

FAQ for the Avigilon Cloud Services Web Client

A no-install ACC web client enables users to securely view live and recorded video and monitor system health of all cloud-connected ACC sites

Avigilon Cloud Services (ACS) introduces a new browser-based client to view live and recorded video from Avigilon Control Center (ACC). This does not require installing a client and minimizes the reconfiguration of your network firewalls. By connecting your ACC system to Avigilon Cloud Services, operators can use a Chrome, Safari or Edge browser to securely view live and recorded video and monitor the system health of your sites at no additional charge. ACC Mobile 3 deployments are simplified with ACS. By connecting using their ACS credentials, mobile users automatically gain access to every ACC site they have permission to view.

Securely view live and recorded video

- Access camera lists
- View live and recorded video
- Bookmark video segments for future reference
- Control PTZ camera movements
- Trigger digital outputs
- Export snapshots and video in MP4 format

Monitor the system health of your sites

- Review a single system health dashboard that rolls-up the active status of all recorders and connected cameras to help you prioritize your maintenance activities on critical sites
- Access configuration details of servers and cameras such as video streaming settings, software and firmware versions, and IP address information
- Check network performance metrics such as device bandwidth utilization
- Establish if your server is performing to expectation. The server Storage Analysis feature allows you to check if video is being recorded and if the retention targets are being met
- Audit the configuration of devices with a (.CSV) text format report that lists all servers including their site name and cameras with their type, names, location, and configuration.
- Locate and review devices from all your sites with our smart filter that allows you to use partial matches based on device name, device model, site name, IP address, or MAC address

For other activities, administrators may use the traditional ACC Windows client application.

Features & Prerequisites	Page
Q: What are the features the Web Client provides for cloud-connected ACC sites?	4
Q: What are the system requirements for connecting to ACS?	4
Q: What are the system requirements for computers using the Web Client?	4
Q: Are there any new ACC licenses required to use the Web Client?	4
Q: ACS supports firewall traversal so it can offer secure remote access. How do I add my ACC sites to the ACC Mobile 3 app?	5
Q: Which Avigilon mobile app should I use for cloud-connected ACC sites?	5
Q: What are the Privacy Considerations for using Avigilon Cloud Services?	5

Cloud-Connecting ACC sites	Page
Q: How do I cloud-connect my ACC server to Avigilon Cloud Services?	6
Q: Method 1: How do I register my organization using the ACS web client? - Multi-site organizations or to host account outside of the USA	6
Q: How do I register an organization using the ACS Web Client?	6
Q: How do I add an ACC site using an activation code?	7
Q: What do I do if the activation code for my site expires?	7
Q: How do I access my basic self-activated site?	8
Q: What happens if my ACC user account has been web-enabled on multiple self-activated sites or registered organizations?	8
Q: What is a primary administrator on ACS?	8
Q: Can I change the primary administrator for an organization?	8
Q: How do I change a user's ACS role?	9

Enabling Web Users	Page
Q: After connecting my ACC site, how do ACC users gain access to the Avigilon Cloud Services Web Client?	10
Q: What do I do if the link in my email token expires before I use it?	10
Users will receive an email inviting them to set a password for their ACS account. The link will expire in 24 hours. If it expires the ACC administrator need to toggle the "Connect" checkbox to send a new invitation	10
Q: In the ACC Client, I see two new user groups - Cloud Administrators and Cloud Viewers. What are these for?	10
Q: ACC Enterprise Edition can be set-up to automatically synchronize users with Active Directory using LDAP. If a domain user changes their domain password, it is automatically synced to ACC, does it also synchronize this password with ACS?	11

System Health Monitoring	Page
Q: Is there a charge or fee for System Health Monitoring?	12
Q: What user roles can see System Health Monitoring?	12
Q: As a Dealer / Integration how do I access the system health report for my customers?	12

Q: Can I generate a system health report?	12
Q: Can I check the firmware version of a server or camera?	12
Q: Can I review or audit that my recording policies are being followed?	12

Configuration Considerations	Page
-------------------------------------	-------------

Q: What is the performance impact to a live ACC system when using the Web Client?	13
Q: What are the network security risks to a live ACC system when connecting to the Avigilon Cloud Platform?	13
Q: What are the network / Firewall requirements for the server at the ACC site to cloud communications?	13
Q: We have strict firewall policies requiring whitelisting servers, what are the explicit services used?	13

Troubleshooting	Page
------------------------	-------------

Q: What should I do if I receive the message “Avigilon Cloud Services is temporarily unavailable” when trying to connect ACC to ACS?	15
Q: What should I do if I do not see any cameras in the ACS camera tree?	15
Q: I don’t see System Health Monitoring?	16

ScreenShots	Page
--------------------	-------------

ACS View Tab	17
Recorded Video playback with color-coded timeline, bookmark creation and review, Video Snapshot, MP4 video export	17
Recall Saved View from ACC server or create new personal views saved to ACS servers	18
System Health Monitoring Main Tab Site View	18
System Health Monitoring Main Tab Server View	19
System Health Monitoring Server Details	19

Features & Prerequisites

Q: What are the features the Web Client provides for cloud-connected ACC sites?

A: The web client supports:

Securely viewing live and recorded video

- Access camera lists
- View live and recorded video
- Bookmark video segments for future reference
- Control PTZ camera movements
- Trigger digital outputs
- Export snapshots and video in MP4 format

Monitoring the system health of your sites

- Review a single system health dashboard that rolls-up the status of all recorders and cameras
- Access configuration details of servers and cameras
- Check network performance metrics such as device bandwidth utilization
- Establish if your server is performing to recording expectations
- Audit and generate a (.CSV) text format report that lists all servers and cameras
- Locate and review devices from all your sites with our smart filter

Q: What are the system requirements for connecting to ACS?

A: Connecting an ACC site to ACS requires:

- Each ACC server is running a minimum version ACC 7.4.4.14 and higher.
- If not already installed, install the ACC Web Endpoint Service component with the same version as ACC on each server.
- The ACC 6 Gateway component is not required to be installed nor running.
- Using the most recent ACC release will provide additional features in ACS such as Health Monitoring.

Q: What are the system requirements for computers using the Web Client?

A: This feature requires a computer running a recent version of a supported web browser; Chrome 72+, Safari 12.1+, or MS Edge 80+. Microsoft Windows, Apple MacOS, and Chromebooks machines with mid-grade graphics chips are compatible. The mobile web browsers on most mobile phones and tablets and their mobile browsers are **not** formally supported. We suggest using the ACC Mobile 3 app for mobile devices.

Q: Are there any new ACC licenses required to use the Web Client?

A: No, access to the ACS Web Client is free for any host licensed under any ACC edition (Core, Standard, Enterprise).

Q: ACS supports firewall traversal so it can offer secure remote access. How do I add my ACC sites to the ACC Mobile 3 app?

A: ACC Mobile 3 app supports signing in using ACS credentials to access any cloud-connected ACC sites. ACC Mobile 3 app can connect with no additional firewall reconfiguration if the ACC site is already cloud-connected. It's still possible to directly add the IP / hostname to ACC Mobile 3 for ACC 6 sites or for ACC 7 sites that aren't connected to ACS and log in as before.

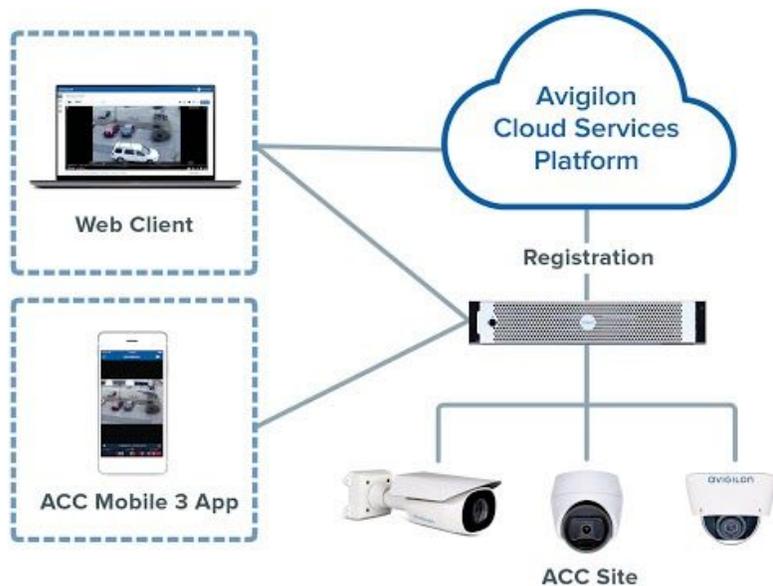
Q: Which Avigilon mobile app should I use for cloud-connected ACC sites?

A: Use the ACC Mobile 3 app. While the Avigilon Blue Mobile app will allow users to login and see the names of their cloud-connected ACC sites, the App is not able to stream video from ACC sites nor can it receive alarm events from the ACC sites.

Q: What are the Privacy Considerations for using Avigilon Cloud Services?

A: Web Client access to ACC sites using Avigilon Cloud Services does not store any video in the cloud. All video travels in the secure encrypted point-to-point connection between client and ACC server. ACS may try to use Traversal Using Relay around NAT (TURN) to establish a peer-to-peer video connection between the server and the web client. In traversing this path, the video will be relayed by the ACS point of presence but is not stored. User account IDs and hashed passwords are stored on Microsoft Azure servers, but no other personally identifiable information is collected or required to use the service.

The method used to register your ACC site will determine which ACS data center will host your account. If you use an email address in the ACC client to register a stand-alone ACC site, then your ACS user accounts are hosted in the Microsoft Azure servers in the United States. If you use the ACS web client to register a registered organization that will connect to multiple ACC sites, you can select a preferred data center by selecting a region before starting the registration on cloud.avigilon.com. Choosing the default region will create your organization and accounts in Microsoft Azure servers in the United States, selecting Asia Pacific or Oceania will host your account in Australia, and for the rest of the world, any option will host your account in the data center in Canada. All users must select this same region to log in to their accounts..



Cloud-Connecting ACC sites

Q: How do I cloud-connect my ACC server to Avigilon Cloud Services?

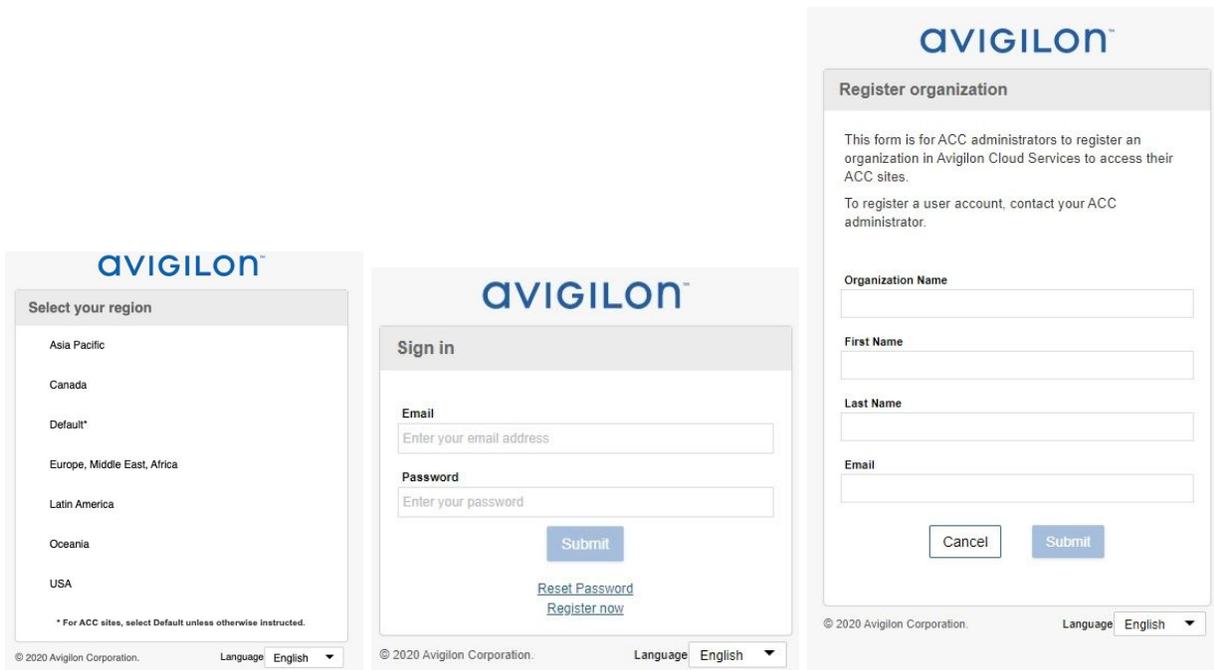
A: There are two ways to register your organization with ACS and add your ACC site; (1) Registering an organization in the ACS Web Client for access to multiple ACC sites under a common organization (2) Self-Activation from ACC client for single stand-alone servers.

Q: Method 1: How do I register my organization using the ACS web client? - Multi-site organizations or to host account outside of the USA

A: For customers with multiple sites like a campus or a distributed enterprise, an administrator should register their organization with ACS. Once you have a registered organization on ACS, you can add ACC sites to ACS using an activation code yourself. The advantage for customers of distributed sites is that users of the web client or ACC Mobile 3 app will gain access to all ACC sites under the registered organization without switching between ACC sites. The ACC Mobile 3 app will receive mobile notifications from all sites in the organization.

Q: How do I register an organization using the ACS Web Client?

A: Go to cloud.avigilon.com and select a region. Click "Register now" to create your organization and primary administrator account.



The image shows three screenshots of the Avigilon web client interface:

- Select your region:** A page with the Avigilon logo and a list of regions: Asia Pacific, Canada, Default*, Europe, Middle East, Africa, Latin America, Oceania, and USA. A note at the bottom states: "* For ACC sites, select Default unless otherwise instructed." The footer includes "© 2020 Avigilon Corporation." and a language dropdown set to "English".
- Sign in:** A page with the Avigilon logo and a "Sign in" header. It contains two input fields: "Email" (with placeholder "Enter your email address") and "Password" (with placeholder "Enter your password"). Below the fields is a blue "Submit" button, and below that are two links: "Reset Password" and "Register now". The footer includes "© 2020 Avigilon Corporation." and a language dropdown set to "English".
- Register organization:** A page with the Avigilon logo and a "Register organization" header. It contains a paragraph of text: "This form is for ACC administrators to register an organization in Avigilon Cloud Services to access their ACC sites. To register a user account, contact your ACC administrator." Below the text are four input fields: "Organization Name", "First Name", "Last Name", and "Email". At the bottom are two buttons: "Cancel" and "Submit". The footer includes "© 2020 Avigilon Corporation." and a language dropdown set to "English".

Choosing the default region will create your organization and accounts in Microsoft Azure servers in the **United States**, selecting Asia Pacific or Oceania will host your account in **Australia**, and for the rest of the world, any option will host your account in the data center in **Canada**.

Note that all ACS users must select this same region to log in to their accounts.

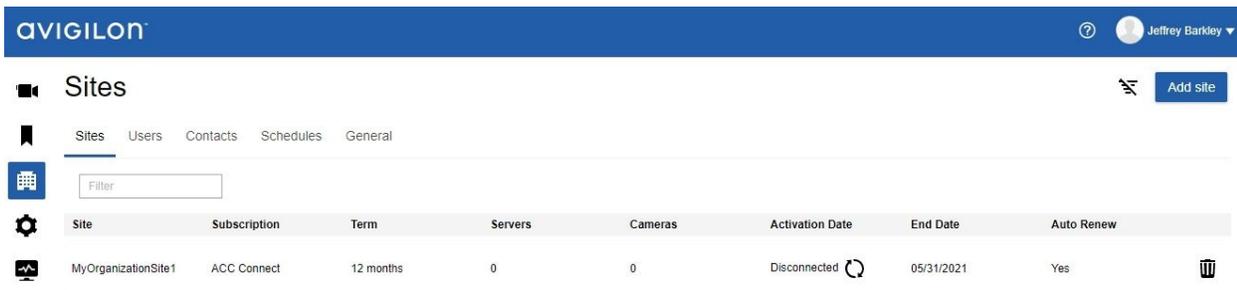
Q: How do I add an ACC site to an organization using an activation code?

A: After registering an organization with ACS as the administrator, you will automatically be taken to the sites page where you can click the “Add Site” button. For each site you add, an activation code will be generated. The code must be used within 24 hours. In the ACC Client, you, as the administrator, can go to the Site Setup > Avigilon Cloud Services settings and enter the code.



Q: What do I do if the activation code for my site expires?

A: An ACS administrator can regenerate a code on the sites tab by clicking the refresh icon next to expired and provide the new code to the ACC administrator.



Q: Method 2: How does Basic Self-Activation from ACC work? - Easiest Solution for One Site

If you only have one site, the easiest method to connect to the cloud is self-activation from the ACC client. Administrators use the ACC Client Site Setup tab to access the Avigilon Cloud Services button, select an ACC administrative user with an email address in the dialog and click Connect.



You will receive an email with a link to activate your organization. Click on the link, enter your password and you will activate the organization and login to ACS. NOTE: The organization will be created in a Microsoft Azure data center in the United States. All users must select the Default or USA region when they attempt to log in.

IMPORTANT: DO NOT CANCEL OR EXIT AVIGILON CLOUD SERVICES DIALOG UNTIL SUCCESSFUL COMPETING ACTIVATION.

Q: How do I access my basic self-activated site?

A: Each registration creates a unique ACS customer organization for each connected ACC site. The name of the organization is the name of the ACC site or the ACC server. An ACC site can consist of a single server or multiple servers. The Web Client or ACC Mobile 3 app will connect the user to the ACC site at login if their user profile was web-enabled / connected on the ACC site (see Enabling Web Users topic below).

Q: What happens if my ACC user account has been web-enabled on multiple self-activated sites or registered organizations?

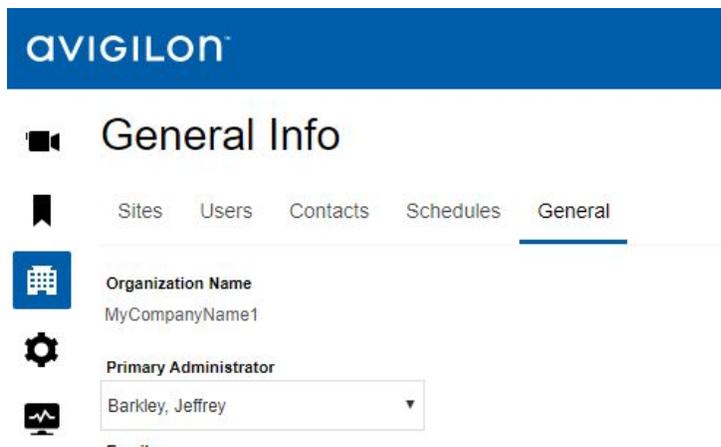
A: From the Web Client or ACC Mobile 3 app, you must select one organization with which to interact. Under your user profile in the Web Client, select “Switch Organization” from the dropdown and choose an organization name. Only video from the selected organization can be viewed. The ACC Mobile 3 app will receive mobile notifications from only the selected organization.

Q: What is a primary administrator on ACS?

A: Every ACS organization has a primary administrator. The primary administrator is notified of changes to the ACS organization. The user that created the organization will by default be the primary administrator.

Q: Can I change the primary administrator for an organization?

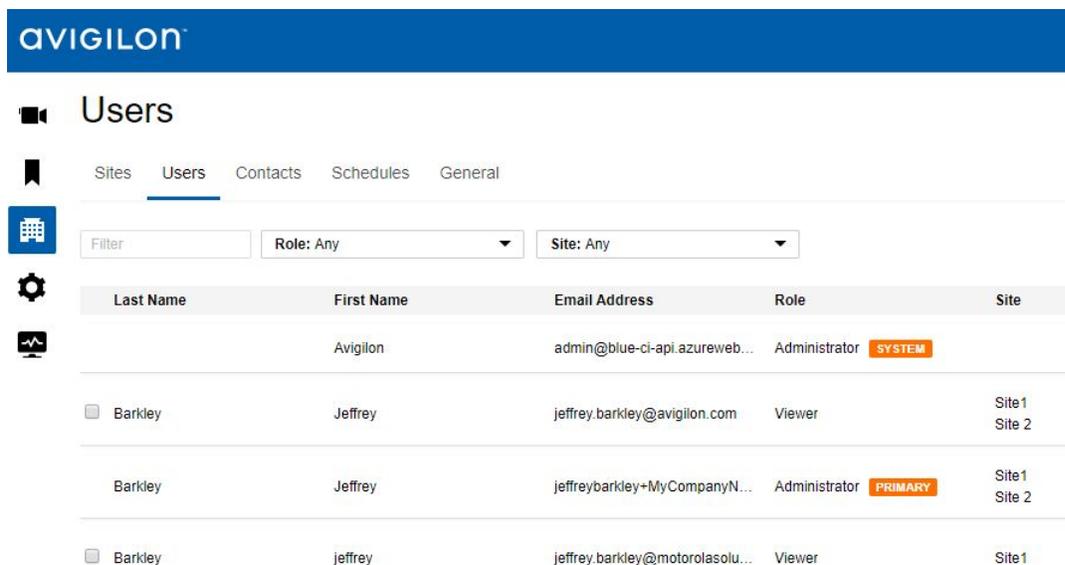
A: Yes, you can change the primary administrator by going to the Organization General Info tab and use the pulldown to select a different administrator to be the primary administrator .



If you do not have any other users with the administrator, role no other users will show up in the list. RECOMMENDATION: Avigilon recommends at all times you have at least two ACS users with an Administrator role.

Q: How do I change a user's ACS role?

A: Any ACS administrator can manage users. They would go to the Organization Users tab to see users' current role and select the user whose role they want to change and use the dropdown to change their role.



AVIGILON

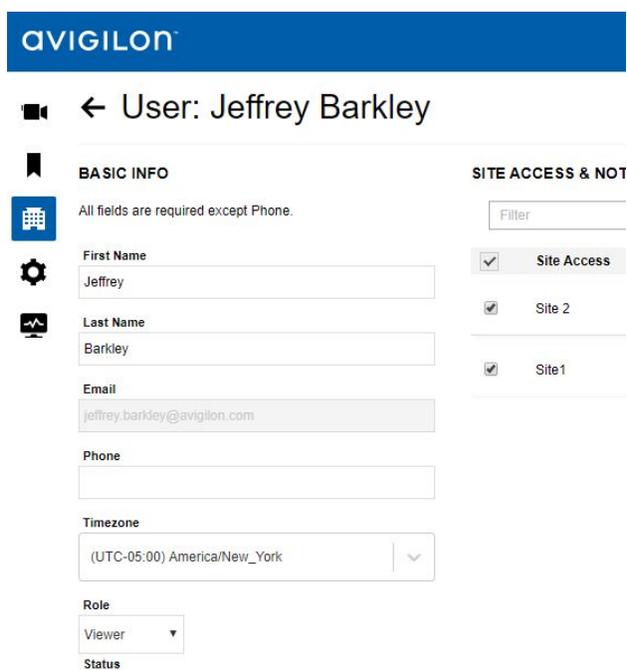
Users

Sites **Users** Contacts Schedules General

Filter Role: Any Site: Any

Last Name	First Name	Email Address	Role	Site
	Avigilon	admin@blue-ci-api.azureweb...	Administrator SYSTEM	
<input type="checkbox"/> Barkley	Jeffrey	jeffrey.barkley@avigilon.com	Viewer	Site 1 Site 2
<input type="checkbox"/> Barkley	Jeffrey	jeffreybarkley+MyCompanyN...	Administrator PRIMARY	Site 1 Site 2
<input type="checkbox"/> Barkley	jeffrey	jeffrey.barkley@motorolasolu...	Viewer	Site 1

When you select the user you see their detailed information.



AVIGILON

← User: Jeffrey Barkley

BASIC INFO

All fields are required except Phone.

First Name
Jeffrey

Last Name
Barkley

Email
jeffrey.barkley@avigilon.com

Phone

Timezone
(UTC-05:00) America/New_York

Role
Viewer

Status

SITE ACCESS & NOT

Filter

Site Access

Site 2

Site 1

NOTE: BY DEFAULT ACC USERS WHO ARE CONNECTED TO ACS ARE ASSIGNED THE ROLE VIEWER. THE VIEWER ROLE CAN ONLY VIEW LIVE AND RECORDED VIDEO.

Enabling Web Users

Q: After connecting my ACC site, how do ACC users gain access to the Avigilon Cloud Services Web Client?

A: ACC users must be given explicit web access privileges to use the Web Client by their ACC site administrator. The process is as follows:

- After an ACC site has been added to Avigilon Cloud services, users can be granted secure remote access to the site
- From the ACC Client:
 - Click the Users and Groups button in the Site Setup tab
 - Create a new user profile or open an existing one
 - Under Avigilon Cloud Services, add an email address to be used as the user's ACS login ID
 - Check the 'Connect' box and save the profile
 - Existing group privileges will apply to Web Client viewing
- Users will receive an email inviting them to set a password for their ACS account. The link will expire in 24 hours. If it expires the ACC administrator need to toggle the "Connect" checkbox to send a new invitation

Q: What do I do if the link in my email token expires before I use it?

A: Contact the administrator of your ACC to toggle the checkbox to cloud connect the user as follows:

- From the ACC Client:
 - Click the Users and Groups button in the Site Setup tab
 - Create a new user profile or open an existing one
 - Under Avigilon Cloud Services toggle the checkmark on the 'Connect' box of and on then save the profile
 - Existing group privileges will apply to Web Client viewing

Users will receive an email inviting them to set a password for their ACS account. The link will expire in 24 hours. If it expires the ACC administrator need to toggle the "Connect" checkbox to send a new invitation

Q: In the ACC Client, I see two new user groups - Cloud Administrators and Cloud Viewers. What are these for?

A: These two groups are reserved for the ACS users who are administrators. These administrators have a few functions:

- Generating Activation Codes on the ACS platform
- Re-sending ACS email invitations to ACC users who's invitation have expired
- Resetting the ACS passwords for ACC users

Q: ACC Enterprise Edition can be set-up to automatically synchronize users with Active Directory using LDAP. If a domain user changes their domain password, it is automatically synced to ACC, does it also synchronize this password with ACS?

A: No, this is a planned enhancement. Today there is no synchronization between ACC password and the ACS password. The ACS password will expire every 90 days. You will receive an email before it expires. If you have not changed the password before it expires you will be sent an email to set the password when you attempt to login to ACS.

System Health Monitoring

Q: Is there a charge or fee for System Health Monitoring?

A: There is no additional charge for end-users to access basic System Health Monitoring. Dealer access to System Health requires a paid subscription to the upcoming Advanced System Health package.

Q: What user roles can see System Health Monitoring?

A: To view the System Health Dashboard you must be assigned an ACS Administrator or ACS Manager role.

Q: As a Dealer / Integration how do I access the system health report for my customers?

A: Dealer access to System Health requires a paid subscription to the upcoming Advanced System Health package. The advanced package will include System Health monitoring across multiple customer sites, health event notifications, scheduled activities such as software downloads, configuration backups, and system health reports. Dealers can currently preview the System Health dashboard by navigating into one customer at a time using the top-left organization selection dropdown. They can then access the end-user's System Health Dashboard.

Q: Can I generate a system health report?

A: Yes, you can export a Site Health Report as a CSV formatted file. ACS will store one file per site on your local drive. It will include Site, Server, and Camera licensing and configuration information for a single site.

Q: Can I check the firmware version of a server or camera?

A: Yes, if you are only interested in a single device you can select the specific server and camera to view the device details. If you want it for all devices on an entire site you can export a Site Health Report as a CSV formatted file. ACS will store one file per site on your local drive. It will include Site, Server, and Camera licensing and configuration information.

Q: Can I review or audit that my recording policies are being followed?

A: Yes, you can access this information from the server details page under the Storage Analysis tab and ensure recording policies are being met to follow local Privacy laws and regulations. For every camera review:

- Whether camera recording is active
- Number of days of video retention (Requires minimally ACC 7.6.2)
- Heavy storage usage outliers
- Click to review camera configuration

Configuration Considerations

Q: What is the performance impact to a live ACC system when using the Web Client?

A: The risk of affecting performance of a running ACC site is low. The functionality is all client side within the browser on the client computer. A single web-client user places a similar performance load on the ACC server as an ACC Mobile 3 user since both interface to the server through the ACC Web Endpoint Service.

Q: What are the network security risks to a live ACC system when connecting to the Avigilon Cloud Platform?

A: The ACC site remains secure. Communications between the cloud and ACC server uses WebRTC signaling, a technology that is often used for Video Conferencing applications. This feature is capable of firewall traversal and uses a secure tunnel to protect the communications. In most cases, no firewall setting changes should be required.

Q: What are the network / Firewall requirements for the server at the ACC site to cloud communications?

A: The ACC WebEndpoint establishes a relationship and connects to the Avigilon Cloud Service when enabled from the ACC Client. Once connected, the Web clients use WebRTC protocol to access video from any ACC site with minimal firewall reconfiguration. Specifically, it is not necessary to enable web clients on the internet direct access into the network running the ACC server. The following are the minimum requirements:

- The ACC server must be capable of initiating an outbound connection from the ACC host to the Internet on HTTPS port 443. Connections are negotiated using trusted Certificates and traffic is encrypted using TLS. In most cases, no firewall changes should be required.
- Web Browser clients initiate a connection to the Avigilon Cloud Service Platform on the standard HTTPS port 443. All traffic on this connection is encrypted using TLS.
- When streaming video, browser clients create a direct peer-to-peer connection to the ACC server. This connection is secured using TLS and trusted certificates. This connection is negotiated using WebRTC signaling on Port 443 and depending on your network firewall configuration may use:
 - Port 1025-65535 (TCP) for Session Traversal Utilities for NAT (STUN)
 - Port 3478 or 443 (UDP or TCP) for Traversal Using Relays around NAT (TURN)
- If only Port 443 is open, then remote sessions will use TURN on Port 443. If the Web Client is visible on the internal network to the ACC host, it will use a direct connection over Port 443 without TURN.

Q: We have strict firewall policies requiring whitelisting servers, what are the explicit services used?

A: Avigilon Cloud Services are hosted at the follow IP addresses:

- Azure Web Services - TCP port 443
 - US: us.cloud.avigilon.com
 - CA: ca.cloud.avigilon.com
 - AU: au.cloud.avigilon.com
- Azure IoT Hub - TCP port 443
 - US: blue-prodeastus01-iot-hub.azure-devices.net
 - CA: blue-prodcentralca01-iot-hub.azure-devices.net
 - AU: blue-prodeastau01-iot-hub.azure-devices.net
- Azure Blob Storage - regional IP address mentioned above
- Aply - TCP port 443 for IP address that may change without notice
- PubNub - TCP 443 for IP address that may change without notice

- Twilio (WebRTC) - TCP 443 for IP address that may change without notice
- Google Analytics - TCP 443 for IP address that may change without notice

Troubleshooting

Q: What should I do if I receive the message “Avigilon Cloud Services is temporarily unavailable” when trying to connect ACC to ACS?

A: While trying to connect, or when clicking the cloud connect button on the ACC client Site Setup tab, if the dialog responds that the “Avigilon Cloud Services is temporarily unavailable” it can be due to several reasons:

- The version of ACC that is installed does not meet the minimum version of ACC 7.4.4.14. NOTE: If the ACC site is a cluster all servers in the cluster should be running the same version.
 - Upgrade to ACC 7.4.4.14 or higher before attempting to connect to ACS
- The ACC Web Endpoint Service is not installed, is not running or it has not been upgraded to the current version. NOTE: ACC and Web Endpoint should be the same version for all servers at the site.
 - Manually restart or uninstall and reinstall the ACC Web Endpoint Service
- Firewall or antivirus is interfering with outbound communications. See question about network / Firewall requirements above.
- The Avigilon Cloud Service is refreshing during a maintenance window.
 - Most maintenance activity is completed in less than an hour

Q: What should I do if I do not see any cameras in the ACS camera tree?

A: If the ACC site has been successfully connected to the ACS platform and from the web client View Tab you do not see your connected cameras in the camera tree:

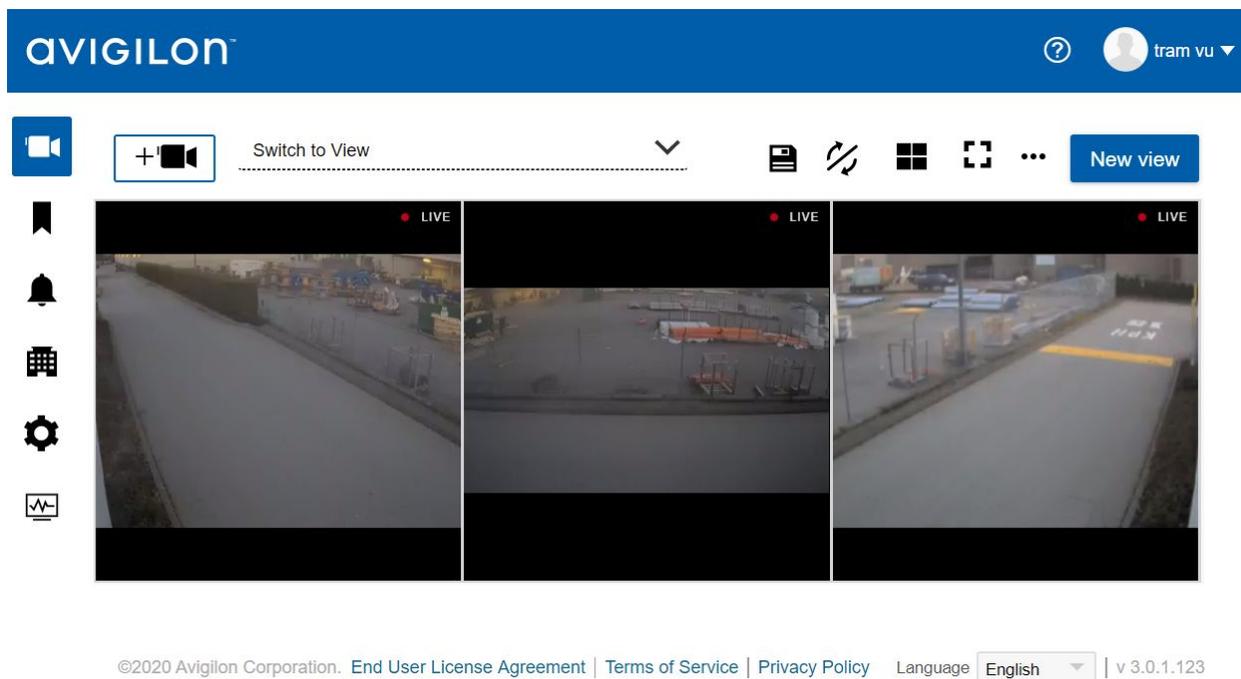
- Click on the information icon (i) next to the site name in the camera tree to reveal the connection diagnostic window. A red exclamation mark will appear if there are issues with the connection to the ACC site.
 - Connection is not open. Gone. (410)
 - You are not using a supported browser. Switch to a supported browser.
 - Error initiating p2p connection. Gateway timeout. (405)
 - Your ACC site is not communicating with ACS. If this is a stand-alone server, contact your administrator to ensure the ACC web endpoint service is running or is upgraded to match the ACC release. In addition, if the site is a cluster of ACC servers, have your administrator contact Avigilon Customer Support.
 - Authentication Failed
 - Your user account is not linked to any user account on the ACC server. Contact your administrator to investigate and potentially restart the ACC Web Endpoint process to resynchronize users accounts.
 - Permission Denied
 - Your user account does not have permission to access the device. Contact your administrator to update your user privileges using the ACC client.

Q: I don't see System Health Monitoring?

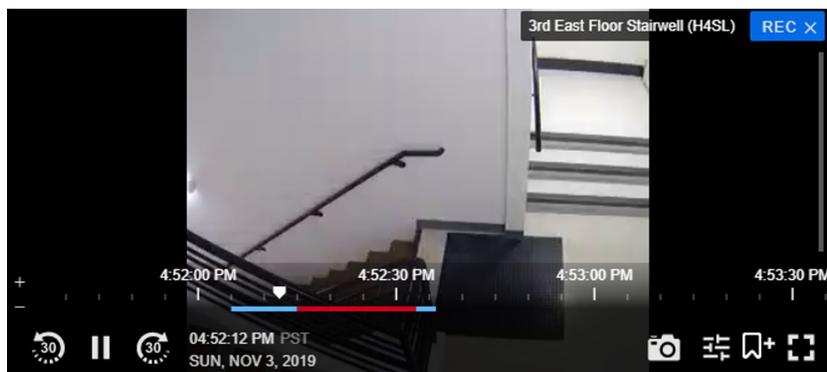
A: To view system health you must be assigned an ACS Administrator or Manager role. Have an ACS Administrator check your role and if necessary and appropriate change your role.

ScreenShots

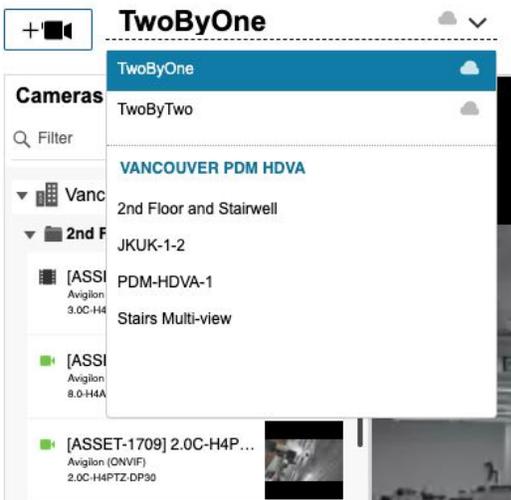
ACS View Tab



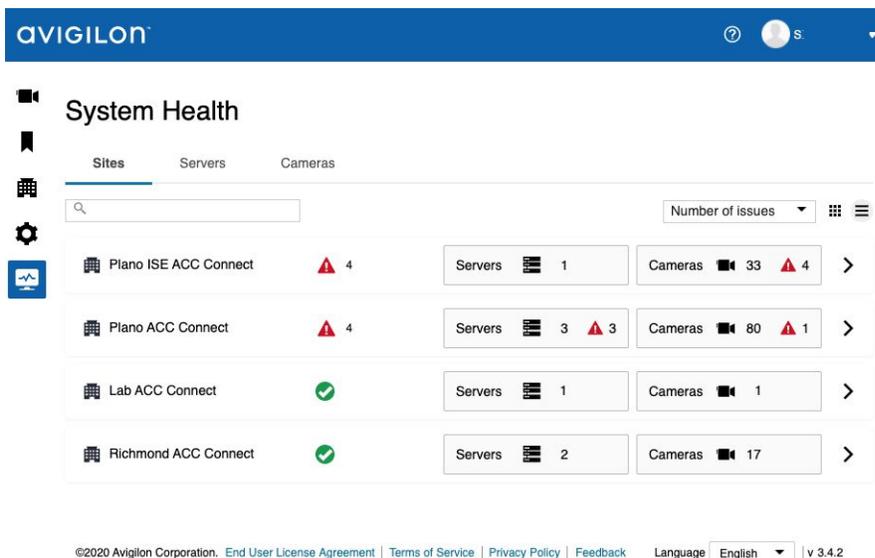
Recorded Video playback with color-coded timeline, bookmark creation and review, Video Snapshot, MP4 video export



Recall Saved View from ACC server or create new personal views saved to ACS servers



System Health Monitoring Main Tab Site View



System Health Monitoring Main Tab Server View

AVIGILON
?
S

System Health

Sites Servers Cameras

Filter

Device	Status	Duration	Site	IP address	MAC address
01 - Plano Main	DISCONNECTED	364:28 Hours	Plano ACC	Unknown	Unknown
02 - Plano Failover	DISCONNECTED	1109:55 Hours	Plano ACC	Unknown	Unknown
01 - Richmond Main	CONNECTED	7:35 Hours	Richmond AC..	Unknown	Unknown
02 - Richmond Failover	CONNECTED	0:48 Hours	Richmond AC...	Unknown	Unknown

©2020 Avigilon Corporation. [End User License Agreement](#) | [Terms of Service](#) | [Privacy Policy](#) | [Feedback](#) Language: English | v 3.4.2.3

System Health Monitoring Server Details

AVIGILON
?
S

←Server: 01 - Richmond Main

Details Storage Analysis

General Information

Server Version	IP Address	Model	Service Tag
7.6.0.22.106897	Unknown	Unknown	Unknown

CPU Load	Memory Usage	System Available Memory	Up Time
4%	Unknown	24488.2 MB	6 days, 21 hours, 50 minutes

Analytics Service	Peak Load (Last 3 Days)	Site License Usage
Unavailable	Unknown	Camera Channels: 7/64 POS Sources: 0/0

Network Adapters

Adapter Name	Status	Link Speed	IP Address	Incoming	Outgoing
NIC3	Up	1 Gbps	10.20.50.2	0.18 Mbps	0.22 Mbps
NIC4	Up	1 Gbps	169.254.211.60	79.62 Mbps	0.41 Mbps
NIC2	Down	10 Gbps		0 Mbps	0 Mbps
NIC1	Down	10 Gbps		0 Mbps	0 Mbps

©2020 Avigilon Corporation. [End User License Agreement](#) | [Terms of Service](#) | [Privacy Policy](#) | [Feedback](#) Language: English | v 3.4.2.3