Avigilon Cloud Services User Guide

Avigilon Corporation
avigilon.com

PDF-CLOUD-C

Revision: 21 - EN

20230324

Table of Contents

User Guide

Use Avigilon Cloud Services to connect to Avigilon (ACC) sites to perform remote and secure video monitoring, system health checks and user administration for your organization or customer organizations.

Connecting ACC™ to the Cloud

This section describes how to connect your ACC site to Avigilon Cloud Services so users can view video from their browser or mobile device.

Before Connecting Your ACC Site

- Check the *System Requirements* on page 4.
- Ensure your ACC site has Internet access.
- Ensure that each ACC Server is version 7.12 or later and that the same version of the ACC Web Endpoint Service is installed and running.
- If you have a multi-server site, add all servers to the site before connecting to Avigilon Cloud Services. Otherwise you will have to disconnect the standalone servers from Avigilon Cloud Services before adding them to your single ACC site.
- Ensure each server has the correct time zone, date, time, and daylight saving time settings. For a multi-server site, ensure the servers are synchronized to a network time protocol (NTP) server.

Registering Your Organization

Administrators should register their organization in Avigilon Cloud Services. This organization can include one or more ACC sites and provides users with access to cameras across all sites.

1. In your browser, go to **cloud.avigilon.com**.
2. Select a **region*** then click **Create a new ACS organization**.
3. Enter the organization name and your contact information. Click **Submit**.
4. If Google™ reCAPTCHA is not supported, you will be directed to contact **support@avigilon.com**.
5. A registration email will be sent. Complete your registration:
    a. In the email, click the registration link. This link is only valid for 24 hours.

    If the link expires, register your organization again.

    If the link expires, contact *AvigilonCloud Services Support* to resend the link.

    b. Create a password. This password is unique to Avigilon Cloud Services and does not need to match your ACC password.

    Your password must contain 8-50 characters and include at least one:

    - Uppercase letter
    - Lowercase letter
    - Number
    - Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

    Your password cannot include the word "Password".

    If you are a federated user, you are not prompted to set a new password. Avigilon Cloud Services will use your identity provider credential, such as a Microsoft account.

    c. Select your **Preferred communication language**. This sets the language for emails from Avigilon Cloud Services.

    d. Click **Submit**, then click **Sign in** and enter your credentials.

    e. Review and accept the End User License Agreement.

Adding a Site to Your Organization

1. After the organization has been created, get an activation code in Avigilon Cloud Services:
    a. In the Sites tab, click **Add site**.

    b. Enter the site name, address, and select a Primary Contact who will receive email notifications about the site.

    c. Click **Add**. A code is displayed.

    > **Note:** Administrators can get a new code for sites with an expired activation code.
    >
    > Click the  icon next to the Code Expired label to generate a new code.

2. Copy the code and enter it in the ACC Client software:

a. In the New Task menu , click **Site Setup**.

b. Click the site name, then click **Avigilon Cloud Services** .

c. Click **If you have an activation code, click here.**.

d. Enter the activation code and click **Connect**.

The system should connect shortly. If the system takes more than 15-20 minutes to finalize the connection, disconnect your site and try again.

Adding Users to Avigilon Cloud Services

After the ACC site is connected, an ACC administrator can enable users to access Avigilon Cloud Services. Users imported from Active Directory or ACM™ can also be enabled, however these users will have a unique password for Avigilon Cloud Services that may differ from their ACC password.

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. Select a user, then click **Edit User**.
4. Enter an email address if not already specified. This will be the username in Avigilon Cloud Services.
5. Select the **Connect** checkbox and click **OK**.
6. Click **Yes** to confirm the email address.

   The user will receive an email invitation with a registration link that expires within 24 hours. If the email does not appear, check the junk or spam folder.

Signing In to Avigilon Cloud Services

Users can sign in with their Avigilon Cloud Services credentials at **cloud.avigilon.com** and on the ACC Mobile 3 app.

Note: When you connect to Avigilon Cloud Services, two user groups are automatically created:

- Cloud Administrators
- Cloud Viewers

By default, these user groups have access rights to view all cameras in Avigilon Cloud Services and cannot log in to the ACC Client. Update these groups' access rights according to your organization's policies.

Do not assign ACC users to be members of these groups.

Giving Users Additional Privileges

Avigilon Cloud Services administrators can manage sites, users, and view the System Health dashboard. Avigilon Cloud Services managers can also view dashboards without site or user management privileges. For

more information, see *User Roles* on page 63. You can elevate users to be an administrator or manager.

In Avigilon Cloud Services:

1. On the  Organization Management page > Users tab, select a user.
2. In the **Role** drop-down list, select Administrator or Manager.
3. Click **Save**.

* Avigilon Cloud Services Regions

Selecting USA will host your organization and accounts on Microsoft Azure servers in the United States. Selecting Asia Pacific or Oceania will host your account in Australia. All other options will host your account in Canada. Note that all users must select the same region to log in to their accounts.

System Requirements

Software Requirements

- ACC Server software version 7.12 or later

  Sites with ACC software below this version may not have access to complete Avigilon Cloud Services functionality.
- ACC Web Endpoint Service version 7.12 or later
- ACC software edition Core, Standard, or Enterprise

Supported Cameras

- Avigilon H5 Pro cameras
- Avigilon H5A, H5SL and H5M cameras
- Avigilon H4A and H4SL cameras
- Avigilon H4 and H5A Fisheye cameras with dewarp
- Avigilon H4 Pro cameras
- Avigilon Multisensor cameras
- Avigilon pan, tilt, and zoom (PTZ) cameras
- Avigilon HD Pro cameras
- ONVIF® Profile S cameras
- Analog cameras with the use of an **Avigilon analog encoder** or an ONVIF encoder

  ONVIF is a trademark of Onvif, Inc.

Avigilon Edge Solution (ES) cameras are not supported. H.265 video streaming is supported on all the supported browsers as listed below with the exception of Google Chrome. JPEG2000 and MJPEG streaming formats are not supported in the web client.

Microsoft Edge browser can be used to stream H.265 video sources by installing and enabling the High Efficiency Video Coding (HEVC) codec extension:

1. Install the **HEVC Video Extensions** plug-in from the Microsoft Store. It is a paid plug-in and covers royalties.
2. Enter `edge://flags` in the address bar of the Microsoft Edge browser and hit enter.
3. Enable the **PlayReady DRM for Windows 10** flag.
4. Restart the browser.

Supported Browsers

The following browsers are supported on Windows 10, macOS®, and Chromebook™ devices:

- Google Chrome™ browser version 72.0 or later
- Safari browser version 12.1 or later
- Microsoft Edge browser version 80.0.361 or later

Browsers on mobile devices are currently not supported.

Supported Devices

- ACC Mobile 3 app version 3.18 or later available on the App Store and the Google Play™ store

The minimum device requirements are:

	Android	iOS
Platform	Android version 10.0 or later	iPad with iOS 14 or later iPhone with iOS 14 or later iPod touch with iOS 14 or later
Processor	n/a	64-bit (Apple A7 or later)

Bandwidth Requirements

Tip: For guidance on bandwidth recommendation and to learn how to check your bandwidth, go to the **Avigilon Support Community** and search for "How to Check Internet Bandwidth for Avigilon Cloud Services (ACS) and WEP" to read the support article.

Streaming Video

The number of streams you can view at the same time depends on your download bandwidth and other activity on your ACC server or appliance, including other users who may be streaming or downloading video.

For example, a 3 MP camera running at 6 fps requires 1-3 Mbps depending on the video quality. Each user viewing a camera will take up a concurrent stream.

In addition to the streaming capacity of the hardware used to run the ACC software, you may also be limited by your internet service provider's download speed.

Downloading Video

Downloading video uses upload bandwidth and is affected by other network activity, including the number of people trying to stream or retrieve video at the same time.

If users try to stream and download video at the same time, the users streaming video will be given priority.

If you have an upload speed of 5 Mbps, only one user can download high quality video from one 3 MP

camera running at 6 fps. Up to 5 users could concurrently download low quality video from the same camera.

Using the Cloud Platform

With Avigilon Cloud Services, you can:

- View live and recorded video.
- Access ACC Saved Views. These views are read-only and display only the first 9 cameras when viewed in the web client.
- Create personal Saved Views. These are only available in the Avigilon Cloud Services 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.
- If your user account has the appropriate permissions in the ACC site, you can also:
    - 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.

Disconnecting ACC from the Cloud

Note: An Internet connection is required.

You can disconnect your site from Avigilon Cloud Services at any time. Cloud users will no longer have access to cameras or video from the site.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Avigilon Cloud Services** .
3. Click **Disconnect**.
4. To confirm, click **Yes**.

   A success message is displayed and your site is disconnected.

   Synchronized cloud users are deleted from the ACC site.
5. Click **Close**.

You can confirm the status of your connection on the ACC Site Health page.

Getting Started

Registering Your User Account

When an Administrator invites you to Avigilon Cloud Services platform, you'll receive an email invitation from the Avigilon Cloud Services Team.

1. In the email, click the registration link. This link is only valid for 24 hours.

   If the link expires, contact your administrator to disable and re-enable cloud access for your ACC user account.
2. Create a password. This password is unique to Avigilon Cloud Services and does not need to match your ACC password.

   Your password must contain 8-50 characters and include at least one:

   - Uppercase letter
   - Lowercase letter
   - Number
   - Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

   Your password cannot include the word "Password".

   If you are a federated user, you are not prompted to set a new password. Avigilon Cloud Services will use your identity provider credential, such as a Microsoft account.
3. Select your **Preferred communication language**. This sets the language for emails from Avigilon Cloud Services.
4. Click **Submit**, then click **Sign in** and enter your credentials.
5. Review and accept the End User License Agreement.

Registering from the Sign In Page

1. Click the **Not registered? Sign up** link on the Sign In page.
2. In the Register organization page, fill out your **Organization Name** and **Email**.
3. Click **Submit**. Look in your inbox for a registration email, register your user account, and sign in using your identity provider credential, such as a Microsoft account.

Changing Organizations

If you have access to multiple Avigilon Cloud Services organizations, you can switch between them.

1. In the top-right corner, click your name.
2. Click **Switch Organization**, then select an organization.

You can only view video from the selected organization.

Viewing Organization Information

For subscriber administrators only.

- If the circle indicator is displayed next to the Organization Management > General tab, click the tab to fill out incomplete organization details.

Signing In

Note: If an incorrect password is entered three times, the account will be locked for 30 minutes. Click **Forgot my password** to change your password and access your account. This occurs only if you are a non-federated user who is not using an identity provider credential, such as a Microsoft account.

1. Go to cloud.avigilon.com.
2. Select the region specified by your administrator.

   After the first time you sign in to a region, you can bookmark the selected region.
3. Enter your email and click **Next**.
4. Enter your password and click **Submit** or **Sign in**.

   You are signed in.

Signing Out

- In the top-right corner of your browser, click your name and select **Sign Out**.

Provisioning Federated Authentication with an Identity Provider

Administrators of Avigilon Cloud Services and Microsoft Azure™ cloud services can enable Federated Authentication with a trusted identity provider and then configure Avigilon Cloud Services to allow users of the end-user organization, or service provider, to log in using their identity provider credentials, such as a Microsoft Azure Active Directory.

Note: Avigilon Cloud Services Federation supports authentication and does not currently support authorization. As a result, you must add users as described in *Adding a Federated User* on page 12. In a future release we will add support for authorization based on group membership.

Configuring Your Azure Active Directory for Federation

1. For Azure cloud configuration information, see Azure Active Directory (AD).

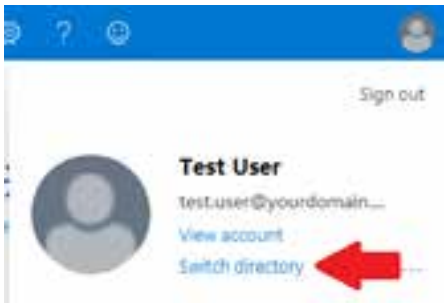
   To register the Azure AD tenant application for your customer end-user or service provider organization, complete the following steps. See also the general steps at Microsoft.com (docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-add-identity-providers#create-an-azure-active-directory-application).

a. Register an application within your organizational Azure AD tenant.

   This step enables sign-in from an AD B2C organization.

b. Sign in to the Azure portal.

c. Make sure you're using the directory that contains your organizational Azure AD tenant. Select the **Directory + subscription filter** in the top menu and then choose the directory that contains your Azure AD tenant.



d. Choose **All services** in the top-left corner of the Azure portal, and then search for and select **App registrations**.

e. Select **New registration**.

f. Enter a **Name** for the application. Accept the default selection of **Accounts in this organizational directory only**.

g. Select the **Access Tokens** and **ID Tokens** check boxes. The settings are required for MSAL.js integration.

h. For the **Redirect URI**, accept the value of **Web** and enter the following URL in lowercase letters: https://acsb2cprod.b2clogin.com/acsb2cprod.onmicrosoft.com/oauth2/authresp

i. Select **Register**. Record the **Application (client) ID** and **Tenant ID**.

j. Select the **Access Tokens** and **ID Tokens** check boxes. The settings are required for MSAL.js integration.

> **Note:** The MSAL.js 2.0 version does not currently support Azure AD B2C for use with the PKCE authorization code flow. Thus, Azure AD B2C recommends using the implicit flow.

k. Select **Certificates & secret** and then **New client secret**.

l. Enter a **Description** for the secret, select an expiration, and then select **Add**. Record the **Value** of the secret immediately.

m. Grant Permissions to the **Graph API**:

   i. Complete the steps at [Microsoft.com (docs.microsoft.com/en-us/azure/active-directory-b2c/microsoft-graph-get-started?tabs=app-reg-ga).]

   ii. Select **Add a permission**.

   iii. Select **Microsoft Graph**.

   The following permissions are required:

   - **User.Read (Delegated)**: To read user profile via the Graph API.
   - **User.Read.All (Application)**: To read user profile via the Graph API.
   - **Profile (Delegated)**: To add user profile information to the token.
   - **Openid (Delegated)**: To add preferred_username to the token

n. Check **Grant Admin Consent** after granting permissions to the **Graph API**.

o. Enable optional claims in the ID token configuration:

   - **family_name**: Provides the last name or family name of the user.
   - **given_name**: Provides the first name or given name of the user.
   - **preferred_username**: Provides the preferred username claim.

2. Submit a form (forms.gle/W7Dvea6eB6FqtrgD6) to Avigilon with the following information:
    - The recorded Application (Client) ID
    - The Tenant ID
    - The Secret
    - Requested date and time for federation
    - Your time zone

Configuring Okta for Federation

1. Create a new app integration:
    a. Sign in to your Okta organization with your administrator account.
    b. In the Admin Console, go to **Applications** > **Applications**.
    c. Click **Create App Integration**.
    d. Select **OIDC - OpenID Connect** as the Sign-in method.
    e. Select **Web Application** as the Application type and click **Next**.
    f. Enter an application name in the **Application name** field.
    g. Under **Grant Type**, select the **Authorization Code**, **Confidential** and **Implicit (Hybrid)** check boxes.
    h. Under **Sign-in Redirect URIs**, enter `https://acsb2cprod.b2clogin.com/acsb2cprod.onmicrosoft.com/oauth2/authresp`.
    i. Leave **Sign-out Redirect URIs** blank.
    j. Click **Save** to finish creating the Okta app integration.
    k. In the General tab, copy the **Client ID** and **Client secret** values from the Client Credentials section, and the **Okta Domain** value from the General Settings section and provide it to Avigilon.
    l. In the Okta API Scopes tab, grant consent to the `okta.users.read.self` scope.

    See the Okta Developer portal for more information.
2. Configure a Custom Groups Claim:

    A custom group claim is needed to include group information in the token.
    a. In the Admin Console, from the Security menu, select **API**, and then select the default Authorization Server.
    b. Under the Scopes tab, add a new scope and call it **groups**.
    c. Select **Include in public metadata** for this scope.
    d. Go to the Claims tab and click **Add Claim**. Enter **Groups** as the name for the claim.
    e. In the **Include in token type** section, leave Access Token selected.
    f. Select **groups** as the Value type.
    g. In the Filter drop-down box, select **Matches regex** and then enter `.*` as the Value.
    h. Select the **Include in the following scopes** option and enter the **groups** scope.

    See the Okta Developer portal for more information.

3. Create an Access token scope to be used in API calls:
    a. In the Admin Console, from the Security menu, select **API**, and then select the default Authorization Server.
    b. Under the Scopes Tokens tab, add a new scope and call it **access_token**.
    c. Select **Include in public metadata** for this scope.
4. Under Applications, click **Assign Users to App** and assign your users to the newly created application.
5. Create an Access Policy:
    a. In the Admin Console, from the Security menu, select **API**, and then select the default Authorization Server.
    b. Select **Access Policies**, and then **Add Policy**.
    c. Enter a **Name** and a **Description** for the policy.
    d. Select **The following clients:** and enter the name of the Okta OpenID Connect application that you created above. This field auto-completes the names of your OpenID Connect applications as you type.
    e. Click **Add Rule**.
    f. For the Scopes requested field, select **The following scopes:** and add **groups**, **openid**, **profile**, **email**, **phone**. Leave everything else to the default value.
    g. Click **Create Policy**.

    See the **Okta Developer** portal for more information.
6. Submit a form (**forms.gle/W7Dvea6eB6FqtrgD6**) to Avigilon with the following information:
    - Supported email domain
    - The Okta Client ID
    - The Okta Client Secret
    - The secret expiry date
    - The Okta Domain
    - Requested date and time for federation
    - Your time zone

Adding a Federated User

Avigilon Cloud Services federation does not automatically provision users from Active Directory groups. Once your organization is federated, and if you haven't already added users to your organization, you must select and add users to ACS as described above.

Federated users can be added to Avigilon Cloud Services by selecting the Connect to Cloud check box for the users on the ACC server, or by adding the user on the ACS Users tab. If the user already exists on the ACC server, adding them from the server is recommended since they have already been assigned to the correct groups in the ACC system. These users will then be added to ACS with a Viewer role, which can be changed in ACS if required.

For more information about the 2 methods for adding federated users:

- Syncing users from the ACC server. See *Creating and Syncing ACC Users to the Cloud* on page 65.
- Adding a user on Avigilon Cloud Services:

    1. In the  Organization Management > Users tab, click **Add user**.
    2. Enter the email account in **Email**.
    3. Enter a **Role**. For more information, see *User Roles* on page 63.
    4. Click **Save**. An invite is sent to the email account.

Note: If you already have an organization on ACS, you do not need to create a new organization when you federate. The original ACS passwords expire and users log into ACS using the federated identity provider instead of ACS for authentication.

Port Configuration

Refer to the following table to make sure that:

- Avigilon devices can connect to the Avigilon Cloud Services platform.
- Avigilon Cloud Services users can connect to the platform.
- Avigilon Cloud Services users can view live and recorded video streamed peer to peer from the Avigilon device to their browser or mobile device.

Definitions:

- **Public Internet**: Ports required to be open for the device to be connected to Avigilon Cloud Services platform and stream video
- **Camera Network**: Ports required to be open for cameras to connect to the local Avigilon device for configuration and streaming video to the device
- **Corporate Network**: Ports required to be open for the Avigilon device to be discovered on the local network and time services

Port	Network	TCP or UDP	Service or Protocol Name	Used by
443	Public Internet	TCP	Secure Sockets Layer (SSL or HTTPS)	• Avigilon device Web UI • Avigilon Cloud Services platform • Device connection to cloud API over SSL • File upload to cloud storage • WebRTC
1025-65535	Public Internet	TCP	Session Traversal Utilities for NAT (STUN)	Peer to peer video streaming to a host or server reflexive

Port	Network	TCP or UDP	Service or Protocol Name	Used by
3478 or 443	Public Internet	UDP or TCP	Traversal Using Relays around NAT (TURN)	Video streaming using the Avigilon Cloud Services platform relay service
1935	Public Internet	TCP	Real-Time Streaming Protocol (RTSP)	Video streaming to third-party integrations that use the media API to get RTSP streams
3702	Camera Network	UDP	ONVIF	ONVIF camera discovery messages (only needed on the camera network)
123	Corporate Network	UDP	Network Time Protocol (NTP)	Provides date and time settings to the Avigilon device outgoing on the corporate local area network (LAN) and date and time settings to cameras incoming on the corporate LAN **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.
51000-55000	Camera Network	UDP	Real-Time Transport Protocol (RTP)	Cameras (only needed on the camera network)
49152	Corporate Network	TCP	Universal Plug and Play (UPnP)	Device discovery on Microsoft Windows
5353	Corporate Network	UDP	Multicast DNS (MDNS)	Bonjour (device discovery on Macintosh)

Safelisting Services Used by ACS

ACS uses Microsoft Azure and other third-party services to deliver its feature set. Users may not have remote

access to video, but need to review System Health from multiple remote sites, or receive security and health events from sites.

Add firewall rules for Microsoft Azure at the following fully qualified domain name (FQDN) locations. The services in the table below are required to establish base system communication, system health heartbeats, and event notifications:

	United States (TCP port 443)	Canada (TCP port 443)	Australia (TCP port 443)
Azure Web Services	us.cloud.avigilon.com (52.179.97.15)	ca.cloud.avigilon.com (40.85.212.173) and us.cloud.avigilon.com (52.179.97.15)	au.cloud.avigilon.com (13.75.218.45) and us.cloud.avigilon.com (52.179.97.15)
Azure Blob Storage	blueprodeastus01ops.blob.core.windows.net (52.239.154.100)	blueprodcentralca01ops.blob.core.windows.net (40.85.235.62) and blueprodeastus01ops.blob.core.windows.net (52.239.154.100)	blueprodeastau01ops.blob.core.windows.net (13.75.240.84) and blueprodeastus01ops.blob.core.windows.net (52.239.154.100)
Azure IoT Hub	blue-prodeastus01-iot-hub.azure-devices.net (40.114.53.146)	blue-prodcentralca01-iot-hub.azure-devices.net (52.237.27.123)	blue-prodeastau01-iot-hub.azure-devices.net (104.210.105.7)
Kubernetes	ingress.cluster.prodeastus01.acs314159.com	ingress.cluster.prodcentralca01.acs314159.com	ingress.cluster.prodeastau01.acs314159.com

Note:
The listed IP addresses may change without notice but can be verified through DNS lookup.

All the servers of a multi-server ACC site must have access to the services listed above. Notifications to the ACC Mobile 3 app require that each server can contact the listed Azure services.

ACS uses messaging hubs to facilitate negotiation of secure media access. Ably and PubNub services are used for WebRTC signalling and Twillo provides Traversal Using Relays around NAT (TURN) media relay services. These are required to view live or recorded video on the ACS web client or the ACC Mobile application.

Ably (TCP port 443)	• REST requests: `rest.ably.io` • Realtime (WebSocket) connections: `realtime.ably.io` • Ably services are hosted on AWS servers. The service is elastic and IP addresses are reassigned dynamically.

PubNub (TCP port 443)	• `ps.pndsn.com` • PubNub services are hosted on AWS servers. The service is elastic and IP addresses are reassigned dynamically.
Twilio (WebRTC) (TCP port 443)	• `global.turn.twilio.com` • Reference: **https://www.twilio.com/docs/stun-turn/regions**

Note: Third-party video integrations using ACS media API use TCP port 1935 outbound to relay 40.87.44.243.

Video

Viewing Live Video

You can view live video on the Views page from cameras in sites you have access to. If you already have saved views, see *Opening a View* on page 32.

1. Select an image panel, and then click .

   The camera list is displayed, and the selected image panel is outlined in blue.

   For more information, see *Camera List* on page 33.

   Tip: You can hover your mouse over a camera name to display a snapshot of the video.

2. Select the camera you want to view.

   The camera is added to the image panel and its live video is displayed.

   Tip: You can drag and drop a camera into an image panel. If another camera is already displayed, it is replaced by the new camera.

3. While the camera list is displayed, you can continue to select image panels and then select cameras to add to those panels.

Changing Video Quality

By default, the player always uses the **LOW** quality setting in order to conserve bandwidth. You can change the player's video quality for the current player session. Select **AUTO** quality to see more detail. Select **LOW** quality if you have a slower internet connection.

1. In the bottom-right corner of the video player, click  .
2. Select the **Video Quality**.

   The video quality is updated. The video quality will revert back to the default setting after you close or navigate away from the player.

Focusing the Camera

Sometimes a camera may not be focused. Instead of calling for support, you can reset the focus from the video player.

1. In the bottom-right corner of the video player, click  .
2. Click **AUTO**.

Video Streaming Timeout

Continuous video streaming in Avigilon Cloud Services may timeout after a specific period of user inactivity. This inactivity duration may differ if you have a restrictive firewall configuration. Click **Resume** to continue streaming video.

Viewing Recorded Video

> **Tip:** In the top-right corner, click  to sync video from all players in a view.

Using the Timeline

The timeline lets you search recorded video from a particular camera.

- Open the video player for the camera.

  For more information, see *Viewing Live Video* on the previous page.

  A timeline appears when you hover over the video player.

  Markers show the time and date. The blue bands represent recorded video. The red bands represent a recorded motion event.

  - **To use one timeline for all video players in a View**, in the top-right corner, click  to sync video.
  - **To search recorded video**, drag the white marker along the timeline or click the date to select when to view video.
  - **To increase or decrease the time range**, scroll over the timeline or click  /  on the left side of the timeline. You can increase the time range up to several days.

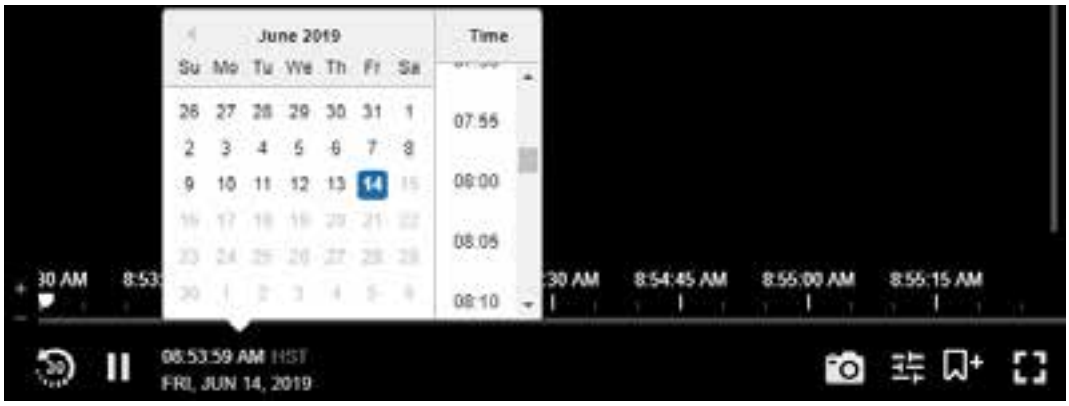
- **To jump backwards or forwards in time**, click the left or right side of the timeline. The video will play from the time selected.
- **To return to live video**, click REC X in the upper-right corner of the player window.
- **To hide the timeline**, move your mouse away from the video player window.

Selecting a Date

You can view recorded video from a certain date and time using the video player.

1. At the bottom of a video player, click the date and time.

   A calendar is displayed.



2. Select a date and time.

   The player will display recorded video from that time.

Using a PTZ Camera

With the Avigilon Cloud Services platform, you can monitor video and control the position of a PTZ camera.

PTZ controls are available when viewing live video from a PTZ camera on the Views page.

Using a PTZ Camera

PTZ controls are available when viewing live video from a PTZ camera on the Views page.

1. In the video player, click or PTZ Off to display the PTZ controls.

The camera's PTZ controls are overlaid on the video and manual pan and tilt controls are enabled. For more information on using manual pan and tilt controls, see *Moving a PTZ Camera* below.

Control	Description
AUTO	Auto-focus the PTZ camera.
	Go to the Home position.
	Display the Presets list where you can move to a preset, or create and delete presets. You can also access the Tours list where you can run, create, and delete tours.
	Display the Zoom controls.

2. To hide the PTZ controls, click or PTZ On.

Moving a PTZ Camera

As you move the PTZ camera's field of view, the camera's recording will move with the changing field of view.

Analytic rules with PTZ cameras can only be used at the Home position of the PTZ camera. Moving the camera will disable analtyics rules until the PTZ has moved back to the home position. For more information,

see *Go To Home Position* on the next page.

> **Tip:** PTZ controls like click-to-center and continuous panning will also function when other PTZ controls are open, such as the Zoom or Preset controls.

Click-to-Center

1. Click  or 

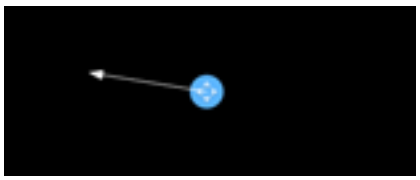
to display the PTZ controls and enable manual pan and tilt controls.
2. If click-to-center is supported by your camera, click anywhere on the video image to center the camera on that point.

   The camera's live video moves to center on the selected point.

Continuous Panning

1. Click  or 

to display the PTZ controls and enable manual pan and tilt controls.
2. Drag your mouse from the center  in the direction you want the camera to pan. The farther the mouse is from the center of the player, the faster the camera will move.

   The camera's live video moves as directed.

   While the camera is panning, you can drag in other directions to adjust the camera movement.
3. Release the mouse button to stop panning.

Keyboard PTZ Controls

Using the PTZ keyboard controls is ideal for small adjustments to the PTZ camera position. Each keystroke will move the camera a small amount.

1. Click  or 

to display the PTZ controls and enable manual pan and tilt controls.
2. Use the keyboard keys to control and pan and tilt movements of the camera. You can tap the key to make a small movement or hold it down to move faster. The table below lists the different PTZ control keys.

PTZ Control	Keyboard Keys		Number Pad Keys
Move left	←	A	4
Move right	→	D	6

PTZ Control	Keyboard Keys		Number Pad Keys
Move up	↑	W	8
Move down	↓	S	2
Zoom in	+		+
Zoom out	–		–

Focusing a PTZ Camera

You can automatically adjust the focus of your PTZ camera. Click AUTO to have the PTZ camera automatically focus on the scene.

Go To Home Position

If your PTZ camera has a Home preset position configured, you can click to move the camera to the Home position.

For more information on configuring the Home position, see *Creating a Preset* below. Select the **Set as Home** checkbox while creating a preset to make it the Home position.

> **Note:** Analytic rules with PTZ cameras can only be used at the Home position of the PTZ camera. Make sure that the field of view of the Home preset includes any areas that require analytic rules.

PTZ Preset Positions

You can control PTZ camera movement by directing the camera to move to preset positions. You can also manage your presets by creating and deleting them.

Click to open the Presets list.

Moving to a Preset Position

1. With the Presets list open, scroll through the list to find the preset you want to move to.
2. Click the Preset.

   The camera's live video will move to the selected preset position.

Creating a Preset

1. Use the camera's PTZ controls to move the camera's field of view to the desired preset position. For more information on moving the camera, see *Moving a PTZ Camera* on page 19, and *PTZ Camera Zoom Controls* on page 23.
2. Click to open the Presets list.
3. Click **Create New Preset** at the bottom of the Presets list.

4. Enter a descriptive name for the new preset.
5. Click ✓ to save the new preset or click ✕ to discard the preset.

   If you want this preset to be the Home position, select the **Set as Home** checkbox.

   > **Note:** You cannot edit a preset. If you want to modify an existing preset you will have to delete it and create a new preset.

Deleting a Preset

1. With the Presets list open, scroll through the list to find the preset you want to delete.
2. Click 🗑 for that preset.

   The selected preset is deleted and removed from the Presets list.

PTZ Tours

You can control PTZ camera movement by directing the camera to run a PTZ tour. Tours allow the PTZ camera to automatically move between a series of preset positions and can be set to pause at each preset for a specific amount of time. The tour will repeat until manually stopped or other PTZ controls are used.

> **Note:** The PTZ tour will stop when you or any other user uses the PTZ controls for that camera.

Click ⛶ to open the list of presets, then click **Tours** to open the list of tours.

Running a PTZ Tour

1. With the Tours list open, scroll through the list to find the tour you want to run.
2. Click the Tour.

   The camera's live video will move through the preset positions configured with the tour.
3. To stop the tour, click **Stop Tour** or use any other PTZ control.

Creating a Tour

1. Use the camera's Presets list to create all of the preset positions that you will need for this tour. For more information on creating presets, see *Creating a Preset* on the previous page.
2. Click ⛶ to open the list of presets, then click **Tours** to open the list of tours.
3. Click **Create Tour** at the bottom of the Tours list.

The Tour Builder dialog box is displayed.

4. Enter a descriptive name for the new tour in the **Tour Name** field.
5. In the **Pause Duration** field, enter the amount of time the tour will pause before it repeats. Tours will repeat until manually stopped or other PTZ controls are used by any user.
6. Select a **Tour Mode** from the drop-down list:
    - **Sequential**: The PTZ camera will go to each preset in the set order.
    - **Random**: The PTZ camera will go through the list of presets in a random order.
7. If you want this tour to run automatically after a set amount of time that the PTZ camera has been idle, select the **Set as default tour** checkbox. Set the time the camera should be idle before it will automatically run in the **Idle Start Time** field.

    The tour will automatically start after the PTZ camera has been idle for the set time.

    > **Note:** Setting the current tour as the default tour will automatically remove this setting from the previous tour that was set as default.

8. Click **Add Another Preset** to add a preset to the Tour Builder.
    a. Select the **Preset** to add from the drop-down list.
    b. In the **Speed** field, enter how fast you want the PTZ camera to move to this preset. The higher the %, the faster the camera will move.
    c. In the **View Time** field, enter the amount of time you want the PTZ camera to stay at this preset position before moving to the next preset. The View Time is 10 seconds by default.
    d. Repeat this step until you have added all of the presets for this tour.
9. To remove the preset from a tour, click  for that preset.
10. To re-order a preset in the tour, click ↑ or ← for that preset. The preset order only affects tours that use Sequential mode.
11. Click **Save** to save the tour.

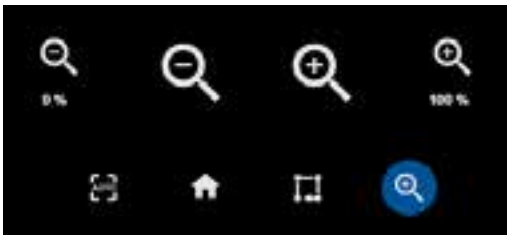
Editing a Tour

1. Click  to open the list of presets, then click **Tours** to open the list of tours.
2. Click  for the tour you want to edit.
3. Edit the tour settings and options. For more information on the tour settings, see *Creating a Tour* on the previous page.
4. Click **Save** to save the tour.

PTZ Camera Zoom Controls

You can control the PTZ camera zoom with the PTZ controls. Zoom in to see more detail or zoom out to see more of the surrounding scene.

Click  to open the zoom controls.



Zoom Control	Description
Zoom all the way out	Click 0 % to zoom all of the way out. This can be used to reset the PTZ zoom to the default view after zooming in on an object in the scene.
Zoom all the way in	Click 100% to zoom all of the way in. This can be used to quickly zoom in to the maximum zoom to see more detail in the scene.
Zoom out	Click to zoom out by 5% increments.
Zoom in	Click to zoom in by 5% increments.
Zooming with the mouse wheel	Use the mouse wheel to adjust the zoom in and out by scrolling the wheel forwards and backwards.
Dragging to zoom	If the camera supports drag to zoom, you can click and drag a green rectangle on the video image to define the area you want to zoom in and see.

Using a Fisheye Camera

Stream, zoom, and pan live and recorded HDSM 2.0 and dewarped fisheye video in ACS. The ACS video player supports full primary resolution of Avigilon panoramic fisheye cameras when the player is displaying a full screen view and the video quality is set to AUTO. The ACS video player checks the ACC setting for fisheye dewarp for a camera and if dewarp is enabled in ACC, then dewarp is also enabled by default in the ACS video player.

To toggle the dewarp mode:

1. In the video player, click to display the video player settings menu.
2. Click **Dewarp**.
3. Click **On** or **Off** to toggle between the dewarp modes.

Scroll with the cursor over the viewport to push the video view into a domed fisheye representation of the view. Click and drag to move in either direction. Zoom in or zoom out with the scroll wheel. When zoomed in and displaying in full screen view, dewarping happens automatically. You can also utilize a 360 panoramic overview in your layouts. A dewarped fisheye device functions and can be controlled as a regular PTZ device.

See *Using a PTZ Camera* on page 19.

You can also display analytics bounding boxes over the video being viewed. See *Displaying Analytics Bounding Boxes* below.

Note: Saving a virtual view from a fisheye camera region of interest is not supported.

Triggering a Digital Output

Note: The proper permissions in the ACC site are needed.

All users can trigger available digital outputs from a camera's video player.

Digital outputs are only available while viewing live video.

1. Hover over the player to display the Digital Outputs  .

   Hover over a toggle to see the output name.
2. Click  next to the output you want to trigger:
   - If the output mode is set to **Pulse**, the output will stop after the specified pulse duration.
   - If the output mode is set to **Hold**, click  again to stop the digital output.

Displaying Analytics Bounding Boxes

Depending on where the player is used, analytic bounding boxes may or may not display over the video being viewed. You can change the Analytics Activity setting to show analytic activity bounding boxes around recognized objects such as persons or vehicles. You can display bounding boxes on any type of video, such as live video, recorded video, event video, or bookmarked video.

1. In the bottom-right corner of the video player, click  .
2. Click **Analytics Activity**.
3. Click **All**, **Motion Only**, or **Off** to enable or disable the analytic bounding boxes.

   The analytics activity setting will revert to the default setting after you close or navigate away from the player.

Enabling Audio

If a camera has its Speaker settings configured in the ACC Client software, you can enable the camera's audio in the Avigilon Cloud Services player.

- In the video player, click  to enable audio or  to disable audio.

Downloading Video

Note: The proper permissions in the ACC site are needed.

You can download an MP4 video from a specific date and time from any camera you have access to in a video player. You can use the video for further investigation or archive it.

1. In the video player, click  .

   The Download video dialog box is displayed.
2. Using the camera's local time, select the date and start time.
3. In the **Duration:** box, enter how long the video should be. The maximum duration is 60 minutes.
4. Set the Quality to **High** to download a high resolution clip or **Low** to download a low resolution clip.
5. Click **Submit**.

Downloading a Snapshot

Note: The proper permissions in the ACC site are needed.

If you notice something interesting while monitoring live or recorded video, you can download a PNG snapshot of the video player to your computer. You can use the image as evidence in an investigation, or share it across your team to raise awareness of a person of interest.

- In the video player, click  .

  A snapshot is downloaded.

Video Player Controls

The following table describes each video player control. Available controls may vary based on whether you are viewing live or recorded video.

Control	Description
	Skip back 30 seconds.
	Pause video.
	Play video.
	Skip forward 30 seconds.

Control	Description
	Volume off. Click to enable audio.
	Volume on. Click to disable audio.
	View PTZ controls.
	Download a snapshot of the video.
	Configure the video player's settings.
	Download video.
	Create a bookmark of the selected video.
	Go to fullscreen mode.
	Exit fullscreen mode. You can also press Esc.
	Zoom in on the timeline. You can also hover over the timeline and scroll.
	Zoom out on the timeline. You can also hover over the timeline and scroll.
	Trigger a digital output. Hover over this control to see the digital output name.
Camera name	View player and connection details. Click  to pin player details to the video player.
Click to Jump	Jump backward and forward by clicking the left or right side of the timeline.
Scroll to Zoom	Zoom the video in and out.
Drag to Move	While zoomed in, you can click and drag to move the video's field of view.

Bookmarks

Adding a Bookmark

> **Note:** The proper permissions in the ACC site are needed.

Bookmark recorded video to find and review an event later. Bookmarked video can be protected from scheduled data cleanup so that the video is never deleted.

1. Find the point in the recorded video timeline that you want to start the bookmark and click  .

   The Create Bookmark dialog box appears with the selected Start time and End time.
2. In the **Cameras** pane, select the cameras to include.

   You can only bookmark multiple cameras from the same site.
3. Enter a **Name** and **Description**.
4. Enter the **Duration** of the bookmark.

   This will automatically update the End time. You can also update the End time to specify the duration of the bookmark.
5. To protect the bookmarked video from being deleted, under Protect bookmark, select **Yes**.

   Important: Protected bookmarks are never automatically deleted. Be aware that protected bookmarks take up storage space and can become your oldest stored video. Protected bookmarks should be manually deleted when they are no longer needed. For more information, see *Protecting and Unprotecting a Bookmark* below.
6. Click **Save**.

Protecting and Unprotecting a Bookmark

Protecting bookmarks prevents them from being deleted. Protected bookmark can become the oldest stored video on your server. Unprotected bookmarks on the other hand may be deleted by scheduled or automatic data cleanup.

1. On the  Bookmarks page, expand a site.
2. Next to a bookmark, click  . The Edit a Bookmark page is displayed.
3. Under Protect bookmark, select **Yes** or **No**.
4. Click **Save**.

Note: Too many protected bookmarks may fill available storage on your server and may impact normal operation. Delete protected bookmarks that are no longer needed or set them as unprotected so they will be automatically deleted.

Searching for a Bookmark

1. On the  Bookmarks page, expand a site.
2. On the right, select a date range. The date range refers to the bookmark video Start Time, not Date

Created.

3. In the **Bookmark name or description** box, search for a bookmark.

   Only matching results within the date range are displayed.

Viewing Bookmarked Video

1. On the Bookmarks page, expand a site.
2. Click a Bookmark Name to view the bookmarked video and details.
3. Use the timeline and player controls to review the video.

   For more information, see *Viewing Recorded Video* on page 17.
4. If the bookmark is linked to multiple cameras, select the camera to view from the **Cameras** list to the left of the video player.
5. To edit the bookmark, click **Edit**.

   For more information, see *Editing a Bookmark* below.

Editing a Bookmark

1. On the Bookmarks page, expand a site.
2. Next to a bookmark, click . The Edit a Bookmark page is displayed.

   You can also edit a bookmark when you are viewing that bookmark.
3. Make any changes needed to the bookmark.

   For more information about the editable options, see *Adding a Bookmark* on page 27.

Deleting a Bookmark

1. On the Bookmarks page, expand a site.
2. Next to a bookmark, click .
3. Click **OK**.

   The bookmark is removed from the bookmarks list.

Views

Adding a View

> **Note:** Views are unique to each user and are not shared between users. Changes will not appear in the ACC site.

Create new views to help monitor related groups of cameras from a single view.

1. In the top-right corner, click **New view**. This clears cameras from the current view.
2. Set up the view to your requirements:
    - **Set the view layout to the desired number of video panels.**
    - **Add and change the camera feeds in the view.**
    - **If necessary, make this view a favorite or default view.**
    - **Save and name the new view.**

    Once it has been saved, this view can be used any time you sign in to your account.

Changing the Layout

You can change the number of image panels displayed on the Views page by changing the layout. You can have up to nine image panels in a single layout. Choose the number of image panels that makes sense for the scene you're viewing.

Note: Changing the layout will not remove cameras from your view.

- In the top-right corner, select a Layout.

Changing a Camera in a View

Use the camera list to change the camera displayed in an image panel.

You can review recorded video for a disconnected camera by adding that camera to a view and using the timeline controls to find the recorded video. For more information, see *Viewing Recorded Video* on page 17.

1. Select an image panel, and then click .

   The camera list is displayed, and the selected image panel is outlined in blue.

   > **Tip:** You can hover your mouse over a camera name to display a snapshot of the video.

2. Select the camera you want to view.

   The camera is added to the image panel and its live video is displayed.

   > **Tip:** You can drag and drop a camera into an image panel. If another camera is already displayed, it is replaced by the new camera.

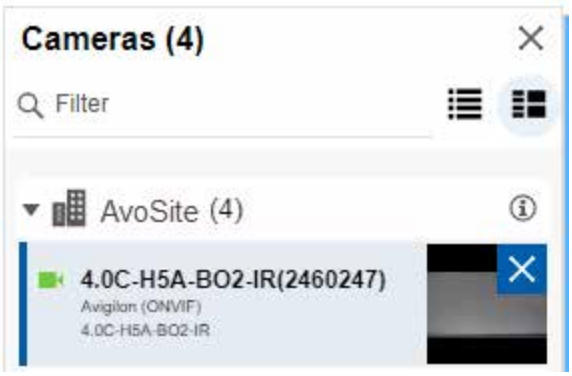
3. While the camera list is displayed, you can continue to select image panels and then select cameras to add to those panels.

Removing a Camera from a View

If a camera requires maintenance or you no longer need to see its video, you can remove the camera from an image panel.

1. Select an image panel, and then click .

   The camera list is displayed, and the selected image panel is outlined in blue.



2. Next to the selected camera, click **X**.

   The camera is removed from the image panel.

Saving a View

> **Note:** Views are unique to each user and are not shared between users. Changes will not appear in the ACC site.

Save views for each area in your site so you can monitor your site effectively. When a view is saved, it will appear in the

Views drop-down list so you can access it later.

1. In the Views page, update or create a new view.
   Set up the view to use the cameras and layout required.
2. *Optional*. Set the view as a favorite or the default view.
3. In the top-right corner, click .
   The Save View dialog box is displayed.
4. Enter a descriptive **Name** for the view.
5. Click **Save**.
   The view is saved.

Opening a View

Note: Up to 9 cameras from a Saved View will be displayed. Other content, like maps or point-of-sale (POS) transactions will not be displayed.

- In the Views drop-down list, select a view. Search for a view by typing.
  - Indicates the view is a favorite.
  - Indicates the view is saved to your Avigilon Cloud Services platform user account.

To expand your view to the full browser width, in the top-right corner click .

To return to the Views page, click .

To use one timeline to control all video feeds in a View, in the top-right corner, click to sync video.

Updating a View

Note: Views are unique to each user and are not shared between users. Changes will not appear in the ACC site.

If you make a change to a previously saved view, you can overwrite the view with your changes, or save your changes as a new view.

- In the top-right corner, click .
  The Save View dialog box is displayed.

To overwrite changes:

1. Select the **Replace** option.
2. Click **Save**.

To save as a new view:

1. Select the **Save as** option.
2. Enter a descriptive **Name** for the view.
3. Click **Save**.

Favoriting a View

> **Note:** To favorite a Saved View, first save the view to your Avigilon Cloud Services account.

If you have a lot of saved views, it can be difficult to find the view you're looking for. You can choose to make a view your default view. Default views are displayed every time you go to the Views page. You can also favorite a view for quick access in the Views drop-down list.

To make a view the default:

- In the top-right corner, click ••• and select **Set as default**.

  The view appears at the top of the Views drop-down list.

To favorite a view:

- In the top-right corner, click ••• and select **Add favorite**.

  The view appears at the top of the Views drop-down list.

Camera List

The camera list displays all of the cameras that you can view from all of the sites you have access to. The camera list provides information about the cameras that are connected and options for displaying the list of cameras.

To show or hide the camera list:

- In the top-left corner, click .

Camera List Item	Description
Cameras heading	The number in parentheses indicates the number of cameras available to view. In the example above there are 10 cameras available.
Filter	Filter cameras by name.

Camera List Item	Description
	Switch to a compact list of cameras that does not include camera details or thumbnail images. **Tip:** You can hover your mouse over a camera name to display a snapshot of the video.
	Switch to a thumbnail list of cameras that displays camera details and a thumbnail image.
 (Site name)	The name of the site that the cameras are connected to. • The number in parentheses indicates the number of cameras available from that site. • Click  to view the site details. • Click ˅ or ^ to expand or collapse the list of cameras for a site.
 (Folder name)	The name of the folder that contains cameras. For ACC sites only.
 (Camera name)	Indicates the camera has live video that can be viewed.
 (Camera name)	Indicates the camera has recorded video that can be viewed but no live video. Use the timeline controls to find the recorded video for these cameras.
 (Camera name)	Indicates the camera has been removed from the site and video is no longer available.
 (Camera name)	Indicates the camera is not connected and video is no longer available.

Licenses

Viewing ACC License Information

Administrators can view a summary of all ACC software licenses that were purchased and used in a customer organization. The types of licenses may include temporary licenses, such as trials, demos, 30-day licenses and 180-day licenses; and annual recurring licenses, such as 1-year to 5-year Smart Assurance Plan licenses.

1. On the  Organization Management page, click the **Licenses** tab.

   The License Summary is displayed:

Name	Description
Site	The site name.
Cameras	The number of site licenses used for cameras across all servers out of the total available channels on your site. Devices that do not generate video streams do not use camera channels.
Failover	The number of site licenses used for failover across all servers out of the total available channels on your site.
LPR6	The number of site licenses used for license plate recognition (LPR) across all servers out of the total available channels on your site.
Analytics	The number of site licenses used for analytics across all servers out of the total available channels on your site.
POS	The number of site licenses used for point-of-sale (POS) sources across all servers out of the total available channels on your site.
Face	The number of site licenses used for face detection across all servers out of the total available channels on your site.

2. Click a site name.
3. Optional. Type in **Filter** to search for site licenses by activation ID, part number or type of license.

Name	Description
Activation ID	The activation identifier for the site license.
Part Number	The part number for the site license.
Quantity	The number of activated channels.
Type	Demo, Perpetual or Subscription. **Tip:** A reminder is displayed when a license is about to expire or renew. For example, **Demo expires** on **12/31/2021** or **Subscription requires renewal** on **12/31/2021**. A perpetual license never expires.
Expiry	The date of license expiration.
Version	The ACC software version.

4. For Avigilon Hardened OS appliances (AI NVR, ENVR, AIA part numbers), click the **Built-In Server Licenses** row or ⌄ on the right.

5. Optional. Type in **Filter** to search for server licenses by server name.

   Built-In Server Licenses is displayed:

Name	Description
Server	The server name.
Cameras	The number of server licenses used for cameras on the server out of the total available channels.
Failover	The number of server licenses used for failover on the server out of the total available channels.
LPR6	The number of server licenses used for license plate recognition (LPR) on the server out of the total available channels.
Analytics	The number of server licenses used for analytics on the server out of the total available channels.
POS	The number of server licenses used for point-of-sale (POS) sources on the server out of the total available channels.
Face	The number of server licenses used for face detection on the server out of the total available channels.

COVID-19 Dashboard

The Avigilon Cloud Services Reports page displays data from configured ACC events across an organization, site or area over a specified time range. For more information, see the **Avigilon COVID-19 Response Technology guide**.

Avigilon Cloud Services Administrators or Managers can access the Reports page to gain business insights and access the **Entry Control Screen**.

Viewing the COVID-19 Dashboard

1. Click **Reports**.
2. Select a site to view information on a per-site level.
3. Select an area to view information on a per-area level.
4. Select a camera to view information on a per-camera level. You can drill down for more event information.

> **Tip:** Select a card to view more details.

Changing the Time Range

The default time range is the last 60 minutes.

- In the top-left, select a new **Time Range**.

> **Note:** The system remembers your new setting until you log out or fresh the page.

Downloading a Report

You can print a chart you are viewing to a PDF formatted report The chart allows you to view data across a site, area, or camera over the specified time range.

You can also export the summarized data points from the chart you are viewing into a CSV file. The data is summarized into 5 minute, one hour or daily totals depending on the time range used for the chart.

PDF Reports

1. Select the site, area or camera. Update the Time Range if needed.
2. Select a card and in the top-right of the table that appears, click **Print**.
3. In the Print dialog, select **Save as PDF** and click **Save**.
4. Select where to save the file.

   A PDF report is downloaded.

> **Tip:** You can also use the browser print settings to save a PDF report. Press Ctrl+P on Windows or Command-P on Mac.

CSV Reports

1. Select the site, area or camera. Update the Time Range if needed.
2. Select a card and in the top-right of the table that appears, click **CSV**.

   A CSV report is downloaded.

Card Details

Name	Description
Current Occupancy	The number of people in an occupancy area in an organization, site or area at this time.

Name	Description
Peak Occupancy Trend	The greatest number of people in the area at a time over the selected time range. It is not the total number of people in an area at a time. For example, the total number of people in the area over an hour was 20. But if for 20 minutes there were 12 people then for 20 minutes there were 8 people and then for 20 minutes there were no people, the peak occupancy would be 12.
Entries and Exits	The total number of people who entered or left an occupancy area over the selected time range. The Event Trend chart shows the number of events that occurred over time.
People Without Mask	The number of detected people without masks in an organization or site over the selected time range. The Event Trend chart shows the number of events that occurred over time.
Social Distancing Violations	The number of detected social distance violations between two people over the selected time range. The Event Trend chart shows the number of events that occurred over time.
Elevated Temperature percentage or Elevated Temperature Events	The percentage of temperature events that are elevated. To get the Elevated Temperature percentage details, you must have configured all 3 temperature events: Elevated, Low, and Expected. If only the elevated temperature event is configured, only the Event Trend chart will display on this card. The Event Trend chart shows the number of events that occurred over time.
Events	The number of events detected by the specified camera over the selected time range. Only displayed when viewing camera details.

Configuring the Occupancy Settings

Specify the maximum occupancy for a site or area to ensure that the Entry Control Screen displays up-to-date data.

1. On the **Reports** page, select a site or area.
2. In the top-right corner, click , then click **Settings**.
3. Enter the **Maximum Occupancy**.
4. *Sites only*. Enter when the occupancy should reset to 0 in the **Reset occupancy daily at** box.
5. Click **Save**.

Tip: You can set different maximum occupancies for each area and for the site as a whole.

Updating the Occupancy with Manual Counts

You can manually update the current occupancy if a person enters or exits and from an entrance that is not monitored. This can also be used by a greeter at the door to update the current occupancy inside the site.

1. On the **Reports** page, select a site or area.
2. In the top-right corner, select and update the current occupancy:
   -  — *Areas only.* Enter a number to decrease or increase the current occupancy.
   -  — Set the current occupancy to 0.
   -  — Set the current occupancy to the maximum occupancy.

   The current occupancy is automatically updated.

Tip: To reset the current occupancy daily, see *Configuring the Occupancy Settings* on the previous page.

Displaying the Entry Control Screen

The Entry Control Screen can be displayed on a monitor or tablet at an entrance to let visitors know the current occupancy.

The Entry Control Screen can be displayed on a device that is signed in to an Avigilon Cloud Services account or a URL can be generated and used on devices that are not authenticated with Avigilon Cloud Services.

1. On the **Reports** page, select an area.
2. In the top-right corner, click , then click **Settings**.
3. Click **Regenerate Auth Key** to ensure the correct access URL and authentication key is generated. An access URL must be generated at least once to enable theEntry Control Screen.
4. To display the Entry Control Screen on a device that is signed in to an Avigilon Cloud Services account:

a. Click **Save**. The COVID-19 Dashboard displays.

b. In the top-right corner, click **Entry Control Screen**.

The Entry Control Screen will load in a new tab.

5. To display the Entry Control Screen on a device that is not authenticated with Avigilon Cloud Services:

a. Copy the **Access URL** to your clipboard so you can send it to the device that needs to display the Entry Control Screen.

b. At the site, enter the copied URL into your web address bar to open the Entry Control Screen.

c. Click **Save**.

Tip: Secure the monitor or tablet to prevent people from interacting with the display.

Changing the Entry Control Screen Messages

You can customize the messages that are displayed when the occupancy is full or when there is still room for people to enter.

1. On the **Reports** page, select a site.
2. In the top-right corner, click , then click **Settings**.
3. Enter the following:
   - **Valid entry heading** — The text displayed if only one person is allowed to enter. The number 1 will be displayed in front of this text. Maximum 22 characters.
   - **Valid entry heading (plural)** — The text displayed if multiple people are allowed to enter. The number of people allowed to enter will be displayed in front of this text. Maximum 22 characters.
   - **Invalid entry heading** — The text displayed if the maximum occupancy is reached. Maximum 22 characters.
   - **Invalid entry subheading** — Additional text to display if the maximum occupancy is reached. You can use this to advise social distance guidelines. Maximum 23 characters.
   - **Maximum occupancy status** — The text displayed when the maximum occupancy is reached. Maximum 7 characters.
4. Click **Save**.

Hiding an Area

If you have an area that is no longer used, you can hide the area to exclude any analytic events from the site total.

1. On the **Reports** page, select a site and then an area.
2. In the top-right corner, click .
3. Click **Hide Area**.

Showing an Area

You can view previously hidden areas and reactivate them.

1. On the **Reports** page, select a site.
2. In the top-right corner, click .
3. Click **Show hidden areas**.

To reactivate a hidden area:

- Click **Set Active**.

Viewing Events

You can get a list of events detected by each camera and view the recorded video linked to the event.

1. On the Reports page, select a site, then a camera.

   For Enter or Exit Area events, select the **Occupancy Area** and then select a camera.

   For Face Mask Detection & Social Distancing Events & Temperature Events, scroll down to the list of cameras in the section for **Face Mask Detection & Social Distancing Events & Temperature Events** and then select a camera.
2. Select a **Time Range** and **Event Types** to display.
3. To review video of an event, click the date and time of the event in the **Start Time** column to open the event clip in the video player.

   You must have the **View recorded images** group privilege for the camera in the ACC system, otherwise video will not stream.

   Use the timeline and player controls to review the video.

Event Details

Name	Description
Start Time	When the event was triggered. Click to view the event video.
Event	The type of event.
Direction	The direction of an Enter or Exit occupancy area event.
Temperature	The temperature reading of the person that triggered the event. This Event detail is only available for Temperature events.
Number of People	The number of people detected in the event.
Source	Whether the event was detected by a camera or manually entered.

Sites

Adding a Site

Administrators can add ACC sites to their organization.

1. On the Organization Management page, in the Sites tab, click **Add site**.
2. Enter the site name, address, and select a Primary Contact who will receive email notifications about the site.
3. Click **Add**. A code is displayed.

   Note: Administrators can get a new code for sites with an expired activation code. Click the icon next to the Code Expired label to generate a new code.

4. Copy the code and enter it in the ACC Client software:
   a. In the New Task menu , click **Site Setup**.
   b. Click the site name, then click **Avigilon Cloud Services** .
   c. Click **If you have an activation code, click here.**.
   d. Enter the activation code and click **Connect**.

Upgrading ACC Sites

Note: Requires the Advanced System Health Package. See *Preview Features* on page 44 to enable a preview of this package. This feature requires a minimum ACC 7.12 software version be installed on the device.

You can update multiple site services remotely, rather than updating each component at its physical location. You can install or upgrade server software, services and plug-ins, language packs, and camera firmware.

It's recommended that you upgrade the ACC Server first, before upgrading other components.

Note: The ACC Client software can be upgraded before or after the ACC Server, but ACC Clients with older software versions will lose administration features until they are upgraded.

1. In the  System Health Dashboard, select a site to see the list of servers in the site.
2. In the Servers tab, click **Upgrade Site**.

   The button may not be enabled if the site does not have the minimum required ACC version.
3. Select the **Update Component** option and select the required installer for the site from the drop-down list.

   The Add Component option can be selected to add components only after upgrading to the latest ACC Server.
4. Click **Download**.

   After download, an Upgrade button is displayed next to each eligible ACC Server.
5. Click **Upgrade** next to each ACC Server.

If you leave the page before the download completes, it will continue in the background. When you return to the upgrade page, the status may indicate 'retry'.

- Click **retry** once to resume the download.

If an installer takes more than a couple of hours to download:

1. Click **Reset**, then restart the ACC Web Endpoint Service in the Windows Services dialog.
2. After the service restarts, try downloading the installer again.

Adding a Service Package

> **Note:** Your ACC site and ACC Web Endpoint Service must be version 7.10 or later.

Administrators can request monitoring services from an Avigilon Cloud Services Provider for each site. Your service provider will give you a code to enter.

1. On the  Organization Management page > Sites tab, select a site.
2. Select the **Service Packages** tab.
3. In the top-right corner, click **Add service package**.
4. Enter the given code and review that the provider information is correct.
5. Click **Save** to submit the service request.

   Your service provider will need to accept or decline your request. You will be notified by email once this happens.

   If you are changing service providers, your previous provider will be notified that they no longer have access to your site.

Canceling a Pending Request

Before a service provider accepts your service request, you can cancel it.

1. On the  Organization Management page > Sites tab, select a site.
2. On the Service Packages tab, select a service package.
3. Click  .
4. Click **Yes**.

   A notification will be sent to your service provider.

Canceling a Service Package

When you cancel a service package, your service provider will no longer have access to your site or video. If you cancel all service packages, your default service provider will be Avigilon. You cannot cancel service packages provided by Avigilon.

1. On the  Organization Management page > Sites tab, select a site.
2. On the Service Packages tab, select a service package.
3. Click  .
4. Enter the provider name and click **Yes**.

   A cancellation request will be sent to your provider.

   Your service provider will need to accept or decline your request. You will be notified by email once this happens.

Deleting a Site

Remove unused sites to clean up your organization.

1. On the  Organization Management page > Sites tab, click  next to the site you want to remove.
2. Enter the site name and click **Delete** to confirm.

Preview Features

Enjoy free access to preview features for a limited time and **provide feedback** about your experience. After the trial period, an additional service package may be required to continue using each feature. Administrators can enable and disable preview features for all sites in their organization.

1. On the  Organization Management page, click the **Preview Features** tab.
2. Select **On** or **Off** to enable or disable a feature.
3. Click **Save** to confirm your changes.

System Health

Note: System Health is only available for registered organizations.

Administrators and Managers can view the status of servers and cameras on the System Health Dashboard.

1. Click  **System Health** to view the dashboard.

   The dashboard summarizes the number of server or camera issues per ACC site.
2. Use the top navigation or click a site to view a summary of the device status. For more information, see *Site Details* below.
3. Click a server or camera to see more detailed information. For more information, see *Server Details* on the next page and *Camera Details* on page 49.
4. In the top-left, click ← to return to the previous page.

List View and Card View

Display the Sites page as a list or as cards.

- In the top-right, click ☰ for list view or ⠿ for card view.

Sorting and Filtering Sites

- Use the drop-down list on the right to sort Site results by Name, Number of issues, Servers with issues, Cameras with issues, or Number of devices.
- Begin typing in the Filter to search for a site.

Sorting and Filtering Devices

- Click a column heading to sort Server and Camera results.
- Begin typing in the Filter to search for results by Device Name, Status, Organization, or IP address.

Site Details

Select the Servers or Cameras tab to view the following information, or select a site on the Sites tab to view only devices from that site.

Name	Description
Device	The device name.
Status	The device connection status.

Name	Description
Status duration	The amount of time the device has been in its current status.
Site	The site the device is connected to.
IP address	The device IP address.
MAC address	The device MAC address.

Server Details

Select a server to view its details. If a status is not available, the system will display Unknown.

There are two tabs:

- **Details** — summarizes the server configuration and status.
- **Storage Analysis** — summarizes the number of days of recording and bandwidth used for each camera.

General Information

Name	Description
Status	The server connection status.
Up Time	The amount of time the server has been running since it was last rebooted.
Analytics Service	The ACC Analytics Service status, if installed.
Model	The server's model name. Only available if the server's SNMP service is enabled.
Server Version	The ACC Server version.
Service Tag	The server's service tag. Only available if the server's SNMP service is enabled.
IP Address	The server IP address.
System Available Memory	The amount of storage available for video recording.
Memory Usage	The amount of memory used by the ACC Server software.
CPU Load	The percentage of server processing power that is used by the ACC Server software.
Peak Load (Last 3 Days)	The highest percent usage of the ACC Analytics Service over the last 3 days.

Server Licenses

Name	Description
Camera Channels	The number of server licenses used for cameras on the server out of the total available channels.
Failover	The number of server licenses used for failover on the server out of the total available channels.
LPR6 Channels	The number of server licenses used for license plate recognition (LPR) on the server out of the total available channels.
Analytics	The number of server licenses used for analytics on the server out of the total available channels.
POS Sources	The number of server licenses used for point-of-sale (POS) sources on the server out of the total available channels.
Face Match Channels	The number of server licenses used for face detection on the server out of the total available channels.

Site Licenses

Name	Description
Camera Channels	The number of site licenses used for cameras on the server out of the total available channels. Devices that do not generate video streams do not use camera channels.
Failover	The number of site licenses used for failover on the server out of the total available channels.
LPR6 Channels	The number of site licenses used for license plate recognition (LPR) on the server out of the total available channels.
Analytics	The number of site licenses used for analytics on the server out of the total available channels.
POS Sources	The number of site licenses used for point-of-sale (POS) sources on the server out of the total available channels.
Face Match Channels	The number of site licenses used for face detection on the server out of the total available channels.

Network Adapters

Name	Description
Adapter Name	The name of the network adapter that is connected to the server.
Status	The operational status of the network adapter.

Name	Description
Link Speed	The maximum speed supported by the network adapter based on its network connectivity. Ensure this is at least 1 Gbps for the camera network.
IP Address	The IP address of the network adapter. Appears empty for network adapters that are disconnected.
Incoming	The bandwidth usage of incoming data.
Outgoing	The bandwidth usage of outgoing data. This includes video streaming to the ACC Client software, ACC Virtual Matrix software, and ACC Mobile 3 application.

Hard Drives

Only available if the server's SNMP service is enabled.

Name	Description
Name	The hard drive name.
Status	The drive status.
Product ID	The hard drive product number.
SMART Alert	If there is a Self-Monitoring, Analysis, and Reporting Technology (SMART) Alert for the disk reliability or imminent failure, it will appear in this column.

Power Supplies

Only available if the server's SNMP service is enabled.

Name	Description
Location	The power supply location in the chassis.
Status	The power supply status.
Type	The power supply type.
State Settings	Additional information about the power supply provided by the sensor.

Cooling Devices

Only available if the server's SNMP service is enabled.

Name	Description
Location	The cooling device location in the chassis.
Status	The cooling device status.
Type	The cooling device type.

Name	Description
State Settings	The cooling device state.

Temperature Probes

Only available if the server's SNMP service is enabled.

Name	Description
Location	The temperature probe location in the chassis.
Status	The temperature probe status.
Type	The temperature probe type.
State Settings	The temperature probe state.

Storage Analysis

Name	Description
Camera	The camera name.
Status	The camera connection status.
Model	The camera model number.
Actual Video Retention	The age of the oldest video stored on the server.
Total Bandwidth	The bandwidth used by the camera in Mbps.
Image Rate	The image rate of the camera in fps.

Camera Details

Select a camera to view its details. If a status is not available, the system will display Unknown.

General Information

Name	Description
Model	The camera model number.
Firmware Version	The camera firmware version.
Serial Number	The camera serial number.
Logical ID	The camera logical ID if assigned.
MAC Address	The camera MAC address.
IP Address	The camera IP address.
Device Location	The camera location if assigned.

Image and Compression

Name	Description
Format	The camera streaming format.
Total Bandwidth	The bandwidth used by the camera in Mbps.
Resolution	The camera image resolution.
Image Quality	The image quality setting of the camera. 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.
Image Rate	The image rate setting of the camera in fps. A higher Image Rate results in better video quality but more storage and network bandwidth usage.
Keyframe Interval	The number of frames between each keyframe. At least one keyframe per second is recommended.

HDSM SmartCodec

Name	Description
Enabled	If supported on the camera, whether High Definition Stream Management (HDSM) SmartCodec™ technology is enabled to reduce bandwidth usage.
On Motion	The background image quality when motion is detected. An image quality setting of 1 will produce the highest quality background image but will require the most bandwidth.
Bandwidth Reduction	Low, Medium, High, or Custom level of bandwidth savings.

Audio

If the device does not have a microphone or speaker, or is not ONVIF-compliant, the sytem will display Unknown.

Name	Description
Speaker	Whether a speaker is enabled on the camera.
Microphone	Whether a microphone is enabled on the camera.

Digital I/O

If the device does not have digitial inputs or outputs, or is not ONVIF-compliant, the sytem will display Unknown.

Name	Description
Inputs	Lists the digital input linked to the camera.

Name	Description
Outputs	Lists the digital outputs linked to the camera.

Scheduling Automatic Site Health Reports

Schedules allow administrators and managers to automatically and periodically run site health reports and generate `.csv` files at the time and day defined by the them. The generated site health reports are stored on ACS and can be downloaded on the local client hard drive or shared in the form of a URL.

There are two ways you can view the generated site health reports for recently run schedules:

- Go to the Files page to download the specific files. See *Viewing Downloaded Files* on page 53.
- Go to the System Health page, in the Schedules tab, click **View Files** for a specific schedule from the Recently run table. The Files page with a filtered All Files table shows the generated report for that specific schedule.

> **Note:** Scheduling automatic and periodic generation of site health reports in ACS requires an Advanced System Health Package subscription.

Administrators and Managers can create and manage schedules on the System Health page, in the **Schedules** tab.

Adding a Schedule

You can create as many schedules as needed for your organization. You can also create recurring schedules and specify an expiration time for your schedules.

1. On the System Health page, in the Schedules tab, click **New Schedule**.
2. In the **Name** text box, enter a name for the schedule.
3. In the **Starts** field, select the date and time when users on this schedule will receive notifications.
4. To repeat the schedule, enable the **Repeats** toggle.
    a. From the **Repeats every** drop-down menu, select how often to repeat the action.
    b. To set an expiration time, enable the **Expires** toggle and select the date and time when the schedule will expire.
5. From the **Select action** drop-down menu, select the required action to add to the schedule.
6. From the **Sites** drop-down menu, select the sites to run the action on.
7. Click **Save**.

   The schedule is added.

Editing a Schedule

You can update schedules that have not been run or the ones that are set as recurring.

1. On the  System Health page, go to the Schedules tab.
2. In the **All Schedules** table, find the schedule you want to edit from the list of schedules. You can also filter the list of schedules by entering text in the **Search** field.
3. Click ⋮ at the end of the schedule entry in the table and click **Edit schedule**.
4. Update the schedule information. The **Select action** and **Sites** fields cannot be edited.

   Tip: To discard your changes and start over, click **Cancel**.

5. Click **Save**.

   The schedule is updated.

Deleting a Schedule

If a schedule is no longer needed, you can delete it from the list.

1. On the  System Health page, go to the Schedules tab.
2. In the **All Schedules** table, find the schedule you want to delete from the list of schedules. You can also filter the list of schedules by entering text in the **Search** field.
3. Click ⋮ at the end of the schedule entry in the table and click **Delete schedule**.
4. Click **Delete** in the confirmation dialog.

   The schedule is deleted.

Downloading a Site Health Report

You can download an audit report of the current server and camera inventory for each site. The report will provide device configuration details as well as the current system health status for each device in the site.

1. In the  System Health Dashboard > Sites tab, select a site.
2. In the top-right, click **Download Site Health Report**.

   The report will download as a CSV file to the default download location.

Tip: You can view and download reports created up to 2 weeks ago on the Files page. See *Viewing Downloaded Files* on the next page.

Downloading a System Bug Report

Avigilon Cloud Services allows you to document key system configurations and logs in a single file that can

submitted with your technical support requests to Avigilon Technical Support.

To generate a System Bug Report that contains configuration data, system logs and more for your servers:

1. In the  System Health Dashboard > Servers tab, select a server.
2. In the upper-right corner of the Details tab, click **Generate System Bug Report** and wait a few minutes for the file to be generated.
3. When the button changes to **Download System Bug Report**, click it and then the upper-right corner of your browser to specify that the zip file be downloaded to your browser's Downloads folder.

   After the file is downloaded, .**Generate System Bug Report** reappears.

> **Tip:** You don't have to wait for the log to finish generating. You can check the availability of the report on the Files page. See *Viewing Downloaded Files* below. It will remain archived for up to 2 weeks.

Viewing Downloaded Files

You can view Site Health and System Bug Reports that were generated and downloaded up to 2 weeks ago on the Files page. You can edit the report name and description, download the reports again or share a direct download link with others.

On the  Files page:

- To download a report, click  .
- To copy a direct download link, click > **Share**.
- To delete a report, click > **Remove**.
- To filter reports, click  in **All Files** and use the advanced search options to narrow down the list of reports. Search for files by site name, server name, file type, date generated or description text. Partial matches are displayed.
- To review the details about a generated file, click the file name in the **All Files** list. The **Details** panel slides out from the top-right corner. In the panel, you can edit the file name or provide description text. Your entries are saved automatically.

Disabling System Health

By default, System Health is available for all registered organizations.

To disable the collection of system health data, contact Avigilon Technical Support.

Notifications

ACC Health events are categorized as Health Notifications in ACS.
ACC events, such as analytic or motion detection events, that have been configured as alarms in the ACC

software are categorized as security notifications in ACS. See your ACC documentation for more information on configuring alarms.

Reviewing Notifications

Administrators, Managers, and Responders can review and resolve notifications for sites they have access to from their browser in the Notifications page. You can view the full event recording.

Viewing a Notification

You can view a notification from the Notifications page. If you have the type of notification enabled on your user account page, you can view Health, Security, or All notifications.

> **Note:** Users must have a schedule selected from the Health Notifications and Security Notifications drop-down lists on their account page in order to view those notifications. These schedules set when the user will be able to receive that notification type for that site. For more information, see *Updating a User's Schedule* on page 71.

- Click a notification.

  > **Tip:** You can filter notifications to find specific events. For more information, see *Filtering Notifications* on the next page.

  The notification details are displayed.

  Use the timeline to view the video.

  To view the previous or next notification, in the top-right corner click or .

Downloading Event Video

If a notification shows an unusual event, you can download the video in MP4 format for investigation and archiving from your browser. You can download up to 60 minutes of the full event video.

To download recorded video:

1. In the video player, click  .

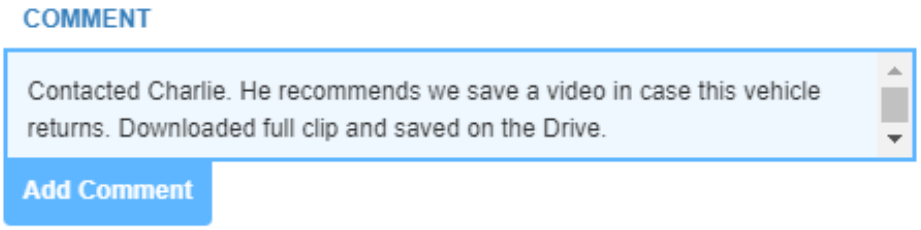
   The Download video dialog box is displayed.
2. Using the camera's local time, select the date and start time.
3. In the **Duration:** box, enter how long the video should be. The maximum duration is 60 minutes.
4. Set the Quality to **High** to download a high resolution clip or **Low** to download a low resolution clip.
5. Click **Submit**.

Adding a Comment

You can leave a comment to report if an action was taken or if the issue was resolved. The comment can be

up to 256 characters.

1. In the **Comment** box, enter a description.



2. Click **Add Comment**.

   The comment appears in the Activity Log.

Resolving a Notification

Once a notification is resolved, you can mark it as reviewed. Reviewed notifications can be filtered from the Notifications to help other users focus on unreviewed notifications.

You can also mark a notification as a false analytic detection. False detections should still be marked as reviewed, so they do not clutter the Notification Table. If you have many false detections, you may need to adjust your analytic rules for your ACC site.

To mark a false detection:

- Next to False Detection?, select **Yes**.

To mark the notification as reviewed:

- Next to Reviewed?, select **Yes**.

Filtering Notifications

You can filter notifications by status, site, device, event type, and date. The Notifications will show results only for the filtered criteria.

> **Note:** You will only see notifications from sites you have access to, during the schedule specified by your Administrator.

To clear a filter, click ✕ .

To clear all applied filters, click **Clear**.

Calling a Contact

If an event requires escalation and you are not at the physical site, you can call a site Contact from a phone

app on your computer. Examples of contacts include local police, emergency services, or site managers.

For example, if you spot an intruder while on-the-go, you can contact both the police and alert your site manager from the Avigilon Cloud Services app, without having to scroll through your phone's contact list.

Contacts are configured by Administrators in the browser application.

You can call a Contact while viewing a notification.

1. At the top of a notification, click  .

   A list of Contacts is displayed.
2. Click the number you want to call.
3. Select an app from your computer.

   The call is sent.

Blocking Notifications

To block notifications from a camera, you can disarm it. This is useful if you know maintenance work will be done in an area with analytic rules and do not want to receive security notifications during that time. You can disarm a camera while viewing a notification.

In a notification:

1. Click  .
2. Select how long you want to disarm the camera, then click **Save**.

   The camera is disarmed.

Resuming Notifications

To resume notifications from a disarmed camera, you can rearm it.

In a notification:

1. Click  .
2. Click **Rearm**.

   The camera is armed.

Email Notifications

The Avigilon Cloud Services platform can send an email notification each time a security or health notification occurs, so you can keep up with site activity while you're away. Security notifications may include a link to a clip of the event that you can view while on the go.

> **Note:** You will only receive notifications based on your Health Notifications and Security Notifications schedule for the sites you have access to.

You can change whether you receive email notifications on your profile page.

1. In the top-right corner, click your name.
2. Click **Profile settings**.

   The Profile page is displayed.
3. Select whether you receive **Enable email notifications for events**.

   > **Tip:** Enabling and disabling email notifications will only affect the email notifications for the organization you are currently connected to. This gives you more control over which organizations your receive email notifications from. If you have more than one organization you want to change this setting on, you will have to connect to each organization and update the setting.
4. Click **Save**.

Health Notifications

Health notifications are health events that are sent from an Avigilon Control Center site or a camera. These notifications let you know if there was a communication or connection error. See your ACC documentation for more information on the types of health notifications that can be sent.

Health notifications appear in the Notification Center in your browser. You can review health notifications the same way you review notifications triggered by an analytic rule. For more information, see *Reviewing Notifications* on page 54.

Administrators, Managers, and Responders can view health notifications for sites they have access to. Dealers can also proactively monitor their subscribers' health notifications if health monitoring is enabled.

Avigilon Control Center Device Notifications

The following table describes the Avigilon Control Center device health notifications and how you can solve them.

Health Notification	Description	Troubleshooting
Analytics Server Connection Lost	Connection to analytics server has been lost.	Contact your Dealer.
Analytics Server Queue Full	The analytics server queue is full.	Contact your Dealer.
Device Disconnect	The Avigilon Control Center device lost connection to your network.	Sometimes the device reconnects automatically. If the connection is not restored, try restarting the device.
Device Reconnect	The Avigilon Control Center device reconnected to your network.	No workaround required.

Health Notification	Description	Troubleshooting
Application Server Stop	The Avigilon Control Center device application is shutting down.	You may receive this notification if you restart your device from your browser or mobile device. If you did not restart your device, contact your Dealer.
Application Bad Shutdown	The Avigilon Control Center device application ended unexpectedly.	Contact your Dealer.
System Low Resources	The Avigilon Control Center device's memory resources are low.	Contact your Dealer.
Db Lost	The database on the Avigilon Control Center device was corrupted.	Contact Avigilon Support.
Db Environment Deleted	The database on the Avigilon Control Center device experienced a critical error. The database environment was recreated.	Contact Avigilon Support.
Db Environment Deleted With Dbs	The database on the Avigilon Control Center device experienced a critical error. The database environment was recreated and some data may have been lost.	Contact Avigilon Support.
Db Environment Recovered	The database on the Avigilon Control Center device experienced a critical error. The database environment was successfully recovered.	Contact Avigilon Support to determine why the error occurred.
Db Reindex	The database on the Avigilon Control Center device was reindexed.	Contact Avigilon Support.
Storage Init Error	The primary data volume on the Avigilon Control Center device failed to initialize.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.
Storage Volume Failed	The data volume on the Avigilon Control Center device is missing or cannot be found.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.
Storage Volume Restored	The data volume on the Avigilon Control Center device was restored to its normal state.	No workaround required.

Health Notification	Description	Troubleshooting
Storage Low Disk Space	The data volume on the Avigilon Control Center device was reduced to 50% of its target size due to low disk space.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.
Storage Write Queue Full	Data for a device was dropped due to storage system performance, insufficient system resources, or invalid camera stream on the Avigilon Control Center device.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.
Storage Write Failed	A device connected to the Avigilon Control Center device failed to write data to the data volume.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.
Storage Writes Blocked	A device connected to the Avigilon Control Center device was blocked from writing data to the data volume.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.
System Cluster Network Failure Detected	A network issue was detected between this Avigilon Control Center device and another Avigilon Control Center device. Your site may experience poor performance.	Contact your Dealer to replace your Avigilon Control Center device. Export video if possible.

Camera Notifications

The following table describes the camera health notifications and how you can solve them.

Health Notification	Description	Troubleshooting
Camera Connected	A camera connected to the Avigilon Control Center device.	No workaround required.
Camera Disconnected	A camera disconnected from the Avigilon Control Center device.	If the camera comes back online, the system will automatically resolve this issue. If the camera does not come back online, check your camera and network settings.
Camera Tampering	A camera detected sudden changes to the scene.	Check the live video to see if you need to readjust the camera placement or focus.

Health Notification	Description	Troubleshooting
Device Communication Lost	A camera disconnected from the Avigilon Control Center device.	This may be due to a loose Ethernet connection. Reconnect the device cables and the system will automatically resolve the event.
Device Connection Error	A camera connection failed. Device data cannot be received.	Check your camera and network settings.
Device Packets Lost	A camera experienced network packet loss (more than 50% of packets were lost over the last 60 seconds).	Contact your IT department. If the camera is connected to the Camera Uplink Port, contact your Dealer.
Device Packets Recovered	A camera no longer experiences network packet loss.	No workaround required.
Server Firmware Upgrade Started	The camera firmware upgrade started.	No workaround required.
Camera Firmware Upgrade Complete	The camera firmware upgraded.	No workaround required.
Server Firmware Upgrade Error	An error occurred during a firmware upgrade.	Contact your Dealer.
Device Record Interrupted	A camera's recording was interrupted.	Check your camera and network settings.
Device Record Restored	A camera's recording was resumed.	No workaround required.

Security Notifications

Security notifications are any ACC events that are configured as alarms in the ACC software. These could be analytic events, motion detection events, or any other type of ACC events. The event must be configured to trigger an ACC alarm in order to receive an ACS security notification. These notifications let you know that there was an event triggering an alarm at your ACC site. See your ACC documentation for more information on the types of events that can be used and how to configure them to trigger an alarm.

Security notifications appear in the Notification Center in your browser. You can review security notifications the same way you review other notifications. For more information, see *Reviewing Notifications* on page 54.

Administrators, Managers, and Responders can view security notifications for sites they have access to if they have the security notification privilege.

Notification Center

Administrators, Managers, and Responders can view the Notification Center, but will only see notifications for

the sites that they have access to based on their health and security notification schedules. Administrators can update your site access and notification schedule.

To view the Notifications, click  .

Notification List

A summary of recent notifications. Filter notifications using the toolbar at the top of the page. For more information, see *Filtering Notifications* on page 55.

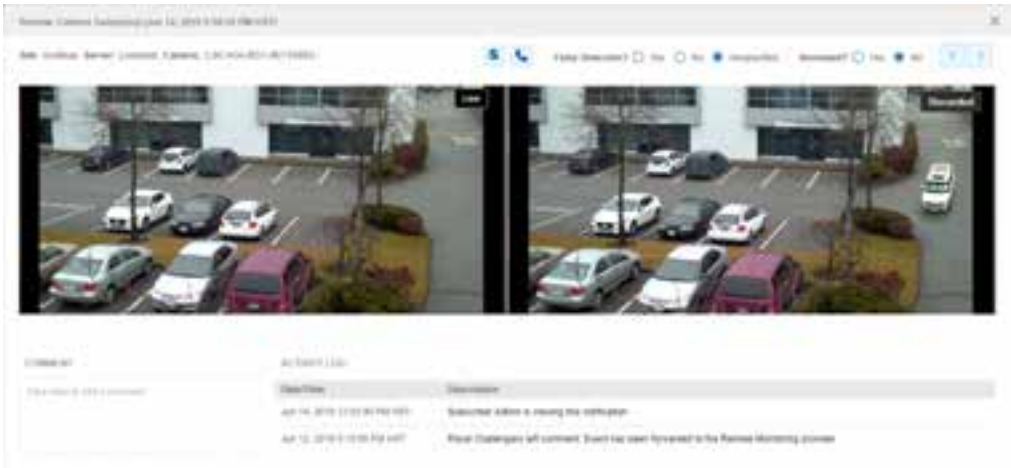
Click a notification to view more details. See *Reviewing Notifications* on page 54.

The following table describes the columns in the notifications list.

Column	Description
Status	The following notification status icons appear next to each notification.  — An unreviewed Device Health notification. For more information, see *Health Notifications* on page 57.  — An unreviewed notification.  — A notification currently under review.  — A notification marked as reviewed.
Date/Time	When the notification occurred.
Event Description	The name of the analytic rule that triggered the notification.
Site	The site where the notification occurred.
Device	The camera or Avigilon server that recorded the notification.
Last Viewed By	The last user to view the notification details.
Last Updated	The last time the notification details were updated.

Notification Details

Click a notification to view more information.



You can view if others have commented or viewed the notification in the Activity Log. The Activity Log also captures whether the notification was marked as a false detection or if it was previously marked as reviewed. Other users in your Avigilon Cloud Services platform site can see your activity from their browser or mobile device.

Notification Issues

Can't See Your Notifications?

You may see fewer notifications listed in the Notification Table than events in the Notification Chart. This is because the chart displays all events that occurred, while the table displays only notifications you're assigned based on your schedule, site access, and filters.

To troubleshoot:

- Clear all filters.
- Have an Administrator or Manager check that your site and cameras are connected and working. Ensure that your analytic rules were added properly.
- If there are still no notifications on the Notifications page, your user account may not be set up to receive notifications for that site at that time.

  An Administrator can update your user account to ensure that the correct user role, site, and schedule were selected.

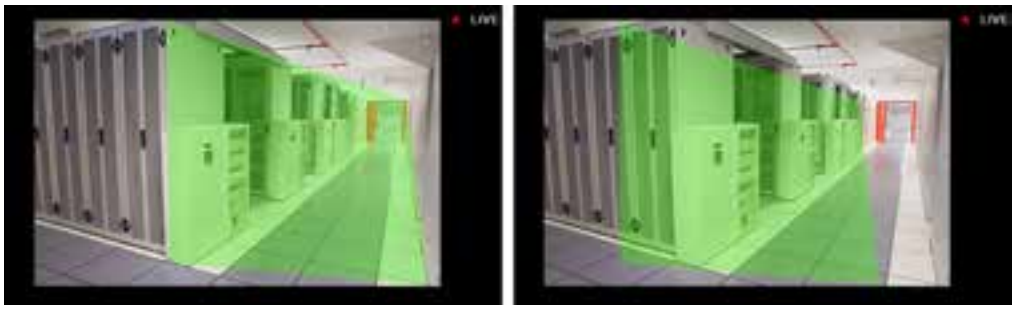
  Once your user account is updated, you will begin receiving notifications. Note that you will not see any notifications prior to the update.
- If your problem is not solved, contact Avigilon Support at +1.888.281.5182 Option 1, then Option 5.

Too Many Notifications?

If you're receiving too many notifications, you may need to adjust your analytic rules. For more information see your ACC documentation.

Too Many False Alarms?

If you're receiving too many false alarms, your analytic rules' region of interest may be misaligned. This can happen if the camera is moved after configuration.



If the overlay is not aligned properly, an Administrator or Manager can configure the camera's analytic rule.

Users

User Roles

Avigilon Cloud Services has four user roles: Administrators, Managers, Responders, and Viewers. Each role has access to different features. A user's role applies to all sites that they have access to.

	Administrator	Manager	Responder	Viewer
Monitor Video	✓	✓	✓	✓
Manage Bookmarks	✓	✓	✓	✓
Receive and Respond to Notifications	✓	✓	✓	—
View System Health	✓	✓	—	—
Manage Sites and Users	✓	—	—	—

Tip: It is recommended that you have at least two active users with an Administrator role in your organization at all times.

Primary Administrator

Every organization has a primary administrator who is notified of changes to the organization. The user that created the organization is the primary administrator by default, but another administrator in the organization can be made a primary administrator.

To change the current primary administrator to another administrator:

1. On the  Organization Management page, navigate to the General tab.
2. From the Primary Administrator drop-down list, select a different administrator.

   If you do not have any other users with the Administrator role, no users will show up in the drop-down list.
3. Click **Save**.

Support User

Every organization has a Support user identified by the `support@avigilon.com` email. This System Administrator user cannot be deleted but you can change whether they have access to sites or what sites they have access to. By default, the Support user does not have either the ability to login or access to any of your sites. The Support user can be used by Avigilon Support to provide troubleshooting support to cloud users.

An organization administrator can grant the Support user access to sites, however, ACC has the final authority of privileges for the Support user on the ACC Server. When the Support user is granted access to a site from the ACS web client, the ACC Servers in that site will create a user for Avigilon Support. This user cannot be deleted using the ACC Client. The Support user is a member of and has all the privileges of the Cloud Administrator group.

The Support user enables Avigilon Support to access your sites without the organization administrator having to create a new user for that purpose. When on the phone with Avigilon Support, they will ask you to grant the Support user access to a site so that they can help you troubleshoot your issue. An Administrator can grant access to the required sites. If the Support user has appropriate privileges, Avigilon Support can log in to your organization to make a virtual visit with their Avigilon enterprise credentials with 2-factor authentication as the Support user. During the virtual visit the Avigilon Support team member can only access the sites that they have been granted permission to access.

When your support session is done, the privileges and access granted to the Support user can be removed by an Administrator. Removing the Support user's access in ACS automatically removes their access from the corresponding ACC Servers.

Other System Administrator Users

When you add a service package from a dealer or service provider to a site in your organization, it creates and lists System Administrator users in your users table. You cannot directly delete these users. When you accept a service package, you authorize the corresponding System Administrator user to be able to access your site to deliver specific services.

The most common service providers are:

- Avigilon dealers who may provide support, system health, or video monitoring services to one or more of your sites
- Service providers who provide commercial video monitoring services to one or more of your sites
- Local law enforcement entities that you authorize connection to one or more of your sites to allow them access to some of your cameras as part of a public-private partnership

In addition to being a System Administrator user in your organization, this user will be created with the same name on the ACC Server for the site as a member of the Cloud Administrator group. This user cannot directly be deleted from the ACC Client. You cannot remove the user from the Cloud Administrator group, but you

can:

- Modify the privileges granted to that group
- Add the user to one or more other groups

By modifying the privileges of the Cloud Administrator group and adding this user to other groups, you can specify what permissions and devices this user has access to.

If you delete a service package from your site, the corresponding System Administrator user is also removed from the ACC Server of that site. The user remains listed in your ACS organization until all the service packages that they support have been removed.

Adding a User

1. On the  Organization Management page, in the Users tab, click **Add user**.
2. Enter the user's email information.
3. In the **Role** drop-down menu, select the user's role. See *User Roles* on page 101 for a description of each role.
4. Select a site from the **Site Access** and select a schedule for **Security Notifications** and **Health Notifications** for that site.
    - Users can only view video, notifications, and devices for sites they have access to.
    - The schedule determines when the user will receive security and health notifications for that site. If a user does not need to receive security or health notifications, select **Never** for those schedules. For Viewer roles, the schedules will be set to **Never** and cannot be edited.
5. Click **Save**.

    The user will receive an email invitation with a registration link that expires within 24 hours.

When a user clicks the registration link, they will be prompted to create a password. For more information, see *Registering Your User Account* on page 7.

Once the user registers, their status will change from Invited to Enabled.

Syncing ACC and ACS Users

> **Tip:** To simplify access rights and privileges, create and manage users in the ACC Client and sync them to Avigilon Cloud Services.

Users can be created in both the ACC Client and Avigilon Cloud Services and synced from one platform to another.

Users created in Avigilon Cloud Services will not be able to log in to the ACC Client by default. Create users in Avigilon Cloud Services if they are from an external organization and need web and mobile access.

Creating and Syncing ACC Users to the Cloud

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. Click **Add User**.
4. Enter an email address. This will be the username in Avigilon Cloud Services.
5. Select the **Connect** checkbox and click **OK**.

   The user will receive an email invitation with a registration link that expires within 24 hours. If the link expires, an ACC administrator needs to clear and select the **Connect** checkbox again to send a new invitation.

   > **Note:** ACC users that connect to the cloud using the ACC Client are assigned the Viewer role by default. You can edit the user on ACS to assign a different role. For more information, see *User Roles* on page 63.

Creating and Syncing Avigilon Cloud Services Users to an ACC Site

Sync Avigilon Cloud Services users to an ACC site if they need web or mobile access only. Add the user to a new or existing group in the ACC Client to give them access to the cameras they need.

In Avigilon Cloud Services:

1. On the Organization Management page > Users tab, click **Add user**.
2. Enter the user's contact information.
3. Select the user's **Role**. For more information, see *User Roles* on page 63.
4. Select which sites the user can access.
5. Click **Save**.

   The user will receive an email invitation with a registration link that expires within 24 hours. If the link expires, an ACS administrator needs to send the invitation again.

In the ACC Cient:

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. Select the ACS user, then click **Edit User**.
4. In the Member Of tab, select the permission groups that should be applied.
5. Click **OK**.
6. Repeat steps 2 - 5 for each site the user has access to.

Configuring Camera Access for Cloud Users

Synced ACC users have the same access to cameras and privileges as defined in the ACC Client.

Depending on their user role, Avigilon Cloud Services users become members of the following ACC user groups when synced:

- **Cloud Administrators** — Administrators and Managers
- **Cloud Viewers** — Viewers and Responders

By default, both of these user groups have access to all cameras. For increased security, remove access to all cameras for these groups.

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Select a site, then click **Users and Groups** .
3. In the Groups tab, select the Cloud Administrators group and click **Edit Group**.
4. Remove access to all cameras and click **OK**.
5. Repeat steps 3 - 4 for the Cloud Viewers group.

You can then add the ACS users to an existing ACC group with the desired camera access rights.

Resending a Registration Email

If a user does not register within 24 hours, their registration link expires. Administrators can resend an Avigilon Cloud Services invitation.

1. On the Organization Management page > Users tab, select a user.
2. Click **Resend Invite**.

   A new email invitation is sent to the user.

Resetting a User's Password

After 3 failed attempts to sign in, a user will be locked out of their account for 30 minutes. They can click **Forgot my password** on the sign in page, or an administrator can reset it.

1. On the Organization Management page > Users tab, select a user.
2. At the bottom of the page, click **Reset Password**.

   A password reset email is sent to the user.

Updating a User

If a user's information or role changes, you can update the user account.

> **Tip:** Filter users by their name, email address, role or site access.

1. On the Organization Management page > Users tab, select a user.
2. Enter the new information.
3. Click **Save**.

Removing a User

To remove a user from Avigilon Cloud Services, you can delete their account.

1. On the  Organization Management page > Users tab, click  next to the user you want to remove.
2. Click **Delete** to confirm.

   The user is removed from Avigilon Cloud Services and their ACC user account's Connect check box is cleared.

> **Note:** All ACS organizations will have the `support@avigilon.com` user listed in Users table as a System Administrator. You cannot delete this user. This user will not have login or video access to any of your sites by default. However, you can change what sites this user has access to in order to help Avigilon Support troubleshoot an issue.

Schedules

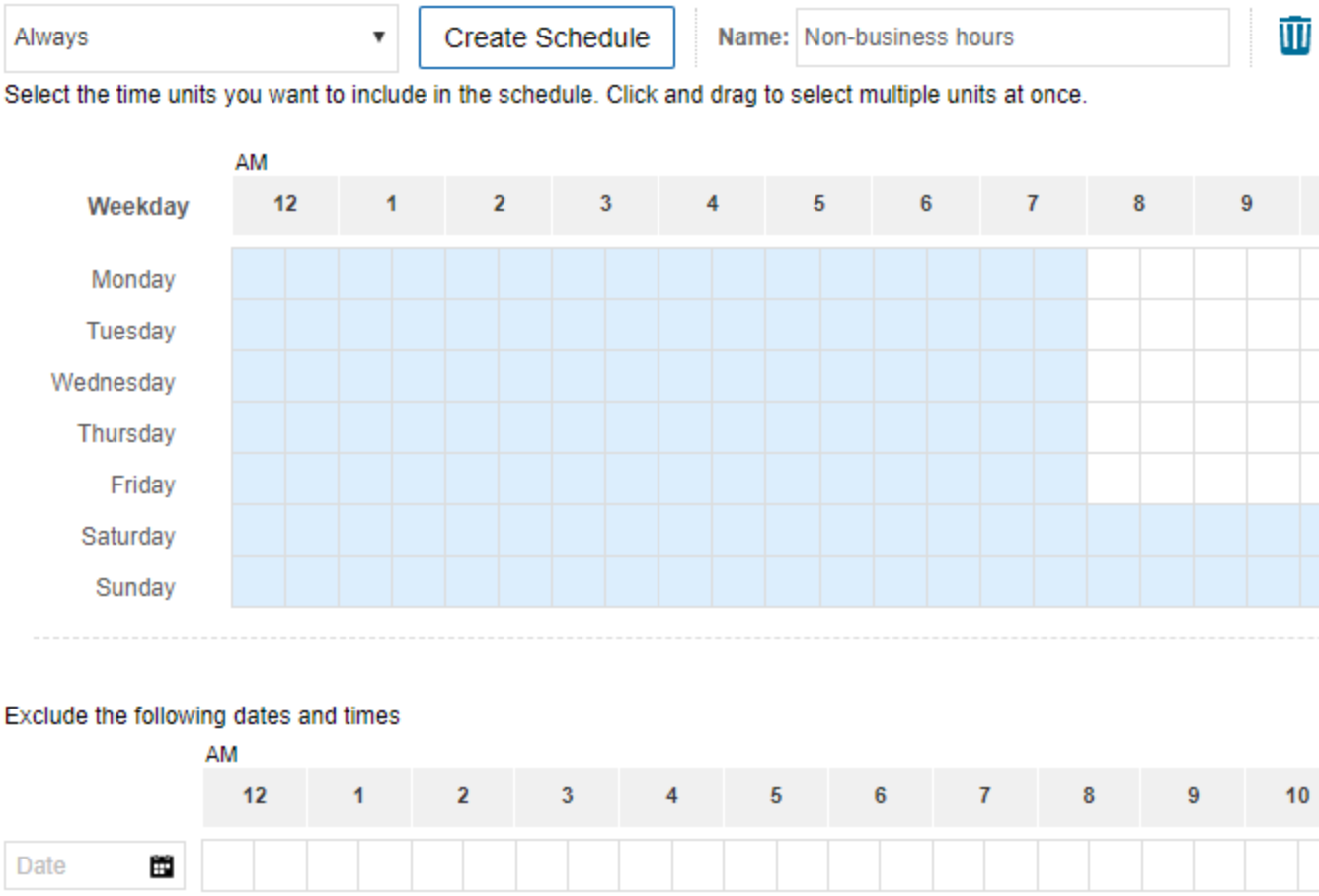
Schedules are a set of days and times throughout the week that determine when a user receives security and health notifications for a site. Schedules are used for Administrators, Managers, and Responders who respond to security and health notifications on their mobile device or in their browser.

There are two default schedules:

- **Always** — The user receives notifications at all times.
- **Never** — The user does not receive notifications.

Use schedules to ensure that users receive notifications during a set time period. You can assign a different security and health notification schedule for each site.

Administrators can create and manage schedules on the  Organization Management page, in the **Schedules** tab. The following example shows a schedule for non-business hours. All hours are selected except 8 - 5 Monday - Friday. Any user with this schedule will only receive notifications for events that occur during the selected times.



Adding a Schedule

You can create as many schedules as needed for your organization. Schedules can be added that exclude certain times like holidays or non-business hours.

1. On the Organization Management page, in the Schedules tab, click **New Schedule**.
2. In the **Name** box, enter a name for the schedule.
3. Select the days and times when users on this schedule will receive notifications. Click and drag the mouse over the calendar to select and clear multiple dates and times.

4. Select dates and times to exclude, like holidays.
    a. Click the **Date** box to open a calendar and select a specific date.
    b. Click or drag the mouse over the times you want to exclude.
    c. To add another date to exclude, click  .
    d. To remove an excluded date, click  .
5. At the bottom of the page, click **Save**.

    The schedule is added and can be assigned to user accounts.

Assigning a Schedule

A user's schedules determine when they receive security and health notifications for each site they have access to. If a user's shift changes, you can update the user's schedules in the **Users** tab. If a user does not need to respond to security or health notifications you can set those schedules to **Never**.

1. On the  Organization Management page, in the Users tab, select a user.
2. Select the sites the user should have access to and select a schedule from the **Security Notifications** and **Health Notifications** drop-down lists. These schedules set when the user will receive security or health notifications for that site.

    Note: The security and health notification schedules can only be selected if your organization has enabled these preview features. Some organizations may only have one type of the notification preview feature enabled. For more information on enabling these features, see *Notifications* on page 53.
3. Click **Save**.

    Tip: To give users access to new sites as they're created, set the **Access to new sites** preference to Yes.

Editing a Schedule

If a shift changes, or if additional dates need to be excluded, you can update schedules as needed. You can also change a schedule's name.

1. On the Organization Management page, in the Schedules tab, select the schedule you want to edit.
2. Update the schedule's information.

   Tip: To discard your changes and start over, click **Cancel**.

3. Click **Save**.

   The schedule is updated.

Updating a User's Schedule

A user's security and health notification schedules determine when they receive security and health notifications from a site. If a user's shift changes, you can update the user's schedules. If a user does not need to respond to notifications you can set their schedule to **Never**. New schedules can be added in the Schedules tab. For more information, see *Schedules* on page 68.

1. On the Organization Management page, in the Users tab, select a user.
2. Select the sites the user should have access to and select a schedule from the **Security Notifications** and **Health Notifications** drop-down lists. These schedules set when the user will receive security or health notifications for that site.

   Note: The security and health notification schedules can only be selected if your organization has enabled these preview features. Some organizations may only have one type of the notification preview feature enabled. For more information on enabling these features, see *Notifications* on page 53.

3. Click **Save**.

   Tip: To give users access to new sites as they're created, set the **Access to new sites** preference to Yes.

Removing a Schedule

If a schedule is no longer needed, you can remove it from the list.

1. On the  Organization Management page, in the Schedules tab, select the schedule you want to remove.
2. Click  .

   A dialog box will ask you to confirm.
3. Click **Delete**.

   The schedule is removed.

Your Profile

Updating Your Profile

You can manage your Avigilon Cloud Services user profile and preferences on the Profile settings page.

You can update your:

- Personal information

  This information is read-only if you logged in using your identity provider credential, such as a Microsoft account.
- Password

  This information is not displayed if you logged in using your identity provider credential.
- Date and number formats

1. In the top-right corner, click your name.
2. Click **Profile settings**.
3. Select a tab and enter the new information.
4. Click **Save**.

Changing Your Password

For increased security, your password automatically expires after 90 days. You'll receive an email reminder 3 days before it expires.

1. In the top-right corner, click your name.
2. Click **Profile settings**.
3. In the Password tab, enter your **Current password**.
4. Enter a **New Password** and **Confirm new password**. Your new password must be different from your last 3 passwords.

   Your password must contain 8-50 characters and include at least one:

- Uppercase letter
- Lowercase letter
- Number
- Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

Your password cannot include the word "Password".

5. Click **Save**.

   A success message will appear.

Changing the Web Client Language

You can change the web client language at any time from any page. You can also select your language when signing in.

> **Tip:** Once you have changed your language, Avigilon Cloud Services will remember your selection and use it every time you sign in to the platform.

- At the bottom of any page, use the **Language** drop-down list to select a language.

  The language is updated.

Changing Your Preferred Language

Avigilon Cloud Services sends emails regarding your account or subscription. The Preferred communication language setting controls the language used in these emails.

1. In the top-right corner, click your name.
2. Click **Profile settings**.
3. In the Personal Information tab, select a **Preferred communication language**.
4. Click **Save**.

Changing Email Notification Preferences

You can choose whether or not to receive email notifications.

1. In the top-right corner, click your name.
2. Click **Profile settings**.
3. In the Personal Information tab, select whether or not to receive **Enable email notifications for events**.
4. Click **Save**.

Changing the Timezone and Date and Number Formats

By default, Avigilon Cloud Services uses your default browser preferences for your timezone, and date and number formats. To personalize your formats:

1. In the top-right corner, click your name.
2. Click **Profile settings**.
3. In the Dates and Numbers tab, select your preferences.
4. Click **Save**.

Restricting Dealer Access

By default, dealers have access to all of their subscriber sites and cameras. This lets dealers view live and recorded video, view and respond to notifications, and configure your devices. If you do not want your dealer to access your sites or cameras, you can restrict their access.

> **Note:** You cannot restrict dealer access to a site with health monitoring or central station monitoring enabled. Request to end health monitoring or central station monitoring services before you restrict the dealer's access.

1. On the  Organization Management page, in the Users tab, select your dealer.

   The User: ${titleText} dialog box is displayed.
2. Clear all the sites you do not want your dealer to access.
3. Click **Save**.

   Your dealer can no longer access those sites.

   If your dealer has other user accounts in your organization, they will still have access according to their site access and user role.

Service Providers

Offer event-based video monitoring services, on-premise or remote guarding services, or camera sharing programs for your customers.

Linking a Customer Organization to Your Partner Organization

As a service provider, you can link a customer organization to your partner organization for customers who have an ACC site connected to Avigilon Cloud Services by offering the *ACC Connect* service package.

Note: The ACC site and ACC Web Endpoint Service must be version 7.10 or later.

1. *For service providers.* On the  Organization Management page > Service Packages tab, copy your **Code** and make it available to the customer to add your service package to one or more of their sites.
2. *For customers of service providers.* The customer administrator uses this code to **make a service request**, which partners can view.
3. *For service providers.* After customers complete the form, you will receive an email notification. Click the link to **Accept** or **Decline** your customer's request for service.

   Tip: You can also go to the  Organization Management > Customer tab and view your Pending Requests.
4. *For service providers.* After the service request is accepted, you will be able to provide services to that site.

Offering Service Packages for Remote Services

As a Service Provider, you can offer value-added service packages to customers who have an ACC site connected to Avigilon Cloud Services. An example of a value-added service package is the *Remote Monitoring* service package for remote video monitoring when events are sent to the provider Central Station.

Note: The ACC site and ACC Web Endpoint Service must be version 7.10 or later.

1. *For service providers.* On the Organization Management page > Service Packages tab, copy your **Code** and make it available to the customer to add your service package to one or more of their sites.
2. *For customers of service providers.* The customer administrator uses this code to **make a service request**, which partners can view.
3. *For service providers.* After customers complete the form, you will receive an email notification. Click the link to **Accept** or **Decline** your customer's request for service.

   > **Tip:** You can also go to the Organization Management > Customer tab and view your Pending Requests.

4. *For service providers.* After the service request is accepted, you will be able to provide services to that site.

Managing Pending Requests

As a Service Provider, you will receive email notifications whenever a customer requests a new service or cancels their subscription. You can accept or decline requests in Avigilon Cloud Services.

To manage a pending request:

- Follow the link in your email and **Accept** or **Decline** the request.
- Go to the Organization Management > Customer tab and **Accept** or **Decline** the request.

  > **Tip:** A circle that is displayed next to the Organization Management > Monitoring tab indicates a reply is needed.

Central Station Monitoring

As a Service Provider, you can enable central station monitoring using a custom webhook integration or SureView Systems Immix® CS software to deliver an end-to-end solution for your customers. Once enabled, the central station can view live and recorded video.

> **Note:** If you have a user account in both the service provider and customer organization, make sure you are signed in as a service provider. You'll know you're signed in as a service provider if you see the organization drop-down list in the top-left area.

Webhooks

Preparing a Webhook Integration

Work with your integrator to determine the following:

- The **URI** that will receive the event message.

  Include the protocol and domain. HTTPS is recommended.

  For example: https://centralstationprovider.com/98c91d60-4a68-4a91-830e-f5aa6a
- A **Username** and **Password** for the webhook integration.
  - The username should be unique, and does not need to be an email address.

    For example: centralstationproviders01
  - Your password must contain 8-50 characters and include at least one:
    - Uppercase letter
    - Lowercase letter
    - Number
    - Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

    Your password cannot include the word "Password".
- A **Shared Secret Phrase** to verify the event message came from Avigilon Cloud Services

  Phrases must have 6 or more characters and can include spaces and punctuation. We recommend using 5-7 words in your phrase.

  For example: Cool cats know where it's at.

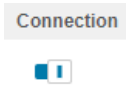
Creating a Webhook Central Station

Once you have the above information, use it to set up central station monitoring. You can set up a single central station to monitor all of your sites or multiple central stations to help organize the different subscribers and sites that will be monitored.

1. Go to **Organization Management** > **Monitoring** > **Central Stations**.
2. On the right side, click **Add Central Station**.
3. Enter a descriptive **Name** for the central station.
4. In the Integration type drop-down list, select **Webhook**.
5. Enter the **URI**, **Username**, **Password**, and **Shared Secret Phrase** determined in the previous step.

6. Click **Save**.

   A success message is displayed and the new central station is added to the list.
7. Click the **Connection** toggle to enable the connection to the central monitoring software.

   A success message is displayed.

Testing the Webhook Connection

- Next to the webhook, click **Test**.

  A sample notification is sent to the URI.

Enabling Site Monitoring

1. In the **Site Configurations** tab, select a subscriber organization to view their sites.

   > **Note:** You will only see sites you have access to.
2. Select the **Central Station** from the drop-down list and select the **Enabled** checkbox on the right.
3. Click **Save**. A success message is displayed.

The webhook is now configured to send notifications whenever an event occurs at the subscriber's site.

Disabling Monitoring

To stop sending notifications to a central monitoring service, disable central station monitoring. You can disable central station monitoring on a per-site basis, or for all subscriber configurations using a single central station.

To disable monitoring for a site:

1. In the Site Configurations section, expand a subscriber organization to view their sites.
2. Next to a site, clear the **Enabled** checkbox.
3. Click **Save** to save your changes.

   A success message is displayed.

To disable monitoring for all sites using a single central station:

- In **Organization Management** > **Monitoring** > **Central Stations**, click the **Connection** toggle for a central station to disable its connection.

  A success message is displayed and central station monitoring is disabled for all subscriber sites that are using that central station.

Partners and Dealers

Register, install and maintain Avigilon security systems for your customers.

If your organization offers other services, see the *Service Providers* on page 75.

For end-user information, see the *Introduction* on page 1.

Getting Started

Registering Your Partner Account

If your organization is offering service packages to customers on Avigilon Cloud Services, register for a partner account.

1. Click the **Partner Organization Request** form (**link**).
2. Fill out the form, including the type of organization.

Avigilon Partner	Register, install and maintain Avigilon security systems for your customers. Your organization must be an Active Official Avigilon Partner.
System Maintenance Services	Offer end-user maintenance services. Your organization is not an Avigilon Partner.
Service Provider	Offer event-based video monitoring services, on-premise or remote guarding services, or camera sharing programs for your customers.

3. When the form is complete, you or the primary administrator will receive a registration email from the Avigilon Cloud Services Team.
    a. In the email, click the registration link. This link is only valid for 24 hours.

    If the link expires, contact *AvigilonCloud Services Support* to resend the link.

    b. Create a password. This password is unique to Avigilon Cloud Services and does not need to match your ACC password.

    Your password must contain 8-50 characters and include at least one:

    - Uppercase letter
    - Lowercase letter
    - Number
    - Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

    Your password cannot include the word "Password".

    If you are a federated user, you are not prompted to set a new password. Avigilon Cloud Services will use your identity provider credential, such as a Microsoft account.

    c. Select your **Preferred communication language**. This sets the language for emails from

Avigilon Cloud Services.

d. Click **Submit**, then click **Sign in** and enter your credentials.

e. Review and accept the End User License Agreement.

Signing In

Note: If an incorrect password is entered three times, the account will be locked for 30 minutes. Click **Forgot my password** to change your password and access your account. This occurs only if you are a non-federated user who is not using an identity provider credential, such as a Microsoft account.

1. Go to **cloud.avigilon.com**.
2. Select the region specified by your administrator.

   After the first time you sign in to a region, you can bookmark the selected region.
3. Enter your email and click **Next**.
4. Enter your password and click **Submit** or **Sign in**.

   You are signed in.

Accessing a Customer Organization

You can view and manage customer sites from your Avigilon Cloud Services account by default. This is useful if you need to remotely support your customer.

You can access subscriber organizations two ways:

- Using the organization drop-down list.
- Changing organizations.

Note: Avigilon recommends using the organization drop-down list rather than the Switch Organization option to switch between customer organizations. Using sites eliminates the need to provision and maintain users in customer organizations.

Using the Organization Drop-Down List

When you use the organization drop-down list, your user role in the customer organization remains the same as your user role in your partner organization. For example, if you are a Responder in your partner organization, you can only act as a Responder, not an Administrator, in the customer organization.

1. In the top-left corner, in the organization drop-down list, begin typing to search for a subscriber.

2. Click the subscriber you want to manage.

   You can now manage the subscriber's site.

To go back to your partner organization:

- In the organization drop-down list, select your partner organization.

Changing Organizations

To change organizations, you must have a user account in the customer organization using the same email address as your partner user.

When you change organizations, your can have a different user role. For example, if you are a Responder in your partner organization, but your user role in a customer organization is an Administrator, you can act as an Administrator in the customer organization.

1. In the top-right corner, click your name. Your account information is displayed.

2. In the Switch Organization menu, select the organization you want to manage.

   Your user account and role is updated.

Signing Out

- In the top-right corner of your browser, click your name and select **Sign Out**.

User Accounts

To access the Avigilon Cloud Service platform, you need a user account. When your organization signs up for an Avigilon Cloud Service partner organization (see *Registering Your Partner Account* on page 79), an Administrator user account is created for the primary contact.

Administrators can create and manage user accounts using the Organization Management page, in the Users tab. From here, you can add accounts for your team.

User Roles

There are four types of user roles: Administrators, Managers, Responders, and Viewers. Each role has access to different Avigilon Cloud Services platform features. A user can have one role that carries across all sites that they have access to. The following table describes the four types of users and the permissions they have.

	Administrator	Manager	Responder	Viewer
Monitor Video	✓	✓	✓	✓
Manage Bookmarks	✓	✓	✓	✓
Receive and Respond to Notifications	✓	✓	✓	—
Manage Cameras and Devices	✓	✓	—	—
Manage Sites and User Accounts	✓	—	—	—

Tip: It is recommended that you have at least two active users with an Administrator role in your organization at all times.

Primary Administrator

Every organization has a primary administrator who is notified of changes to the organization. The user that created the organization is the primary administrator by default, but another administrator in the organization can be made a primary administrator.

To change the current primary administrator to another administrator:

1. On the  Organization Management page, navigate to the General tab.
2. From the Primary Administrator drop-down list, select a different administrator.

   If you do not have any other users with the Administrator role, no users will show up in the drop-down list.
3. Click **Save**.

Support User

Every organization has a Support user identified by the `support@avigilon.com` email. This System Administrator user cannot be deleted but you can change whether they have access to sites or what sites they have access to. By default, the Support user does not have either the ability to login or access to any of your sites. The Support user can be used by Avigilon Support to provide troubleshooting support to cloud users.

An organization administrator can grant the Support user access to sites, however, ACC has the final authority of privileges for the Support user on the ACC Server. When the Support user is granted access to a site from the ACS web client, the ACC Servers in that site will create a user for Avigilon Support. This user cannot be deleted using the ACC Client. The Support user is a member of and has all the privileges of the Cloud Administrator group.

The Support user enables Avigilon Support to access your sites without the organization administrator having to create a new user for that purpose. When on the phone with Avigilon Support, they will ask you to grant the Support user access to a site so that they can help you troubleshoot your issue. An Administrator can grant access to the required sites. If the Support user has appropriate privileges, Avigilon Support can log in to your organization to make a virtual visit with their Avigilon enterprise credentials with 2-factor authentication as the Support user. During the virtual visit the Avigilon Support team member can only access the sites that they have been granted permission to access.

When your support session is done, the privileges and access granted to the Support user can be removed by an Administrator. Removing the Support user's access in ACS automatically removes their access from the corresponding ACC Servers.

Other System Administrator Users

When you add a service package from a dealer or service provider to a site in your organization, it creates and lists System Administrator users in your users table. You cannot directly delete these users. When you accept a service package, you authorize the corresponding System Administrator user to be able to access your site to deliver specific services.

The most common service providers are:

- Avigilon dealers who may provide support, system health, or video monitoring services to one or more of your sites
- Service providers who provide commercial video monitoring services to one or more of your sites
- Local law enforcement entities that you authorize connection to one or more of your sites to allow them access to some of your cameras as part of a public-private partnership

In addition to being a System Administrator user in your organization, this user will be created with the same name on the ACC Server for the site as a member of the Cloud Administrator group. This user cannot directly

be deleted from the ACC Client. You cannot remove the user from the Cloud Administrator group, but you can:

- Modify the privileges granted to that group
- Add the user to one or more other groups

By modifying the privileges of the Cloud Administrator group and adding this user to other groups, you can specify what permissions and devices this user has access to.

If you delete a service package from your site, the corresponding System Administrator user is also removed from the ACC Server of that site. The user remains listed in your ACS organization until all the service packages that they support have been removed.

Adding a User

1. On the  Organization Management page, in the Users tab, click **Add user**.
2. Enter the user's email information.
3. In the **Role** drop-down menu, select the user's role. See *User Roles* on page 101 for a description of each role.
4. Select a site from the **Site Access** and select a schedule for **Security Notifications** and **Health Notifications** for that site.
    - Users can only view video, notifications, and devices for sites they have access to.
    - The schedule determines when the user will receive security and health notifications for that site. If a user does not need to receive security or health notifications, select **Never** for those schedules. For Viewer roles, the schedules will be set to **Never** and cannot be edited.
5. Click **Save**.

    The user will receive an email invitation with a registration link that expires within 24 hours.

When a user clicks the registration link, they will be prompted to create a password. For more information, see *Registering Your User Account* on page 7.

Once the user registers, their status will change from Invited to Enabled.

Resending a User Invite

If a user does not register within 24 hours, their registration link expires. If they click an expired registration link, they will see an error message prompting them to call their administrator. You can resend an invitation.

1. On the  Organization Management page, in the Users tab, select a user.Click **Resend Invite**.

    A new invitation is emailed to the user.

Updating a User

If a user's information or role changes, you can update the user account.

> **Tip:** Filter users by their name, email address, role or site access.

1. On the Organization Management page > Users tab, select a user.
2. Enter the new information.
3. Click **Save**.

Removing a User

To remove a user from the Avigilon Cloud Services platform, you can delete their account.

1. On the Organization Management page, in the Users tab, click next to users you want to remove.
   The Delete User dialog box is displayed.
2. Confirm the users you want to delete and click **Delete**.

Resetting a User's Password

After 3 failed attempts to sign in, a user will be locked out of their account for 30 minutes. They can click **Forgot my password** on the sign in page, or an administrator can reset it.

1. On the Organization Management page > Users tab, select a user.
2. At the bottom of the page, click **Reset Password**.

   A password reset email is sent to the user.

Connecting ACC™ to the Cloud

This section describes how to connect your ACC site to Avigilon Cloud Services so users can view video from their browser or mobile device.

Before Connecting Your ACC Site

- Check the *System Requirements* on page 4.
- Ensure your ACC site has Internet access.
- Ensure that each ACC Server is version 7.12 or later and that the same version of the ACC Web Endpoint Service is installed and running.
- If you have a multi-server site, add all servers to the site before connecting to Avigilon Cloud Services. Otherwise you will have to disconnect the standalone servers from Avigilon Cloud Services before adding them to your single ACC site.
- Ensure each server has the correct time zone, date, time, and daylight saving time settings. For a multi-server site, ensure the servers are synchronized to a network time protocol (NTP) server.

Registering Your Organization

Administrators should register their organization in Avigilon Cloud Services. This organization can include one or more ACC sites and provides users with access to cameras across all sites.

1. In your browser, go to **cloud.avigilon.com**.
2. Select a **region*** then click **Create a new ACS organization**.
3. Enter the organization name and your contact information. Click **Submit**.
4. If Google™ reCAPTCHA is not supported, you will be directed to contact **support@avigilon.com**.
5. A registration email will be sent. Complete your registration:
    a. In the email, click the registration link. This link is only valid for 24 hours.

       If the link expires, register your organization again.

       If the link expires, contact *AvigilonCloud Services Support* to resend the link.

    b. Create a password. This password is unique to Avigilon Cloud Services and does not need to match your ACC password.

       Your password must contain 8-50 characters and include at least one:

       - Uppercase letter
       - Lowercase letter
       - Number
       - Special character ($ @ # ! % * ? & + \ < > . _ - ~ : ; = ^] | ' ` { /) (} {)

       Your password cannot include the word "Password".

       If you are a federated user, you are not prompted to set a new password. Avigilon Cloud Services will use your identity provider credential, such as a Microsoft account.

    c. Select your **Preferred communication language**. This sets the language for emails from Avigilon Cloud Services.

    d. Click **Submit**, then click **Sign in** and enter your credentials.

    e. Review and accept the End User License Agreement.

Adding a Site to Your Organization

1. After the organization has been created, get an activation code in Avigilon Cloud Services:
    a. In the Sites tab, click **Add site**.

    b. Enter the site name, address, and select a Primary Contact who will receive email notifications about the site.

    c. Click **Add**. A code is displayed.

       Note: Administrators can get a new code for sites with an expired activation code.

       Click the  icon next to the Code Expired label to generate a new code.

2. Copy the code and enter it in the ACC Client software:

a. In the New Task menu , click **Site Setup**.

b. Click the site name, then click **Avigilon Cloud Services** .

c. Click **If you have an activation code, click here.**.

d. Enter the activation code and click **Connect**.

The system should connect shortly. If the system takes more than 15-20 minutes to finalize the connection, disconnect your site and try again.

Adding Users to Avigilon Cloud Services

After the ACC site is connected, an ACC administrator can enable users to access Avigilon Cloud Services. Users imported from Active Directory or ACM™ can also be enabled, however these users will have a unique password for Avigilon Cloud Services that may differ from their ACC password.

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click **Users and Groups** .
3. Select a user, then click **Edit User**.
4. Enter an email address if not already specified. This will be the username in Avigilon Cloud Services.
5. Select the **Connect** checkbox and click **OK**.
6. Click **Yes** to confirm the email address.

   The user will receive an email invitation with a registration link that expires within 24 hours. If the email does not appear, check the junk or spam folder.

Signing In to Avigilon Cloud Services

Users can sign in with their Avigilon Cloud Services credentials at **cloud.avigilon.com** and on the ACC Mobile 3 app.

Note: When you connect to Avigilon Cloud Services, two user groups are automatically created:

- Cloud Administrators
- Cloud Viewers

By default, these user groups have access rights to view all cameras in Avigilon Cloud Services and cannot log in to the ACC Client. Update these groups' access rights according to your organization's policies.

Do not assign ACC users to be members of these groups.

Giving Users Additional Privileges

Avigilon Cloud Services administrators can manage sites, users, and view the System Health dashboard. Avigilon Cloud Services managers can also view dashboards without site or user management privileges. For

more information, see *User Roles* on page 63. You can elevate users to be an administrator or manager.

In Avigilon Cloud Services:

1. On the Organization Management page > Users tab, select a user.
2. In the **Role** drop-down list, select Administrator or Manager.
3. Click **Save**.

* Avigilon Cloud Services Regions

Selecting USA will host your organization and accounts on Microsoft Azure servers in the United States. Selecting Asia Pacific or Oceania will host your account in Australia. All other options will host your account in Canada. Note that all users must select the same region to log in to their accounts.

Customer Management

Linking a Customer Organization to Your Partner Organization

As a partner, you can link a customer organization to your partner organization for customers who have an ACC site connected to Avigilon Cloud Services by offering the *ACC Connect* service package.

> **Note:** The ACC site and ACC Web Endpoint Service must be version 7.10 or later.

This section needs to be completed by both the partner organization and customer organization.

1. *For partners.* On the Organization Management page > Service Packages tab, copy your **Code** and make it available to the customer to add your service package to one or more of their sites.
2. *For customers of partners.* The customer administrator uses this code to **make a service request**, which partners can view.
3. *For partners.* After customers complete the form, you will receive an email notification. Click the link to **Accept** or **Decline** your customer's request for service.

   > **Tip:** You can also go to the Organization Management > Customer tab and view your Pending Requests.

4. *For partners.* After the service request is accepted, you will be able to provide services to that site.

Managing Pending Requests

As a partner, you will receive email notifications whenever a customer requests a new service or cancels their subscription. You can accept or decline requests in Avigilon Cloud Services.

To manage a pending request:

- Follow the link in your email and **Accept** or **Decline** the request.
- Go to the Organization Management > Customer tab and **Accept** or **Decline** the request.

> **Tip:** A circle that is displayed next to the Organization Management > Monitoring tab indicates a reply is needed.

Viewing Customer Information

View information about your subscribers, like their contact information and status, on the Organization Management page in the Customers tab.

- Use the Filter to search for subscribers by organization name.
- Select an organization to view information about its sites and subscriptions.

Central Station Monitoring

As a partner, you can monitor video events from customer sites using Central Station software. To connect a site to Central Station, complete this section.

> **Note:** If you have a user account in both the service provider and customer organization, make sure you are signed in as a service provider. You'll know you're signed in as a service provider if you see the organization drop-down list in the top-left area.

Making Virtual Visits to Your Customer Organizations

As a partner, you can make virtual visits to your customer organizations and view their system health status and notifications.

System Health Monitoring

> **Note:** A subscription for the Advanced System Health Package is not required.

1. Click  System Health in the left sidebar.
2. Click **Sites**, **Servers** or **Cameras** to drill down into details for devices in the organization.

Advanced System Health Monitoring

> **Note:** A subscription for the Advanced System Health Package is required to be enabled for both the partner organization and customer organization.

Opt-in as a Partner

1. Log in as an administrator in your partner organization.
2. Click  Organization Management in the left sidebar.
3. Click the **Preview features** tab.
4. Click **On** to enable the **Advanced System Health Package**.

   Receive health and security notifications in the  Notification Center when ACC events occur in the  System Health dashboard.

   Perform remote software upgrade of ACC sites that run ACC software version 7.12 or later.

   > **Note:** ACC events, such as analytic or motion detection events, that have been configured as alarms in the ACC software are categorized as security notifications in ACS. See your ACC documentation for more information on configuring alarms.

5. Click **Save** to confirm your change.
6. Click **OK** to enable the preview feature.

Opt-in as a Customer

To remotely visit customer organizations, instruct the customer to complete the above steps for their organization.

View Advanced System Health

1. Log in as an administrator in your partner organization.
2. Click  System Health in the left sidebar.

   > **Note:** The Organizations tab displays every customer organization linked to your partner organization.

3. Click an organization to drill down into details for devices in the organization.

Notifications

Reviewing Notifications

Administrators, Managers, and Responders can review and resolve notifications for sites they have access to from their browser in the Notifications. You can view a short 10-second clip of the video, or the full event recording.

Viewing a Notification

You can view a notification from the Notifications.

- Click a notification.

  > **Tip:** You can filter notifications to find specific events. For more information, see *Filtering Notifications* on the next page.

  The notification details are displayed.

  In the right-hand video player, a 10-second preview clip plays. The clip may not show the full recorded event. You can choose to watch the entire recorded video from the player.

  To see the full recording:

  - Below the video player, click **Full**.

    Use the timeline to view the video.

  To go back to the 10-second preview:

  - Below the video player, click **Preview**.

  To view the previous or next notification, in the top-right corner click or .

Downloading Event Video

If a notification shows an unusual event, you can download the video in MP4 format for investigation and archiving from your browser. You can download up to 60 minutes of the full event video.

To download recorded video:

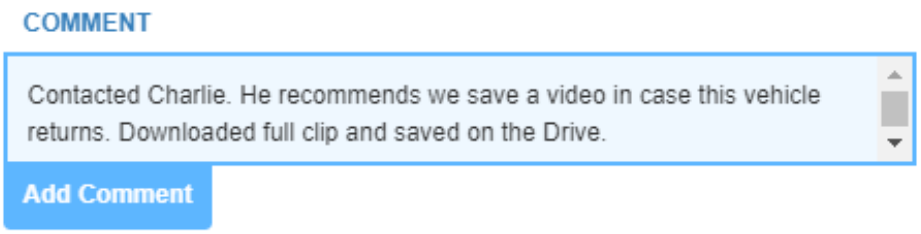
1. In the video player, click  .

   The Download video dialog box is displayed.
2. Using the camera's local time, select the date and start time.
3. In the **Duration:** box, enter how long the video should be. The maximum duration is 60 minutes.
4. Set the Quality to **High** to download a high resolution clip or **Low** to download a low resolution clip.
5. Click **Submit**.

Adding a Comment

You can leave a comment to report if an action was taken or if the issue was resolved. The comment can be up to 256 characters.

1. In the **Comment** box, enter a description.



2. Click **Add Comment**.

   The comment appears in the Activity Log.

Resolving a Notification

Once a notification is resolved, you can mark it as reviewed. Reviewed notifications can be filtered from the Notifications to help other users focus on unreviewed notifications.

You can also mark a notification as a false analytic detection. False detections should still be marked as reviewed, so they do not clutter the Notification Table. If you have many false detections, you may need to adjust your analytic rules.

To mark a false detection:

- Next to False Detection?, select **Yes**.

To mark the notification as reviewed:

- Next to Reviewed?, select **Yes**.

Filtering Notifications

You can filter notifications by status, site, device, event type, and date. The Notifications will show results only for the filtered criteria.

> **Note:** You will only see notifications from sites you have access to, during the schedule specified by your Administrator.

To clear a filter, click ✕.

To clear all applied filters, click **Clear**.

Calling a Contact

If an event requires escalation and you are not at the physical site, you can call a site Contact from the mobile app or from a phone app on your computer. Examples of contacts include local police, emergency services,

or site managers.

Contacts are configured by Administrators in the browser application. For more information, see *Contacts* on page 99.

In Your Browser:

You can call a Contact while viewing a notification.

1. At the top of a notification, click  .
   A list of Contacts is displayed.
2. Click the number you want to call.
3. Select an app from your computer.
   The call is sent.

Blocking Notifications

To block notifications from a camera, you can disarm it. This is useful if you know maintenance work will be done in an area with analytic rules and do not want to receive security notifications during that time. You can disarm a camera while viewing a notification. You can also block notifications from your mobile device.

In a notification:

1. Click  .
2. Select how long you want to disarm the camera, then click **Save**.
   The camera is disarmed.

Resuming Notifications

To resume notifications from a disarmed camera, you can rearm it.

In a notification:

1. Click  .
2. Click **Rearm**.
   The camera is armed.

Email Notifications

The Avigilon Cloud Services platform can send an email notification each time a security or health notification occurs, so you can keep up with site activity while you're away. Security notifications may include a link to a clip of the event that you can view while on the go.

> **Note:** You will only receive notifications based on your Health Notifications and Security Notifications schedule for the sites you have access to.

You can change whether you receive email notifications on your profile page.

1. In the top-right corner, click your name.
2. Click **Profile settings**.

   The Profile page is displayed.
3. Select whether you receive **Enable email notifications for events**.

   > **Tip:** Enabling and disabling email notifications will only affect the email notifications for the organization you are currently connected to. This gives you more control over which organizations your receive email notifications from. If you have more than one organization you want to change this setting on, you will have to connect to each organization and update the setting.
4. Click **Save**.

Health Notifications

Health notifications are sent from an Avigilon device or a camera. These notifications let you know if there was a communication or connection error.

Health notifications appear in the Notification Center in your browser, and in the Notification and Camera pages in the mobile app. You can review health notifications the same way you review notifications triggered by an analytic rule. For more information, see *Reviewing Notifications* on page 91.

Avigilon Device Notifications

The following table describes the Avigilon device health notifications and how you can solve them.

Health Notification	Description	Troubleshooting
Analytics Server Connection Lost	Connection to analytics server has been lost.	Contact your Dealer.
Analytics Server Queue Full	The analytics server queue is full.	Contact your Dealer.
Device Disconnect	The Avigilon device lost connection to your network.	Sometimes the device reconnects automatically. If the connection is not restored, try restarting the device.
Device Reconnect	The Avigilon device reconnected to your network.	No workaround required.
Application Server Stop	The Avigilon device application is shutting down.	You may receive this notification if you restart your device from your browser or mobile device. If you did not restart your device, contact your Dealer.

Health Notification	Description	Troubleshooting
Application Bad Shutdown	The Avigilon device application ended unexpectedly.	Contact your Dealer.
System Low Resources	The Avigilon device's memory resources are low.	Contact your Dealer.
Db Lost	The database on the Avigilon device was corrupted.	Contact Avigilon Support.
Db Environment Deleted	The database on the Avigilon device experienced a critical error. The database environment was recreated.	Contact Avigilon Support.
Db Environment Deleted With Dbs	The database on the Avigilon device experienced a critical error. The database environment was recreated and some data may have been lost.	Contact Avigilon Support.
Db Environment Recovered	The database on the Avigilon device experienced a critical error. The database environment was successfully recovered.	Contact Avigilon Support to determine why the error occurred.
Db Reindex	The database on the Avigilon device was reindexed.	Contact Avigilon Support.
Storage Init Error	The primary data volume on the Avigilon device failed to initialize.	Contact your Dealer to replace your Avigilon device. Export video if possible.
Storage Volume Failed	The data volume on the Avigilon device is missing or cannot be found.	Contact your Dealer to replace your Avigilon device. Export video if possible.
Storage Volume Restored	The data volume on the Avigilon device was restored to its normal state.	No workaround required.
Storage Low Disk Space	The data volume on the Avigilon device was reduced to 50% of its target size due to low disk space.	Contact your Dealer to replace your Avigilon device. Export video if possible.
Storage Write Queue Full	Data for a device was dropped due to storage system performance, insufficient system resources, or invalid camera stream on the Avigilon device.	Contact your Dealer to replace your Avigilon device. Export video if possible.
Storage Write Failed	A device connected to the Avigilon device failed to write data to the data volume.	Contact your Dealer to replace your Avigilon device. Export video if possible.

Health Notification	Description	Troubleshooting
Storage Writes Blocked	A device connected to the Avigilon device was blocked from writing data to the data volume.	Contact your Dealer to replace your Avigilon device. Export video if possible.
System Cluster Network Failure Detected	A network issue was detected between this Avigilon device and another Avigilon device. Your site may experience poor performance.	Contact your Dealer to replace your Avigilon device. Export video if possible.

Camera Notifications

The following table describes the camera health notifications and how you can solve them.

Health Notification	Description	Troubleshooting
Camera Connected	A camera connected to the Avigilon device.	No workaround required.
Camera Disconnected	A camera disconnected from the Avigilon device.	If the camera comes back online, the system will automatically resolve this issue. If the camera does not come back online, check your camera and network settings.
Camera Tampering	A camera detected sudden changes to the scene.	Check the live video to see if you need to readjust the camera placement or focus.
Device Communication Lost	A camera disconnected from the Avigilon device.	This may be due to a loose Ethernet connection. Reconnect the device cables and the system will automatically resolve the event.
Device Connection Error	A camera connection failed. Device data cannot be received.	Check your camera and network settings.
Device Packets Lost	A camera experienced network packet loss (more than 50% of packets were lost over the last 60 seconds).	Contact your IT department. If the camera is connected to the Camera Uplink Port, contact your Dealer.
Device Packets Recovered	A camera no longer experiences network packet loss.	No workaround required.
Server Firmware Upgrade Started	The camera firmware upgrade started.	No workaround required.

Health Notification	Description	Troubleshooting
Camera Firmware Upgrade Complete	The camera firmware upgraded.	No workaround required.
Server Firmware Upgrade Error	An error occurred during a firmware upgrade.	Contact your Dealer.
Device Record Interrupted	A camera's recording was interrupted.	Check your camera and network settings.
Device Record Restored	A camera's recording was resumed.	No workaround required.

Notification Center

Administrators, Managers, and Responders can view the Notification Center, but will only see notifications for the sites that they have access to based on their health and security notification schedules. Administrators can update your site access and notification schedule.

To view the Notifications, click  .

Notification List

A summary of recent notifications. Filter notifications using the toolbar at the top of the page. For more information, see *Filtering Notifications* on page 92.

Click a notification to view more details. See *Reviewing Notifications* on page 91.

The following table describes the columns in the notifications list.

Column	Description
Status	The following notification status icons appear next to each notification.  — An unreviewed Device Health notification. For more information, see *Health Notifications* on page 57.  — An unreviewed notification.  — A notification currently under review.  — A notification marked as reviewed.
Date/Time	When the notification occurred.
Event Description	The name of the analytic rule that triggered the notification.
Site	The site where the notification occurred.
Device	The camera or Avigilon device that recorded the notification.

Column	Description
Last Viewed By	The last user to view the notification details.
Last Updated	The last time the notification details were updated.

Notification Chart

Click the **Display Chart:** toggle to view a graphical summary of notifications. Selected filters will also filter data in the chart.

You can view information about a particular data point on the chart by hovering over it. This is a quick way to filter and view notifications from a point on the chart.

1. Click a data point you're interested in.

   A tooltip displays the details and number of notifications.
2. Click the number of events to filter the notification list. This may change any filters that were previously applied.

> **Note:** The number of notifications that appear in the list may be fewer than the number of events in the link. This is because the chart displays all events that occurred, while the table displays only notifications you're assigned based on your schedule, site access, and filters.

You can compare notifications from the period before to understand trends and anomalies in your organization.

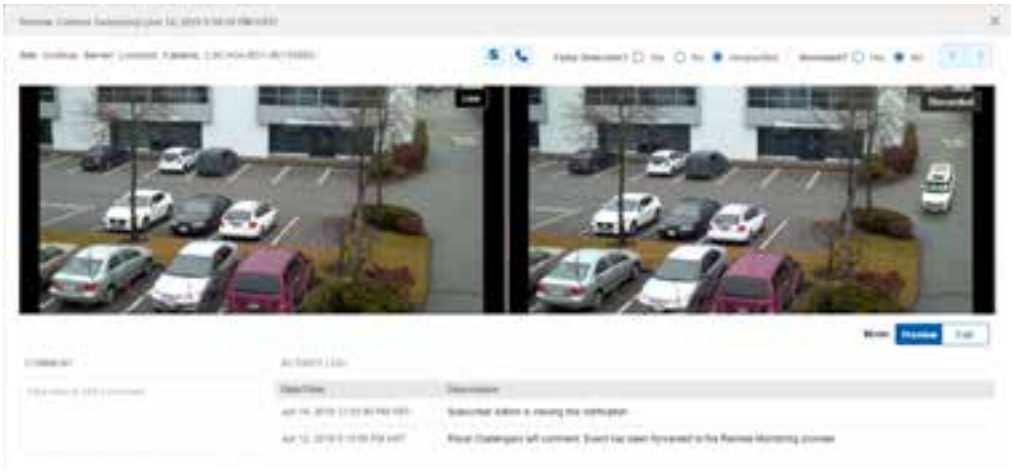
To compare results from the previous period:

- In the chart toolbar, select the **Compare to previous period** checkbox.

  The results from the period before are displayed. The legend displays each period.

Notification Details

Click a notification to view more information.



You can view if others have commented or viewed the notification in the Activity Log. The Activity Log also

captures whether the notification was marked as a false detection or if it was previously marked as reviewed. Other users in your Avigilon Cloud Services platform site can see your activity from their browser or mobile device.

Notification Issues

Can't See Your Notifications?

You may see fewer notifications listed in the Notification Table than events in the Notification Chart. This is because the chart displays all events that occurred, while the table displays only notifications you're assigned based on your schedule, site access, and filters.

To troubleshoot:

- Clear all filters.
- Have an Administrator or Manager check that your site and cameras are connected and working. Ensure that your analytic rules were added properly.
- If there are still no notifications on the Notifications page, your user account may not be set up to receive notifications for that site at that time.

  An Administrator can update your user account to ensure that the correct user role, site, and schedule were selected.

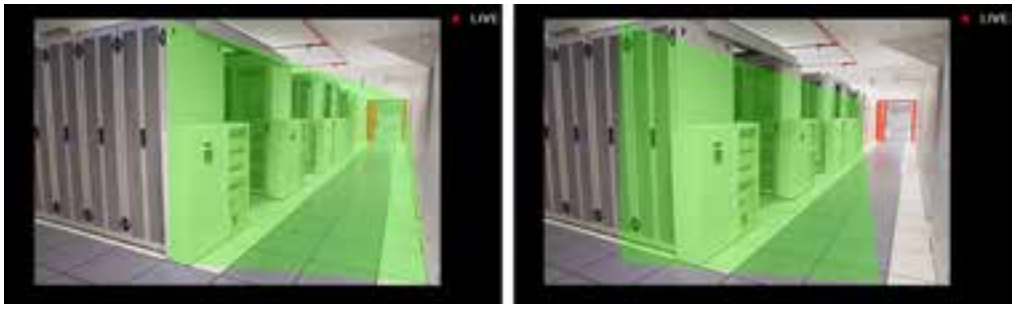
  Once your user account is updated, you will begin receiving notifications. Note that you will not see any notifications prior to the update.
- If your problem is not solved, contact Avigilon Support at +1.888.281.5182 Option 1, then Option 5.

Too Many Notifications?

If you're receiving too many notifications, you may need to adjust your analytic rules. For more information see your ACC documentation.

Too Many False Alarms?

If you're receiving too many false alarms, your analytic rules' region of interest may be misaligned. This can happen if the camera is moved after configuration.



If the overlay is not aligned properly, an Administrator or Manager can configure the camera's analytic rule.

Contacts

When reviewing a security or health notification, Administrators, Managers and Responders can escalate a

situation by calling a contact for that site. For more information, see *Calling a Contact* on page 92.

The Contacts list tells users who they can call if an event needs to be escalated, or in case of an emergency. For example, a store clerk uses the Contacts list when they receive a security notification.

Administrators can manage contacts on the Organization Management page, in the **Contacts** tab.

Examples of contacts include:

- An emergency service number.
- The local police.
- The owner or manager.
- The dealer.
- A site Administrator.

A contact does not need to have a user account in the Avigilon Cloud Services platform site.

Adding a Contact

An organization can have several contacts that can be reached in case of emergency. Each contact can be responsible for one or more sites.

Add a contact for each site in your organization so Administrators, Managers, and Responders have someone they can reach in case of an emergency.

1. On the Organization Management page, in the Contacts tab, click **Add contact**.
2. Enter the contact's **Name** and **Phone Number**.
3. From the **Site** drop-down list, select one or more sites. The contact can be reached for selected sites.
4. Click **Add**.

Editing Contact Details

If a contact's information changes, you can update the contact's details.

> **Tip:** In the top-right corner, click to show or hide filters. You can filter contacts by their name or site access.

1. On the Organization Management page, in the Contacts tab, select a contact.
2. Enter the new information.
3. Click **Save**.

Removing a Contact

If someone leaves your organization, remove them as a contact.

1. On the Organization Management page, in the Contacts tab, select the checkbox next to contacts you want to remove.
2. In the top-right corner, click .

   A dialog box will ask you to confirm.
3. Click **Delete**.

Users

User Roles

There are four types of user roles: Administrators, Managers, Responders, and Viewers. Each role has access to different Avigilon Cloud Services platform features. A user can have one role that carries across all sites that they have access to. The following table describes the four types of users and the permissions they have.

	Administrator	Manager	Responder	Viewer
Monitor Video	✓	✓	✓	✓
Manage Bookmarks	✓	✓	✓	✓
Receive and Respond to Notifications	✓	✓	✓	—
Manage Cameras and Devices	✓	✓	—	—
Manage Sites and User Accounts	✓	—	—	—

Tip: It is recommended that you have at least two active users with an Administrator role in your organization at all times.

Primary Administrator

Every organization has a primary administrator who is notified of changes to the organization. The user that created the organization is the primary administrator by default, but another administrator in the organization can be made a primary administrator.

To change the current primary administrator to another administrator:

1. On the  Organization Management page, navigate to the General tab.
2. From the Primary Administrator drop-down list, select a different administrator.

   If you do not have any other users with the Administrator role, no users will show up in the drop-down list.
3. Click **Save**.

Support User

Every organization has a Support user identified by the `support@avigilon.com` email. This System Administrator user cannot be deleted but you can change whether they have access to sites or what sites they have access to. By default, the Support user does not have either the ability to login or access to any of your sites. The Support user can be used by Avigilon Support to provide troubleshooting support to cloud users.

An organization administrator can grant the Support user access to sites, however, ACC has the final authority of privileges for the Support user on the ACC Server. When the Support user is granted access to a site from the ACS web client, the ACC Servers in that site will create a user for Avigilon Support. This user cannot be deleted using the ACC Client. The Support user is a member of and has all the privileges of the Cloud Administrator group.

The Support user enables Avigilon Support to access your sites without the organization administrator having to create a new user for that purpose. When on the phone with Avigilon Support, they will ask you to grant the Support user access to a site so that they can help you troubleshoot your issue. An Administrator can grant access to the required sites. If the Support user has appropriate privileges, Avigilon Support can log in to your organization to make a virtual visit with their Avigilon enterprise credentials with 2-factor authentication as the Support user. During the virtual visit the Avigilon Support team member can only access the sites that they have been granted permission to access.

When your support session is done, the privileges and access granted to the Support user can be removed by an Administrator. Removing the Support user's access in ACS automatically removes their access from the corresponding ACC Servers.

Other System Administrator Users

When you add a service package from a dealer or service provider to a site in your organization, it creates and lists System Administrator users in your users table. You cannot directly delete these users. When you accept a service package, you authorize the corresponding System Administrator user to be able to access your site to deliver specific services.

The most common service providers are:

- Avigilon dealers who may provide support, system health, or video monitoring services to one or more of your sites
- Service providers who provide commercial video monitoring services to one or more of your sites
- Local law enforcement entities that you authorize connection to one or more of your sites to allow them access to some of your cameras as part of a public-private partnership

In addition to being a System Administrator user in your organization, this user will be created with the same name on the ACC Server for the site as a member of the Cloud Administrator group. This user cannot directly be deleted from the ACC Client. You cannot remove the user from the Cloud Administrator group, but you

can:

- Modify the privileges granted to that group
- Add the user to one or more other groups

By modifying the privileges of the Cloud Administrator group and adding this user to other groups, you can specify what permissions and devices this user has access to.

If you delete a service package from your site, the corresponding System Administrator user is also removed from the ACC Server of that site. The user remains listed in your ACS organization until all the service packages that they support have been removed.

Adding a User

1. On the  Organization Management page, in the Users tab, click **Add user**.
2. Enter the user's email information.
3. In the **Role** drop-down menu, select the user's role. See *User Roles* on page 101 for a description of each role.
4. Click **Save**.

   The user will receive an email invitation with a registration link that expires within 24 hours.

When a user clicks the registration link, they will be prompted to create a password. For more information, see *Registering Your User Account* on page 7.

Once the user registers, their status will change from Invited to Enabled.

Resending a User Invite

If a user does not register within 24 hours, their registration link expires. If they click an expired registration link, they will see an error message prompting them to call their administrator. You can resend an invitation.

1. On the  Organization Management page, in the Users tab, select a user.Click **Resend Invite**.

   A new invitation is emailed to the user.

Viewing and Editing a User's Details

If a user's contact information or schedule changes, you can update the user account.

> **Tip:** In the top-right corner, click  to show or hide filters. You can filter users by their name, email address, role or site access.

1. On the  Organization Management page, in the Users tab, select a user.
2. Enter the new information.
3. Click **Save**.

Removing a User

To remove a user from the Avigilon Cloud Services platform, you can delete their account.

1. On the Organization Management page, in the Users tab, click next to users you want to remove.
   The Delete User dialog box is displayed.
2. Confirm the users you want to delete and click **Delete**.

Troubleshooting and FAQs

Activation Issues

If your activation code expires, generate a new code:

- On the Organization Management page, in the Sites tab, click .
  A new activation code is displayed. Use it within 24 hours.

For additional help connecting your ACC site, see the **Avigilon Cloud Services Web Client FAQ**.

Account Issues

Registration Link Expired

The registration link is only active for 24 hours.

If you are an administrator registering your organization:

- Go to **cloud.avigilon.com** and register your organization again.

If you are an administrator connecting an ACC site:

1. On the Site Setup page, click **Avigilon Cloud Services** > **Cancel**.
2. Click **Avigilon Cloud Services** again and reconnect your site.
3. Complete your registration and sign in.

If you are a user invited to Avigilon Cloud Services, contact your administrator to update your user account in the ACC Client software:

1. On the Site Setup page, click **Users and Groups**.
2. Select the user and click **Edit**.
3. Clear the **Connect** checkbox and click **OK**.
4. Select the user and click **Edit**.
5. Select the **Connect** checkbox and click **OK** to save.

   The user will receive a new registration email.

If you are a partner, dealer or service provider, see *For More Information* on page 107 to resend the link. You will receive a new registration email.

Forgot Your Password or Locked Out

If you forgot your password or are locked out of your account, you can reset it from the Sign in page:

- Click **Forgot my password** or **Forgot your password?** and follow the prompts.

Changed Your Email Address

If your email address changes, contact your administrator to delete your old user account and create a new one using your new email address.

Google™ reCAPTCHA is not supported in your region

If Google™ reCAPTCHA is not supported, you will be directed to contact **support@avigilon.com**.

Viewing Player Details

When calling Avigilon Support to troubleshoot an issue, it can be helpful to know about your cloud connection. You can view that information from the video player.

Hover over the video player to display an overlay on the player with the timeline and controls. This overlay shows the camera name and status in the upper-right corner.

- **To view more information**, click the camera name.

  To show and hide the stream and connection information, click **Details**.
- **To hide the information**, click **X**.

Tip: If you have many players open in a view, pin  the camera details to see at-a-glance which cameras are displayed.

Other Issues

Buttons or text in Avigilon Cloud Services appear skewed

Press **CTRL** + **F5** to clear your cache.

'Avigilon Cloud Services is temporarily unavailable' message is displayed when connecting ACC to the cloud

- The firewall configuration or antivirus software could be interfering with outbound communications. Check your network configuration.
- The installed ACC software version does not meet the minimum required version 7.10. All the servers in a multi-server site should be running the same version. Upgrade to ACC version 7.10 or higher before attempting to connect again.
- The ACC Web Endpoint service may not be not installed, is not running, or is not upgraded to the current version on the ACC Server. The Web Endpoint service should be installed on all servers except for on the AI appliance. ACC and the Web Endpoint service should be the same version for all servers in a site. Use the ACC Site Health report to find the version and status of the Web Endpoint service on all your servers and either manually restart or uninstall and reinstall the Web Endpoint service.

You do not see any cameras in the web client device tree

- Check if the ACC site is connected. Click ⓘ next to the site name to see the site information. A red exclamation mark appears there are issues with connecting to the ACC site.
- Connection may not be open or lost (410): You may not be using a supported browser. See *System Requirements* on page 4 for the list of supported browsers.
- Error initiating a peer-to-peer connection. Gateway timeout error (504): Your ACC site is not communicating with the cloud. If it is a stand-alone server, contact your administrator to ensure the Web Endpoint service is running or is upgraded to match the ACC release.
- Authentication Failed: Your user account is not linked to a user account on the ACC server. From the ACC Users and Groups dialog, clear the Connect check box for the user, click Apply, select the Connect check box again and click Apply. Contact your administrator to investigate further.
- Permission Denied: Your user account does not have the permission to access the device. Contact your administrator to update your camera access privileges using the ACC client.

You do not see the System Health dashboard icon

To view System Health, you must be assigned an Administrator or Manager role.

You do not see the Reports icon

To view Reports, you must be assigned an Administrator or Manager role.

'Invalid username or password (401)' error message is displayed when trying to view cameras

Incorrect time settings on the ACC server unauthorize a user. Make sure the ACC server uses a reliable NTP server such as the **United States National Institute of Standards and Technology (NIST) Internet Time Service** or the **NTP Pool Project**.

For More Information

Support

Fill out this **online form**.

For additional contact information, visit **avigilon.com/contact**.

Feedback

We value your feedback. To help us make our products better, contact us.

- At the bottom of any Avigilon Cloud Services page, click **Feedback**.