the Start menu, select **All Programs** or **All Apps** > **Avigilon** > **Avigilon Control Center Client**.

When logging in to the site for the first time, the default credentials use `administrator` as the username without a password. You'll be asked to immediately enter a new password.

1. In the New Task menu  , click **Site Login**.
2. Select your site from the list of connected sites.

   If you don't see your site, click **Find Site...** to manually search your network.
3. Enter your credentials, or select **Use current Windows credentials** and click **Log In...**.

Managing Certificates on the ACC Server

By default, the ACC server uses a self-signed certificate for verifying client communications. Avigilon recommends using a trusted CA-signed certificate or other intermediate certificate, such as a Windows CA or custom CA certificate. You must be a Windows Administrator to make these changes.

If you are using a CA-signed certificate, you will need to disable trust of the default Avigilon certificates after setting up your CA-signed certificates to ensure the default certificate can no longer be used.

Important: When logging into the server from a client after setting up your certificate, you will need to use the full hostname, including the domain.

Generating the Certificate

1. On the Windows machine running the ACC server, open the Certificate Manager. Select **Run** in the **Start** menu and enter *certlm.msc*.
2. Navigate to the **Personal** > **Certificates** folder.
3. Right-click in the folder contents area and select **All Tasks** > **Request New Certificate...**.
4. Click **Next**.
5. In the Select Certificate Enrollment Policy window, select the **Active Directory Enrollment Policy** and click **Next**.
6. In the Request Certificates window, select the **Avigilon Computer** checkbox, then expand the **Details** drop-down arrow and click **Properties**.
7. On the **General** tab, enter the **Friendly Name** as ***AccServerCert***.

   Important: Make sure to enter the correct Friendly Name, ***AccServerCert***, or the ACC server and clients will not recognize the certificate and will fail to connect.
8. On the **Private Key** tab, in the **Key options** area, fill the **Make private key exportable** check box.
9. If ACC is running as a specific user account, configure permissions on the private key:
   a. On the **Private Key** tab, in the **Key permissions** area, fill the **Use custom permissions** check box.
   b. Click **Set permissions...** and add the corresponding user account to the group or user list.
10. Click **OK**.
11. On the Request Certificates window, click **Enroll**. Click **Finish** when the operation is complete.

Exporting the Certificate and Private Key

1. Using the certlm.msc tool, right-click the new certificate and select **All Tasks** > **Export...**.
2. Click **Next**.
3. Select **Yes, export the private key** and click **Next**.
4. Leave the Export File Format settings as default and click **Next**.
5. On the Security window:

a. Select the **Group or user names (recommended)** check box and select the Active Directory group or user to which you want to assign access to the certificate and private key.
b. Click **Add**.
c. Click **Next**.

6. Enter the name and location for the exported certificate, or click **Browse** to navigate to the location where you want to save the exported certificate. Click **Next**.
7. Click **Finish** to export the certificate and private key.

Importing the Private Key

1. Using the certlm.msc tool, right-click in the **Personal** > **Certificates** folder contents area and select **All Tasks** > **Import...**.
2. Click **Next**.
3. On the File to Import window, enter the certificate name and path in the **File name** field or click **Browse** to navigate to the certificate you want to import. Click **Next**.
4. Select the Import option to **Mark the key as exportable** and **Include all extended properties**, then click **Next**.
5. Leave the settings as default and click **Next**.
6. Click **Finish**.

Managing Private Key Permissions on Existing or Imported Certificates

1. On the Windows machine running the ACC server, open the Certificate Manager. Select **Run** in the **Start** menu and enter *certlm.msc*.
2. Navigate to the **Personal** > **Certificates** folder.
3. Locate and right-click on the ***AccServerCert*** certificate and select **All Tasks** > **Manage Private Keys...**.
4. In the Permissions for AccServerCert private keys window, add the Network Service account to the group or user list.
5. Click **OK**.

Configure Anti-Virus Settings

When anti-virus software runs an automated scan on a heavily utilized Avigilon NVR 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 NVRs or between NVRs and clients.

You may need to set up exceptions in the anti-virus software running on NVRs, 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

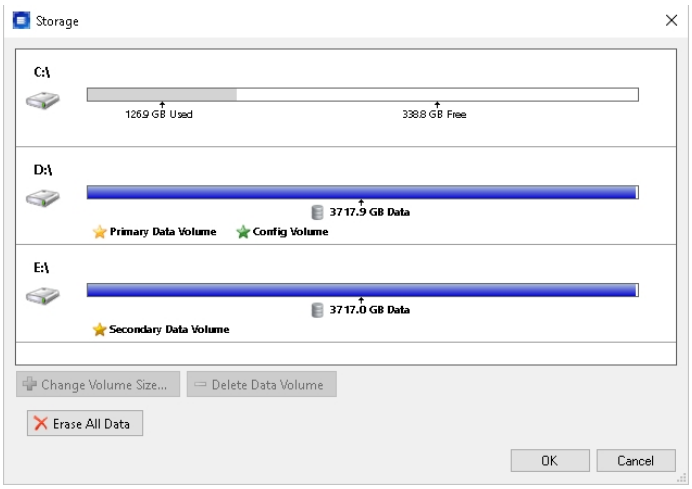
To ensure the anti-virus software does not interfere with the ACC software's ability to write video data and other important files, exclude the following locations from being scanned:

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`.

*Do not use the C drive or an OS drive for these volumes. 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`
  - `C:\Program Files\Avigilon\Avigilon Control Center Web Endpoint\WebEndpointService.exe*`
  - `C:\Program Files\Avigilon\Avigilon Control Center Server\LPR6\LprDaemonApp.exe*`

- `C:\Program Files\Avigilon\Avigilon Control Center Analytics Service\AnalyticsDaemonService.exe`*

  * If installed on the server

- ACC Client Applications:
  - `C:\Program Files\Avigilon\Avigilon Control Center Client\VmsClientApp.exe`
- Avigilon Data folder
  - `D:\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

FOR ENTERPRISE EDITION

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 13.

Note:

- Before you add a server to a site, make sure that Active Directory synchronization is disabled on the server.
- If you're using the Avigilon Artificial Intelligence (AI) Appliance, connect the appliance to an NVR before connecting that NVR to your site.

- Servers must have the same version of the ACC software to be connected.
- Servers should be on the same broadcast domain or broadcast network because the servers will exchange data.
- Ensure ports 38880 to 38884 TCP/UDP are open across the network.
- Ensure servers have unique hostnames.
- When a server joins a site, its site license must be reactivated. For more information, see Reactivating a License.

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.

- Active Directory settings are configured at the site level. Before adding a server to a site with Active Directory, check the following or the connection will fail. For more information, see Importing Active Directory Groups..
  - A Windows server is connected to the same Active Directory domain as the site.
  - If adding an Avigilon Hardened OS appliance to a site with Windows servers, the site must clear the **Use ACC service account** and **Enable nested groups** checkboxes and enter a username (for example, `john.smith@domain.com`) and password.
  - If Active Directory is configured on an Avigilon Hardened OS appliance, it must be connected to the same Active Directory domain as the site. An appliance without any Active Directory configuration can be added to a site and will inherit the domain from the site.

Note: Disconnect the server from a site before making any of the following changes:

- Changing the hostname
- Changing the IP address
- Reinstalling Windows or installing a different version of Windows
- Replacing the server with another server
- Decommissioning the server

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. For more information, see *Reactivating a License* on page 1.

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. For more information, see Deactivating a License.

Site Families

FOR ENTERPRISE EDITION

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 the site name, then click **Manage Site**.
3. Select the site you want to connect as a child.
4. In the bottom-right corner, click **Connect to Parent Site**.

> **Tip:** To connect a single server to a different site, click the server , then click **Connect to Site...**.

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

Disconnecting Site Families

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

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Manage Site**.
3. Select the parent or child site you want to disconnect.
4. In the bottom-right corner, click **Disconnect Child Site...** or **Disconnect from Parent Site...**.
5. Click **OK**.

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

Restricting Login to Parent Sites

If you specify users on a parent site and synchronize them to a child site, to prevent the synchronized users from the child site to be able to log into the parent site:

1. In the parent site Setup tab, click **General**.
2. Select the **Restrict login to only Global and Unranked users** check box.
3. 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 **General**.
3. Enter a name, then click **OK**.

Editing the System Explorer

By default, all cameras are listed in alphabetical order by site in the System Explorer. 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. Each camera grouped under a folder shows up grouped in the Focus of Attention module.

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 the site name, then click **Site View Editor**
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 trial license or a purchased license. Purchased licenses do not expire.

> **Tip:** Keep a copy of the license for future reference.

Activating an Initial Trial License

Activate an initial trial license to access the ACC software for 30 days, enable channel licenses for use after the trial has ended, or try out new features like face recognition or license plate recognition.

> **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 Trial 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.

Online Activation

If you have internet access, use online activation. Licenses are sent in batches to avoid activation failures, which can occur when activating many licenses for large sites. Online activation is recommended over offline activation, however, if online activation does fail, see *Offline Activation* on the next page below.

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

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

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:
   a. In a browser, go to **activate.avigilon.com**.
   b. Click **Choose File** and select the `.key` file.
   c. Click **Upload**.

      A `capabilityResponse.bin` file should download automatically. If not, allow the download to proceed when you are prompted.

   d. Complete the product registration page to receive product updates from Avigilon.
   e. Copy the `.bin` file to the computer running the ACC Client software.
8. In the License Management dialog box, click **Apply...**.
9. Select the `.bin` file and click **Open**.
10. 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

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. To display only devices in uninitialized state, select the **Uninitialized devices** checkbox. The devices are displayed in the Discovered Devices area.
4. 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.

   Note: To connect multiple devices, all cameras must use the same connection settings. To ensure you can enter login credentials for uninitialized devices, do not select a mix of non-factory default devices and factory default devices.
5. Select which server will connect to the devices.
6. 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.
7. 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.
8. In the **Network Type:** drop-down list, select **LAN** (local area network) or **WAN** (wide area network).

   Select the **WAN** network type to connect cameras on your local network if the Internet Control Message Protocol (ICMP) is blocked or disabled.

9. To connect the devices to the ACC Server, enter the password for the `administrator` username, or create a username and set a new password.

   Note: If you forget the login credentials for a device, refer to factory reset instructions in the device manual and repeat these steps to reset its password.

10. 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.

11. Click **OK**.

Device Network Settings

Change the IP address of each device after connecting it to ACC site. Then remove the device's default IP address from the server's network ports.

Note: If the device has a Zeroconf IP address of 169.254.x.x with subnet mask of 255.255.0.0, change its IP address to a unique static private IP address in the same IP subnet as the server network interface card (NIC).

For example:

- Server NIC IP Address / Subnet Mask : 192.168.10.10 / 255.255.255.0
- Current device IP Address / Subnet Mask: 169.254.123.140 / 255.255.0.0
- New device IP Address / Subnet Mask : 192.168.10.100 / 255.255.255.0

1. In the New Task menu , click **Site Setup**.
2. Select a device, then click **Network** .
3. Select how the device obtains an IP address:
    - **Obtain an IP address automatically:** — The device will connect to the network through an automatically assigned IP address.

      The device will attempt to obtain an address from a DHCP server. If this fails, the device will obtain an address through Zero Configuration Networking (Zeroconf) and select an address in the 169.254.0.0/16 subnet.

    - **Use the following IP address:** — Manually assign a static IP address to the device.

      Enter the **IP Address:**, **Subnet Mask:**, and **Gateway:** you want the device to use.
4. Select the **Control Port:** for connecting to the device. This port is also used for manually discovering the device on the network.
5. For cameras, select the **Enable Multicast** checkbox to enable multicast streaming from the device. This is required to set up redundant recording to multiple servers.

   Use the default generated **IP Address:**, **TTL:**, and **Base Port:**, or enter your own values.
6. Click **OK**.
7. For Rialto Video analytics appliances, allow the system to restart the device.

Configure Video Analytics

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

If the system will use the Avigilon Appearance Search™ feature or Face Recognition, enable each required camera to support this feature.

Enabling Analytics

You can enable and disable server-based analytics on cameras throughout your site to manage the server's analytics load.

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

> **Important:** If your site is connected to an AI Appliance to provide analytics processing on the video streams from non-analytics cameras, expand the site and then click on the **Server Analytics** .

3. Select an analytics feature tab and then select the cameras to enable the feature on.

   Only cameras that you have access to that have the prerequisite analytics enabled are displayed in each tab.

   > **Tip:** If you do not see one of the tabs, check that you have the required license. Appearance Search and No Face Mask Detection need ACC Enterprise, while Face Recognition and Firearm Detection require separate licenses.

   > **Important:** Firearm Detection is available only on the AI NVR and not on the AI appliance.

As you enable (or disable) analytics for cameras, the bars at the bottom update to display the server's capacity. The percent usage of each analytics feature is displayed using the color of the analytics feature tab.

To exit the Server Analytics panel, click **Close**.

Identity Data Retention

FOR ENTERPRISE EDITION

> **Note:** These settings override protected bookmarks and video retention settings.

Depending on your privacy policy or regional regulations, you may only be able to retain identifying data for a specific amount of time.

1. In the New Task menu  , click **Site Setup**.
2. Click the site name, then click **Identity Data Retention**  .
3. Select the checkbox next to each available feature and enter the maximum number of days to retain data.
4. Click **OK**.

When choosing these settings, consider the types of acceptable uses for video security footage in your privacy policy. For example, if appearance search signatures are retained for only 3 days, a search initiated from an image of a person will only return results over the last 3 days of video. This happens even if recorded video is retained for a longer period and makes it difficult to determine if someone visited your site at any time outside of the identifying data retention period. Similarly, if license plate data is retained for only 5 days, it will be impossible to use a person's license plate data recorded in the system to search for occurences of their vehicle that may have occurred more than 5 days ago.

Configuring Camera Analytics

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 Camera Configuration Tool available on avigilon.com/support.

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 **Settings** .
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** — suitable for most outdoor environments. This setting optimizes the camera to identify vehicles and people. • **Large Indoor Area** — only detects people and is optimized to detect people around obstructions, like chairs and desks, if the head and torso are visible. • **Indoor Overhead*** — optimized for cameras mounted directly overhead and should only be used when a torso cannot be seen in the camera field of view. Any movement is assumed to be human. Use in areas with limited space but with high ceilings, or to monitor doors. Do not use with the Avigilon Appearance Search feature, Face Recognition, the Self-Learning feature, or to detect people traveling against the crowd. • **Outdoor High Sensitivity*** — optimized to run with higher sensitivity for

Setting	Description
	detecting people and vehicles in challenging outdoor scenes. This option may generate more false positives. Only use this option if you require the system to be more sensitive than the Outdoor setting. • **Long Range Night*** — prioritizes outdoor long-range object detection at night over object classification and tracking during the day. Uses external IR illumination rather than built-in IR illumination from the camera. Object classification and tracking accuracy during the day is reduced compared to other outdoor modes. Available for H4A cameras only. • **Indoor Close-up** — only supported on modular cameras. This option only detects people and is optimized to detect people that occupy most of the camera field of view. Vehicle detection is not supported in this mode and Self Learning analytics is disabled. Object crosses beam and Direction violated analytic events are also not supported in this mode. * These modes are not available for H5A cameras. **Note:** The H5A Fisheye camera does not support video analytics when installed on a wall or on a floor. It must be installed on a ceiling to support video analytics. When a camera is installed on a ceiling, also ensure that the camera View Perspective: is set to Ceiling. For more information, see Dewarping Fisheye Displays.
Enable Noise Filter	Select the checkbox if the camera is too sensitive and falsely detects motion as classified objects.
Display Classified Objects	Select the checkbox to display bounding boxes around classified objects in recorded video.
Enable Tampering Detection	Select the checkbox to enable tampering detection. If cleared, the device will no longer send tampering events.
Sensitivity:	Enter a value between 1-10 to select how sensitive a camera is to tampering 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

Setting	Description
	events will be sent by the camera.
Enable Self Learning	Select the checkbox to enable self-learning. If you clear this checkbox, more classified objects may be falsely detected.

Video Analytics Mode

If your device supports Unusual Motion Detection, you can enable Classified Object or Unusual Motion mode for a video analytics device.

> **Tip:** If your device is connected to a server that provides Classified Object Detection, 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. See *Enabling Analytics* on page 20.

1. In the New Task menu  , click **Site Setup**.
2. Select a device, then, click **General**  .
3. In the **Video Analytics Mode:** drop-down list, select one of the following:
   - **Classified Object** — Detect and classify people or vehicles.
   - **Unusual Motion** — Detect unusual pixel motion based on typical speed and direction of movement in a scene.
   - **None** — Do not use analytic capabilities.
4. Click **OK**.

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 Camera Analytics* on page 21.
5. Click **Apply** to save your settings.
6. If you are prompted, allow the device to reboot.

   You can now enable self-learning or configure video analytic events.

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** checkbox. 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.
	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 **Image and Display**  .
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.

- **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.

> **Note:** The camera bandwidth may vary depending on the mode.

6. Select the **Disable IR filter in Night Mode** check box to disable the IR filter when Day/Night Mode: is set to Night Mode. If the IR filter is disabled, the camera will stream in color.
7. If available, move the:
   - **Day/Night Threshold:** slider to set the exposure value (EV) when the camera changes from day to night mode.
   - **Night/Day Threshold:** slider to set the exposure value (EV) when the camera changes from night to day mode.

> **Note:** The H5 Hardened PTZ camera supports the installation of a narrow spot illuminator that can be controlled from the ACC Client. See Using the H5 Hardened PTZ Illuminator.

8. 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.

Option	Description
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.
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 checkbox 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 checkbox 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

Option	Description
	clockwise.
White Balance	Control white balance settings to adjust for differences in light. To let the camera control the white balance, select **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.

9. 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 **Compression and Image Rate** .

   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. In the **Stream Mode:** drop-down, select the number of streams. **Single Mode** (HDSM 2.0) enhances the resolution and quality from applicable cameras, but may reduce performance in integrated third-party software. Use **Dual Mode** in this case. Dual Mode uses a primary and secondary stream to manage bandwidth usage.
5. Move the **Image Rate:** slider to select the number of images per second (ips) you want the camera to stream. A higher Image Rate results in better video quality but more storage and network bandwidth usage.

   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.

6. In the **Image Quality:** drop-down list, select an image quality setting. An image quality setting of **1** will produce the highest quality video, require the most bandwidth, and use more storage. The default setting is **6**.
7. In the **Max Bit Rate:** field, select the maximum bandwidth the camera can use in kilobits per second (kbps).
8. In the **Resolution:** drop-down list, select the preferred image resolution.
   For thermal cameras, use the default resolution for enhanced video quality.
9. 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. For example, if the Image Rate is 20 images per second (ips), set the Keyframe Interval: to 20. This results in 1 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.
10. If your camera supports multiple video streams, select the **Enable Low Bandwidth Stream** checkbox. Depending on your version of the software, the checkbox 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.
11. Click **Apply to Devices...** to apply the same settings to other cameras of the same model.
12. Click **OK**.

Motion Detection Events

Motion detection is usually used to trigger video recording. For more information, see *Recording Schedule Templates* on page 35.

You can also 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.

  > **Note:** The H5A Fisheye camera displays a circular deadzone in the center, overlayed on the image in the analytics panel. Object detection is not available in this circular area.

- **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.

Select a camera, then click **Motion Detection**  .

When using motion detection to trigger video recording for situations where high security is a requirement, it is recommended to use Pixel Motion Detection instead of Classified Object Motion Detection because:

- Configuration required for analytic settings varies with different environments.
- Recordings triggered by Classified Object Motion Detection are not triggered for the duration of the event and will only record starting from when the event first began for the amount of time specified by the Pre-Motion Record Time: and Post-Motion Record Time: settings. If the event lasts longer than this, some of the event will not be recorded.

If it is still desired to record on Classified Object Motion Detection alone, then additional and through testing needs to be done to ensure that all relevant objects can be detected in the environment.

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 **Motion Detection**  .
3. In the **Pixel Motion Detection** tab, define the region of interest where motion is detected. A motion event is generated for changes in any pixel within this region of interest.

   > **Tip:** 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 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 **Motion Detection**  .

   > **Note:** The H5A Fisheye camera displays a circular deadzone in the center, overlayed on the image in the analytics panel. Object detection is not available in this circular area.
3. In the **Classified Object Motion Detection** tab, configure the green overlay to define the region of interest where motion is detected.

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

- 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. This exclusion area is only for Classified Object Motion detection. It does not apply to other analytics features like Analytic Events, Motion Search, and the Avigilon Appearance Search feature.

  - 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 the objects that will trigger the motion event.
   - **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.

     Important: The system detects both stationary and moving objects. However, an object must be moving for at least 1 second before it is classified as moving and can trigger a motion event. The effect is that any object that moves for less than a second is not classified as a moving object and cannot trigger a motion event. The initial 1 second that an object moves is added to the specified threshold time value to determine if the motion event is triggered.
   - **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 **Recording Schedule** .
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:** checkbox and set the time between each reference image.

Editing and Deleting a Template

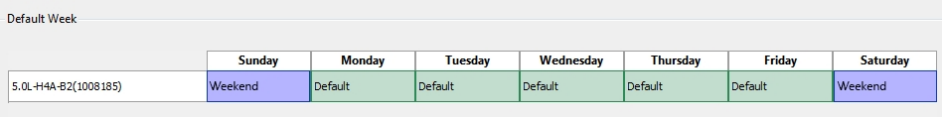
1. In the Setup tab, select the server you want to edit and click .
2. Select a template from the Templates: pane and do one of the following:
   - To edit a template, modify the schedule.
   - To rename a template, click **Rename Template** and enter a new name.
   - To delete a template, click **Delete 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 **Recording Schedule** .
3. Select a template from the **Templates:** list. For more information, see *Recording Schedule Templates* above.

4. In Default Week, click the days your template will cover for each camera on your site.



5. Click **OK**.

Recording and Bandwidth

The Recording and Bandwidth settings define how long recorded video is stored. You can set the maximum record time for each camera connected to a server, and configure Data Aging settings.

Video Retention

The Total Record Time is estimated based on continuous recording and may not reflect the actual video retention.

The actual video retention is determined by the Max. Record Time setting and the average camera data rate. The actual retention time may exceed the Max. Record Time setting by 5 minutes.

Data Aging

Data aging is when ACC deletes videos based on their age in relation to the Max. Record Time setting. ACC prioritizes newer over older recorded video. By default, the Data Aging setting stores both high-resolution and low-resolution video until the Tier 1 storage is full. Once the storage is full, older video will be deleted.

ACC deletes older videos when any of the following occur:

- The Max. Record Time setting is set to the maximum value and the storage is full.
- A new camera is added and the storage is full.
- The Max. Record Time setting is set to X days and the stored videos are older than X days, even if the storage is not full.
- The slider is moved to the left and the change is saved; high-resolution videos are deleted based on the adjustment.

Video storage pertains to the data volume defined using the ACC Admin Tool.

To increase the amount of video stored when the Tier 1 storage is full, update the Data Aging setting to discard a percent of the high-resolution video. The system will discard the oldest high-resolution video and only store the low-resolution video to maximize storage. The oldest video stored will be low-resolution.

Note: Data Aging is shown in approximate days. It is applied as a percentage of the total footage. The number of Data Aging days is not guaranteed to change immediately after there are changes made to the system like adding cameras, or adjusting the Max. Record Time setting. ACC reviews stored recordings of all cameras and recalculates the predicted Data Aging days and Total Record Time. This may take a few days depending on the Data Aging and Max. Record Time settings, the number of cameras, and storage size.

The extent 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. Some cameras have a tertiary stream.

- For H.265 and H.264 cameras that do not support data aging, only the **High Bandwidth** video is kept.

Configuring Data Aging

1. In the New Task menu, click **Site Setup**.
2. Select a server, then click **Recording and Bandwidth**.

   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 users to monitor and manage your site.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups**.
3. Click **Add User**.
4. Complete the User Information area.
5. Select the **Disable user** checkbox to create an account, but prevent access.
6. In the Login Timeout area, select the **Enable login timeout** checkbox 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 checkboxes to assign the user to that group.

    > **Tip:** Click an access group to display the group's privileges and access rights.

    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. To enable access to Avigilon Cloud Services, ensure the correct email address is entered and select the **Connect** checkbox.

    The user will receive an email invitation after the site is connected to the Avigilon Cloud Services.

10. 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 the site name, then click **Users and Groups**.
3. In the Groups tab, 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** checkbox.

    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. Verification 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.

    e. To enable Emergency Privilege Override, select the **Enabled** checkbox. For more information, see *Emergency Privilege Override* on the next page.
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.

Emergency Privilege Override

Emergency Privilege Override is a group permission that gives operators access to the following privileges without needing dual authorization:

- View high-resolution images
- View live images
- View recorded images
- View images recorded before login
- Use PTZ controls
- Broadcast to speakers
- Listen to microphones

Create a new group to manage who has Emergency Privilege Override permissions.

1. In the New Task menu  , click **Site Setup**.
2. Click the site name, then click  **Users and Groups**.
3. In the Groups tab, click **Add Group**.
4. Select an existing group to use as a template for your new group, then click **OK**.
5. Next to Emergency Privilege Override:, select the **Enabled** checkbox.
6. Enter a name and in the Members tab, select users to add to the group.
7. Click **OK** to save the group.

Users assigned to groups with this privilege can enable Emergency Privilege Override. For more information, see *Enabling Emergency Privilege Override* below.

Enabling Emergency Privilege Override

If you are part of a group with emergency override privileges, you can enable access to high-resolution live and recorded video, including video recorded before you logged in, and control PTZ cameras, microphones, and speakers. To configure your group permissions, see *Emergency Privilege Override* above.

1. In the System Explorer, right-click a site and select **Enable Emergency Override**.
2. Click **Yes** in the following dialog box.

Emergency privilege override will be disabled once you log out or if you right-click the site and select **Disable Emergency Override**.

Note: If you are part of a group with emergency override privileges but do not see the Enable Emergency Override option, you may already have access to all emergency privileges.

Customize Video Monitoring Setup

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

Tip: Create a Saved View for each fisheye camera to display each view of the dewarped image.

Saving Views

FOR STANDARD AND ENTERPRISE EDITION

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

FOR STANDARD AND ENTERPRISE EDITION

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.

> **Note:** To learn more about the new Maps (Preview) feature, see the **ACC Maps (Preview) User Guide** on **help.avigilon.com**.

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** checkbox.
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**.

Avigilon Cloud Services

Avigilon Cloud Services (ACS) enables a modern cloud-connected user experience, accessible from a web browser or the ACC Mobile 3 app.

With ACS, you can:

- View live and recorded video.
- Access Saved Views. Only the first 9 cameras are available when opening a Saved View in the web client.
- Create custom Saved Views. These are only available in the ACS web client and cannot be shared between users.
- Control PTZ cameras using mouse controls. Activate existing PTZ presets and tours from the web client. New presets and tours created in the web client will be saved to the ACC site.
- Activate digital outputs. If a digital output is associated with a camera in the ACC client, it can be triggered from the cloud platform.
- Create, view, and manage bookmarks in the web client. Changes are synchronized between the ACC site and web client.
- Download MP4 video clips and snapshots to a local drive.

For more information about using the ACS platform, see **help.avigilon.com/cloud**.

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 Server 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)** checkbox. For servers that use STARTTLS encryption, select the **Use STARTTLS** checkbox.
3. If the email account has a username and password, select **Server requires authentication** checkbox and enter the credentials.
4. Click **OK**.

> **Tip:** After the Email Server is configured, you can add Rules that send email notifications to selected recipients.

Adding Recipients

1. In the **Email Notifications** tab, click **Add**.
2. Configure the following.
    - **Email Group Name:** — Enter a name for the email group.
    - **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. To attach camera images to the email notifications, select the **Attach images from device(s) linked to the event** checkbox.
5. Select an **Email Schedule** and enter a limit on email frequency.
6. Click **OK**.

Editing Email Notifications

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then 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

FOR STANDARD AND ENTERPRISE EDITION

Notifications are supported as XML over SMTP or SIA over IP. Check with your monitoring service for their preferred method.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then 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**.

After Central Station Monitoring is configured, you can create a rule to automatically send email notifications with video or image attachments.

For More Information

For additional product documentation and software and firmware upgrades, visit **support.avigilon.com**.

Technical Support

Contact Avigilon Technical Support at **support.avigilon.com/s/contactsupport**.

Avigilon Corporation
avigilon.com

PDF-ACC7INSTALLWFLW-G

Revision: 5 - EN

20230814

Pre-Site Checklist

Installer: _____

Project Name:_____

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.

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

1. ☐ Confirm if the Keep Your Drive Warranty is needed.
2. ☐ Avigilon Network Video Recorders (NVR).
    - ☐ Spare monitor for server configuration (VGA).
3. Client workstations
    - ☐ Avigilon Remote Monitoring Workstations, including monitors.
        - Some models come with a single Display Port (DP) 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.
4. ☐ Ensure each server has a unique hostname.
5. ☐ Network switches with enough ports and PoE budget for all camera and server connections.
6. ☐ 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 during a power outage when there is a certain percentage or time of battery power left (for example, 25% or 15 minutes).
7. ☐ Ensure switches are also connected to a UPS.
8. ☐ 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.

9. ☐ 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.
10. ☐ IP addresses for the system. This is provided by the IT group at the site if you are putting the system on their network.
    - Ensure IP addresses of cameras are in a private IP subnet (for example. 10.x.x.x, 192.168.x.x, or 172.16.x.x), different from the customer's IP subnet.
    - Use a subnet mask that defines the required network scope (for example, networks with less than 250 devices generally use a 255.255.255.0 subnet mask).
    - The server NIC connecting to the customer's network has one default network gateway. All other server NICs should have no default network gateway.
11. Test each camera. Ensure you have the correct mounting accessories and installation tools:
    - ☐ Laptop for running the Camera Configuration Tool.
    - ☐ USB Wi-Fi Adapter for H4 cameras
    - ☐ PoE splitter
12. Download a copy of the latest firmware and software from **avigilon.com**.
    - ☐ Avigilon Hardened OS appliance firmware
    - ☐ 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 and Face Recognition)

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.

   Test and configure a camera before installing it in a high location (for example, a 20-foot pole). Ensure you have the correct tools and mounting accessories, including a complete set of screws.

   For more information, see *Install Hardware and Software* on page 6.

   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. This should be on a private subnet range (for example, 10.x.x.x or 192.168.x.x), different from the customer's IP subnet.

2. ☐ Install the video recorder.
   - Windows NVR or HD Video Appliance
     a. ☐ Complete initial Windows setup.
     b. ☐ Set date and time.
     c. ☐ Set a unique hostname.
     d. ☐ Set new password for local administrator account.
     e. ☐ Create a back-up administrator account. Set the password.
     f. ☐ Add a trusted CA-signed certificate to the ACC Server. See *Managing Certificates on the ACC Server* on page 7.
     g. ☐ Connect server to a UPS. Refer to your **video infrastructure documentation** for details.

- Avigilon Hardened OS appliance
    a. ☐ Assign password to administrator account in the web interface.
    b. ☐ Set date and time.
    c. ☐ Add a trusted CA-signed certificate to the server using the appliance web interface. Refer to your **video infrastructure documentation** for details.

3. ☐ Configure NTP time synchronization. Avigilon Hardened OS appliances have DHCP configured NTP by default.

> **Note:** Time differences between Avigilon Cloud Services and your ACC Service can cause unexpected behavior. To prevent differences in Avigilon Cloud Services time and ACC Server time, configure your server or appliance to synchronize with a network time protocol (NTP) time server.

4. ☐ Install and run the ACC Client software on local workstation.
    - ☐ Ensure the ACC Client software is the same version as the ACC Server software.
5. ☐ Install and run the ACC Analytics Service on Windows servers. This software is pre-installed on Avigilon Hardened OS appliances.
6. ☐ Configure anti-virus settings for Windows servers and workstations. See *Configure Anti-Virus Settings* on page 9.
7. Configure sites and servers:
    a. ☐ Make sure that all ACC Data Volumes have similar sizes. If there is a storage volume that is much larger than the others, make the largest volume as the Primary Data Volume.
    b. ☐ (Enterprise systems only) Merge multiple servers into a single site as required. See *Multiple Server Sites* on page 11.
    c. ☐ Activate licenses for the new site. See *Activate Site Licenses* on page 16.
    d. ☐ Configure the Site View. See *Editing the System Explorer* on page 15.
    e. ☐ Connect cameras to the servers. See *Connecting a Device* on page 18.
    f. ☐ Enable analytics devices. See *Configure Video Analytics* on page 20.
8. Configure devices:
    a. ☐ Assign a Logical ID to the camera. See *Setting a Device's Identity* on page 25.
    b. ☐ Adjust camera focus. See*Zooming and Focusing the Camera Lens* on page 26.
    c. ☐ Adjust video image and display. See *Image and Display Settings* on page 27.
    d. Set compression and image rate. See *Compression and Image Rate* on page 30.
        - ☐ Image rate.
        - ☐ Quality level.
        - ☐ Keyframe interval.
    e. ☐ Configure video analytics. See *Configure Video Analytics* on page 20.

f. ☐ Configure motion detection areas.
    - ☐ Pixel Motion. See *Setting Up Pixel Motion Detection* on page 32.
        - ☐ Green motion detection area.
        - ☐ Sensitivity.
        - ☐ Threshold.
    - ☐ Classified Object Motion. See *Setting Up Classified Object Motion Detection* on page 33.
        - ☐ Green motion detection area.
        - ☐ Object Type.
        - ☐ Sensitivity.
        - ☐ Threshold.

g. ☐ Recording schedule. See *Recording Schedule* on page 34.

h. ☐ Data aging settings. See *Recording and Bandwidth* on page 36.

9. ☐ Add users and groups. See *Add Users and Groups* on page 38.
10. ☐ Configure Avigilon Rules and Alarms as required to satisfy all system functionality per the system design documentation.
11. Customize video monitoring setup:
    - ☐ Add Saved Views. Create a Saved View for each fisheye camera to display each view of the dewarped image. See *Saving Views* on page 41.
    - ☐ Add maps. See *Maps* on page 42.
    - ☐ Configure joysticks. See *Joystick Settings* on page 43.
12. ☐ Configure external notifications. See *External Notifications* on page 44.
13. ☐ Connect the site to Avigilon Cloud Services to view video from a browser or the ACC Mobile 3 app.
    - ☐ Install the ACC Web Endpoint software on Windows servers. This software is pre-installed on Avigilon Hardened OS appliances.
    - ☐ Connect the ACC site to the cloud and add users. See **help.avigilon.com/cloud**.
    - ☐ Download the ACC Mobile 3 application from the App Store or Google Play™. Sign in with your Avigilon Cloud Services credentials.
14. ☐ Verify setup — Log in as different users to check interface and permissions.