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) offers a browser-based client to view live and recorded video from Avigilon Control Center (ACC) sites. 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 without any configuration.

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.

Prerequisites **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: If I am using ACS how do I add my ACC sites to the ACC Mobile 3 app? 4
Q: Which Avigilon mobile app should I use for cloud-connected ACC sites? 4
Q: What are the Privacy Considerations for using ACS? 4
Q: Where is my ACS data stored? 4

Cloud-Connecting ACC sites **5**
Q: How do I cloud-connect my ACC server to Avigilon Cloud Services? 5
Q: How do I register my organization using the ACS web client? 5
Q: How do I register an organization using the ACS Web Client? 5
Q: How do I add an ACC site to an organization using an activation code? 6
Q: What do I do if the activation code for my site expires? 6
Q: What happens if my ACC user account has been registered with multiple organizations? 6
Q: What is a primary administrator on ACS? 6
Q: Can I change the primary administrator for an organization? 6
Q: How do I change a user's ACS role? 7

Enabling Web Users **8**
Q: After connecting my ACC site, how do ACC users gain access to the ACS Web Client? 8
Q: What do I do if the link in my email token expires before I use it? 8
Q: Why does the ACC Client have two new user groups - Cloud Administrators and Cloud Viewers? 9
Q: My ACC Enterprise Edition synchronizes users with Active Directory. If a user changes their domain password is it automatically synced to both ACC and ACS? 9
Q: If I already have an organization on ACS when I federate will I need to create a new organization? 9
Q: If I federate with ACS does it assign that user to group for authorization similar to ACC? 9
Q: If I federate my identity provider will ACS will I still have to change my password every 90 days? 9
Q: Can I use multi-factor authentication with ACS? 9

System Health Monitoring **10**
Q: Is there a charge or fee for System Health Monitoring? 10
Q: What user roles can see System Health Monitoring? 10
Q: As a Dealer / Integration how do I access the system health report for my customers? 10
Q: Can I generate an inventory audit or site health report like in ACC client? 10

Configuration Considerations **11**
Q: What is the performance impact to a live ACC system when using the Web Client? 11
Q: What are the network security risks to an ACC system when connecting to ACS? 11

Q: What are the network port requirements for the server at the ACC site to cloud communications? 11
Q: We have strict firewall policies requiring safelisting servers, what are the explicit services used? 11
Q: Which data center is used to relay my video traffic when TURN is required? 12
Q: Can I use IPv6 Addresses? 12

Security Considerations **13**
Q: How do I limit ACS user access to cameras on a site? 13
Q: How has ACS and ACC been evaluated for security vulnerabilities? 13
Q: Does ACS encrypt cloud data? 13
Q: Does ACS encrypt or hash passwords? 13
Q: Are ACS emails DMARC-compliant? 13

Troubleshooting **14**
Q: I received the message “Avigilon Cloud Services is temporarily unavailable” when connecting ACC to ACS? 14
Q: What should I do if I do not see any cameras in the ACS camera tree? 14
Q: I don’t see the System Health icon? 14
Q: I don’t see the Reports icon to review the COVID-19 Response Dashboard? 14
Q: A user is unable to view cameras the user sees the message "Invalid username or password, 401 error" 15

ACS Web Client ScreenShots **16**
Views Tab 16
Views Tab - Recorded Video 16
Views Tab - Recall saved views 17
System Health Monitoring Site Summary 17
System Health Monitoring Server Summary 18
System Health Monitoring Server Details 18
Reports - COVID-19 Response Dashboard 19

Prerequisites

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 7.10 or higher.
- If not installed, install ACC Web Endpoint Service of the same version as ACC on each server.
- The ACC 6 Gateway component is not required to be installed nor running.

Q: What are the system requirements for computers using the Web Client?
A: To use the web client the device must have a recent version of a supported web browser:

- Google Chrome 72+
- Apple Safari 12.1+, or
- Microsoft Edge 83+.

Microsoft Windows, Apple MacOS, and Chromebooks devices with mid-grade graphics chips are compatible. The mobile web browsers on most mobile phones and tablets are **not** formally supported. We suggest using the ACC Mobile 3 app if you want to use a mobile device.

Q: Are there any new ACC licenses required to use the Web Client?
A: No, access to the ACS Web Client is free for all ACC editions (Core, Standard, Enterprise).

Q: If I am using ACS how do I add my ACC sites to the ACC Mobile 3 app?
A: ACC Mobile 3 app supports signing in using ACS or corporate 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 Blue Mobile 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 ACS?
A: Avigilon Cloud Services does not store any video in the cloud. All video travels in the secure encrypted point-to-point connection between the 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.

Q: Where is my ACS data stored?
A: When your administrator registered your organization with ACS they first selected a region on cloud.avigilon.com. Choosing:

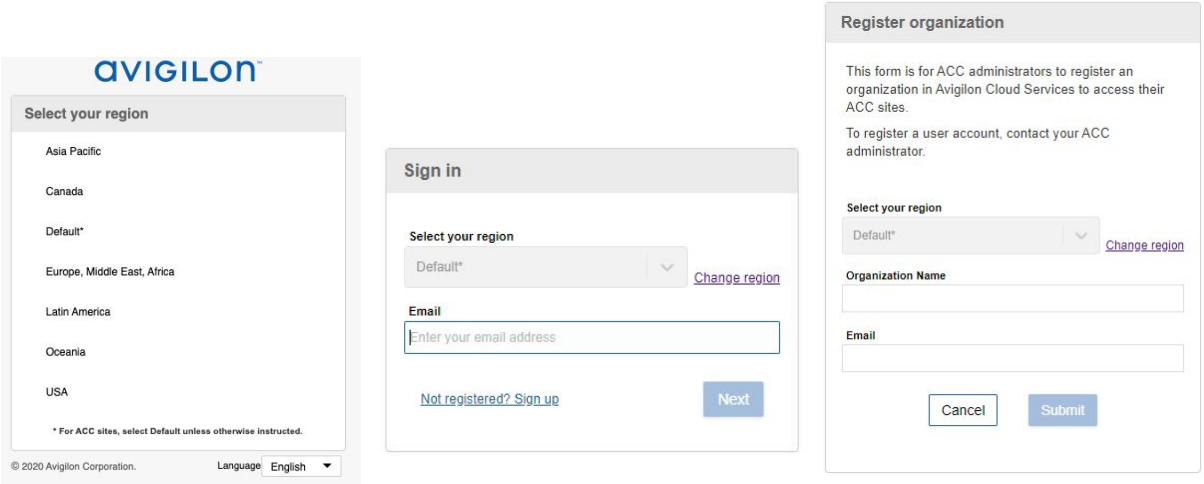
- the default region will create your organization in Microsoft Azure servers in the United States
- Asia Pacific or Oceania will create your organization in Microsoft Azure servers in Australia, and
- Canada, Europe, Middle East and Africa or Latin Americawill create your organization in Microsoft Azure servers in Canada.

Cloud-Connecting ACC sites

Q: How do I cloud-connect my ACC server to Avigilon Cloud Services?
A: You can self-register your organization with ACS and add your ACC site(s); Start at cloud.avigilon.com, select your region and register your ACC sites under a common organization name.

Q: How do I register my organization using the ACS web client?
A: An administrator should first register on organization name with ACS. Once you have a registered organization, you can add ACC sites to the organization using an activation code. Organizations with multiple sites can enable their users of the ACS web client or ACC Mobile 3 app to access all or only selected ACC sites without needing to switch between ACC sites. The ACC Mobile 3 app will receive mobile notifications from only the sites the user is allowed to access in the organization.

Q: How do I register an organization using the ACS Web Client?
A: Go to cloud.aviglon.com and select a region and click "Register now" to create your organization and primary administrator account.



Choosing:

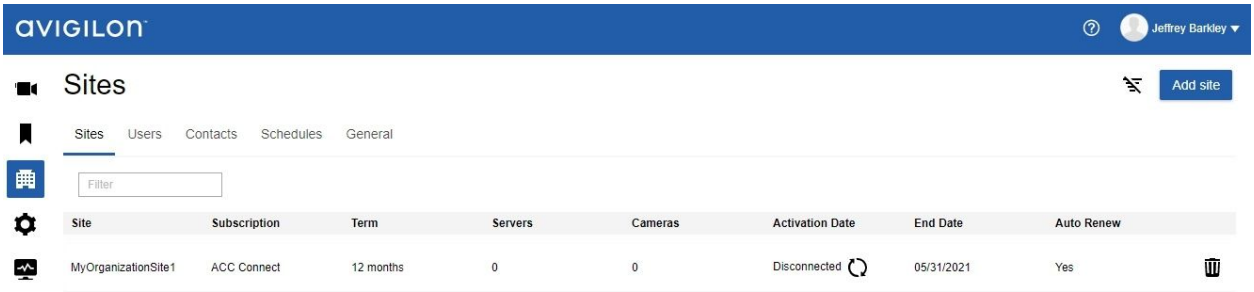
- the default region will create your organization in Microsoft Azure servers in the United States
- Asia Pacific or Oceania will create your organization in Microsoft Azure servers in Australia, and
- Canada, Europe, Middle East and Africa or Lati Americawill create your organization in Microsoft Azure servers in Canada.

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

Wait for the email confirmation email from ACS with a link to activate your organization. Complete the registration by clicking on the link in the email and setting your user password. You must complete this process within 24 hours or the link will expire.
IMPORTANT: DO NOT CANCEL OR EXIT AVIGILON CLOUD SERVICES DIALOG UNTIL SUCCESSFUL COMPETING ACTIVATION.

Q: How do I add an ACC site to an organization using an activation code?
A: After registering an organization with ACS, login with your administrator account and 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 the administrator can go to the Site Setup > Avigilon Cloud Services settings and enter the code.

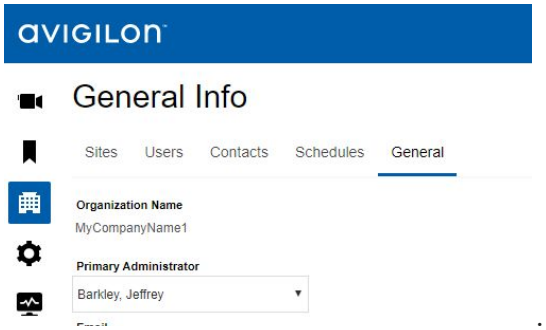
Q: What do I do if the activation code for my site expires?
A: An ACS administrator can regenerate a code on the sites tab by clicking the refresh icon next to expired and provide the new code to the ACC administrator.



Q: What happens if my ACC user account has been registered with multiple organizations?
A: From the Web Client or ACC Mobile 3 app, you must select one organization with which to interact. An organization can consist of a single server or multiple servers. 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 only from the selected organization.

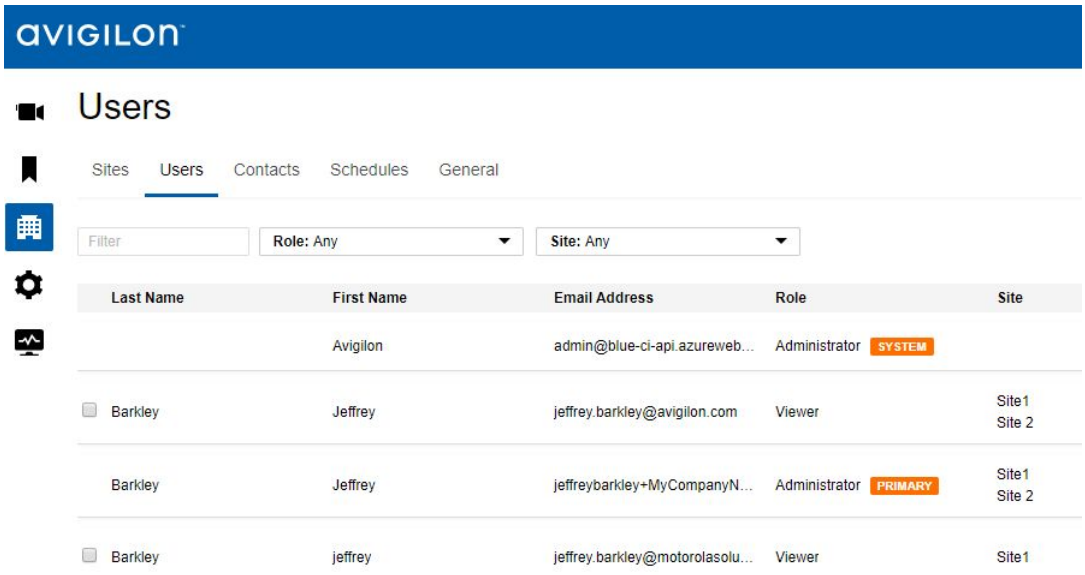
Q: What is a primary administrator on ACS?
A: Every ACS organization has a primary administrator. The primary administrator is notified of changes to the ACS organization. The user that created the organization will by default be the primary administrator.

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 .

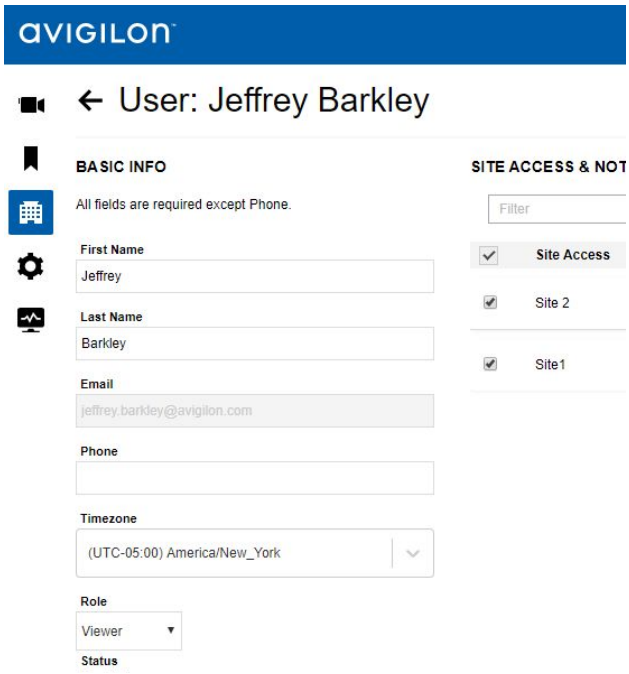


If you do not have any other users with the administrator, role no other users will show up in the list. RECOMMENDATION: Avigilon recommends at all times you have at least two ACS users with an Administrator role.

Q: How do I change a user's ACS role?
A: Only ACS administrators 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.



When you select the user you see their detailed information.



NOTE: BY DEFAULT ACC USERS WHO ARE CONNECTED TO ACS USING THE ACC CLIENT ARE ASSIGNED THE ROLE VIEWER IN ACS. 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 ACS Web Client?
A: ACC users must be given explicit to ACS by their ACC site administrator. The process is 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, 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 viewing video

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: Why does the ACC Client have two new user groups - Cloud Administrators and Cloud Viewers?
A: These two groups are reserved for users created using the ACS Web Client:

- Cloud Administrators is for ACS users who have the role administrator or manager
- Cloud Viewers is for ACS users who have the role responder or viewer

Q: My ACC Enterprise Edition synchronizes users with Active Directory. If a user changes their domain password is it automatically synced to both ACC and ACS?
A: ACC Enterprise Edition users who are synchronizing their ACC users with Active Directory can federate their users with ACS so that domain users will use their domain password with both ACC and ACS. If the end-user organization has their domain in Azure Active Directory then they are all set and can federate with ACS. Many customers already have the active directory in Azure because they are using a Microsoft cloud product. For example, customers who are using Office 365 are using Azure AD.

If the customer does not have their domain in Azure Active Directory -- Microsoft offers Azure AD Connect to allow them to sync their on-premise active directory with Azure. Once they are using Azure AD they can federate with ACS and other Azure cloud-based applications.

Q: If I already have an organization on ACS when I federate will I need to create a new organization?
A: No, when you federate your organization behind the scenes the original ACS only passwords expire and the next time the user logs-into ACS it uses the federated identity provider instead of ACS for authentication.

Q: If I federate with ACS does it assign that user to group for authorization similar to ACC?
A: No, when you add a federated user to ACS you will assign them to one of the predefined ACS roles for their ACS authorization.

Assuming you are synchronizing Active Directory with ACC it will continue to work the same way that it has in the past adding the user and assigning them to the group in ACC. You can sync your ACC users with ACS by selecting the checkbox. If you have federated the user's email domain on ACS then they will use the same password on both ACC and ACS.

Q: If I federate my identity provider will ACS will I still have to change my password every 90 days?
A: No, when you federate a user with ACS, the policies of the identity provider are what are enforced, password complexity, age, etc. not the ACS policy.

Q: Can I use multi-factor authentication with ACS?
A: Yes if you federate ACS with your identity provider your company can use any multi-factor authentication policy supported by that identity provider.

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 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 an inventory audit or site health report like in ACC client?
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 as indicated by the bandwidth usage
- Number of days of video retention (Requires minimally ACC 7.6.2 installed on the ACC server)
- Heavy storage usage outliers
- Click camera 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 though the ACC Web Endpoint Service.

Q: What are the network security risks to an ACC system when connecting to ACS?
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 port 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. The following are the minimum requirements:

- The ACC server must be capable of initiating an outbound connection from the ACC server 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 Avigilon Cloud Services on the HTTPS port 443. All traffic on this connection is encrypted using TLS.
- When streaming video, browser clients and mobile 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 49152 - 65535 (TCP) for Session Traversal Utilities for NAT (STUN)
    - Port 3478 (UDP or TCP) for Traversal Using Relays around NAT (TURN). If only Port 443 is available, then remote sessions will use TURN on Port 443 rather than Port 3478. 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.
- When streaming video to a third party integration that uses the ACS media API to get RTSP streams will use Port 1935 outbound.

Q: We have strict firewall policies requiring safelisting servers, what are the explicit services used?
A: Avigilon Cloud Services uses both Microsoft Azure and third party services to deliver its feature set. Operators who do not wish to provide remote access to video, but want to review System Health from multiple remote sites, or receive security and health events from sites need only add Firewall rules for Microsoft Azure at the following fully qualified domain name (FQDN) locations.

The listed IP addresses may change without notice but can be verified through DNS lookup. The three Azure services listed below are required to establish base system communication, system health heartbeats, and event notifications:

- Azure Web Services - TCP port 443
  - US region: us.cloud.avigilon.com (52.179.97.15)
  - Canadian region: ca.cloud.avigilon.com (40.85.212.173)
  - Australian region: au.cloud.avigilon.com (13.75.218.45)
- Azure Blob Storage - TCP port 443
  - US region: blueprodeastus01ops.blob.core.windows.net (52.239.154.100)
  - Canadian region: blueprodcentralca01ops.blob.core.windows.net (40.85.235.62)
  - Australian region: blueprodeastau01ops.blob.core.windows.net (13.75.240.84)
- Azure IoT Hub - TCP port 443
  - US region: blue-prodeastus01-iot-hub.azure-devices.net (40.114.53.146)
  - Canadian region: blue-prodcentralca01-iot-hub.azure-devices.net (52.237.27.123)
  - Australian region: blue-prodeastau01-iot-hub.azure-devices.net (104.210.105.7)

Avigilon Cloud Services uses messaging hubs to facilitate negotiation of secure media access. Ably and Pubnub services are used for WebRTC signalling and Twillo provides TURN media relay services. These are required to view live or recorded video on the ACS Web Client or the ACC Mobile3 App.

- Ably - TCP port 443
  - REST requests - rest.ably.io
  - Realtime (WebSocket) connections - realtime.ably.io
- PubNub - TCP port 443
  - ps.pndsn.com
- Twilio (WebRTC) - TCP port 443
  - global.turn.twilio.com

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

Q: Which data center is used to relay my video traffic when TURN is required?
A: Twilio Network Traversal Services are used when TURN is required, Twilio automatically selects the closest point-of-presence to the user.

Q: Can I use IPv6 Addresses?
A: No, Microsoft Azure IoT Hub does not support IPv6 addresses
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-understand-ip-address#support-for-ipv6

Security Considerations

Q: How do I limit ACS user access to cameras on a site?
A: The camera access rights are controlled by the ACC server and not by ACS. Depending on if the users are created in ACC or ACS you can limit a users access by making sure the user has the desired rights on ACC.

If the users are created in:

- ACC or from Active Directory integration ACS users will have camera access rights based on the ACC users group membership. When you synchronize the user to ACS using the Connect check box in the edit user dialog, the ACS user will have the same camera access ast they have on ACC.
- ACS and then are synced to ACC they are assigned membership of one of two ACC user groups:
    - Cloud Administrator or
    - Cloud Viewer

  to change the default camera access rights on ACC:
    - Step 1; remove all camera access privileges for these two Cloud groups;
    - Step 2; add the ACS user to an existing ACC group with the desired camera access rights.

Q: How has ACS and ACC been evaluated for security vulnerabilities?
A: Avigilon's design, coding, coding review and scanning practices take every care possible to avoid any of the OWASP top 10 or SANS top 25 vulnerabilities. Avigilon runs complete scans of ACS and ACC with standard tools for every release. Among the tools we use for testing and code scanning for ACS are Tenable Nessus, Blackduck, OWASP ZAP, Trustwave.

While Avigilon does not release the results of these internal tests any issues are handled by the Avigilon Product Security Incident Response Team (PSIRT).

Q: Does ACS encrypt cloud data?
A: Data is encrypted-at-rest using Azure Storage Service Encryption (SSE) which uses 256-bit Advanced Encryption Standard (AES) encryption. Azure Storage automatically encrypts data prior to persisting to storage and decrypts prior to retrieval. The encryption, decryption, and key management are totally transparent to users.

Q: Does ACS encrypt or hash passwords?
A: For users that use ACS's native identity management it uses Argon 2 to hash passwords. If the user account is federated then no password is stored in ACS. According to wikipedia Argon2 is a key derivation function that was selected as the winner of the Password Hashing Competition.

Q: Are ACS emails DMARC-compliant?
A: ACS's emails are not DMARC-compliant. DMARC is Domain-based Message Authentication, Reporting & Conformance is a protocol that uses Sender Policy Framework, (SPF) and DomainKeys identified mail (DKIM) to determine the authenticity of an email message. DMARC makes it easier for Internet Service Providers (ISPs) to prevent malicious email practices, such as domain spoofing in order to phish for recipients' personal information.

Troubleshooting

Q: I received the message "Avigilon Cloud Services is temporarily unavailable" when connecting ACC to ACS?
A: While trying to connect your ACC site to ACS and the dialog responds "Avigilon Cloud Services is temporarily unavailable" it can be due to several reasons:

- Firewall or antivirus is interfering with outbound communications. See question about network requirements above.
- The version of ACC that is installed does not meet the minimum version of ACC 7.10. NOTE: If the ACC site is a cluster all servers in the cluster should be running the same version. Upgrade to ACC 7.10 or higher before attempting to connect to ACS again.
- The ACC Web Endpoint Service is not installed, is not running or it has not been upgraded to the current version on the server. ACC Web Endpoint should be installed on all ACC servers except the AI appliance. NOTE: ACC and Web Endpoint should be the same version for all servers at the site. You can use the ACC Site Health report to find the version and status of the Web Endpoint on all your servers. As necessary manually restart or uninstall and reinstall the ACC Web Endpoint Service

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 ACS and from the web client View Tab you do not see any 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. Some common issues and solutions are the following:

- Connection is not open. Gone. (410): You are not using a supported browser. Switch to a supported browser.
- Error initiating p2p connection. Gateway timeout. (504): 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. From the ACC Users and Groups dialog, uncheck "Connect" for the user, Apply, re-check "Connect" and Apply.
- Permission Denied: Your user account does not have permission to access the device. Contact your administrator to update your user camera access privileges using the ACC client.

Q: I don't see the System Health icon?
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.

Q: I don't see the Reports icon to review the COVID-19 Response Dashboard?
A: To view Reports you must be assigned an ACS Administrator or Manager role. Best practice is to assign the Manager role to report viewers, so they do not have administrative access. Separately, Report viewers with the ACS Manager role can be restricted from viewing video by using the ACC Client to assign the user

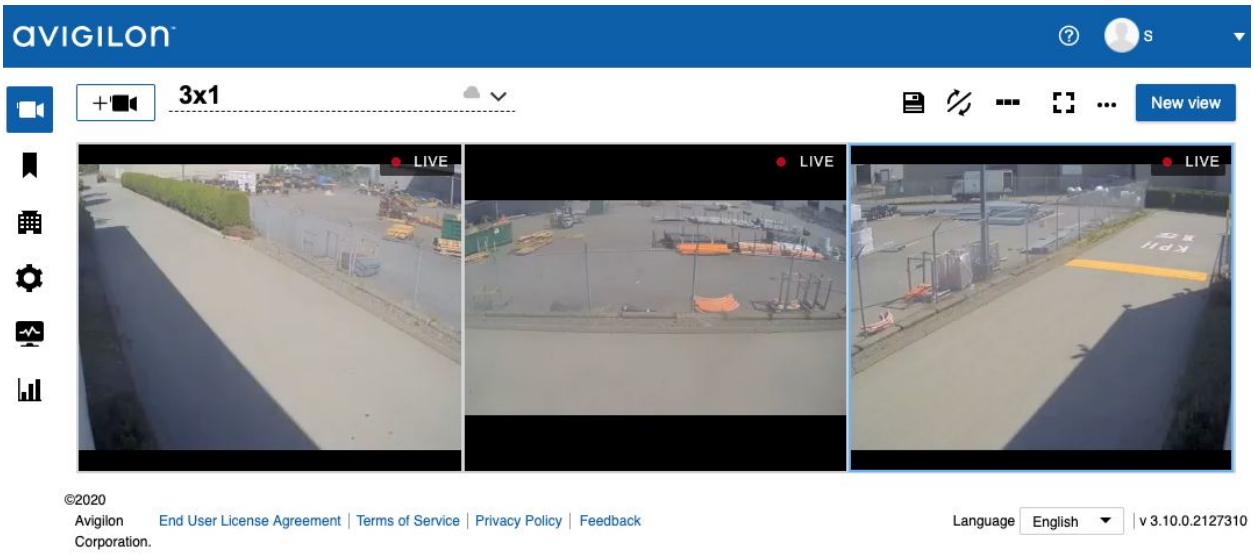
to an appropriate User Group with restricted video access. Have an ACS Administrator check your role and change your role as necessary.

Q: A user is unable to view cameras the user sees the message "Invalid username or password, 401 error"
A: This error comes from ACC as a result of incorrect time settings for the ACC server causing the ACS user authorization to be rejected. When connecting servers to ACS users should ensure that their ACC servers use a reliable NTP server such as:

- the United States National Institute of Standards and Technology (NIST) https://www.nist.gov/pml/time-and-frequency-division/services/internet-time-service-its
- The NTP Pool Project www.ntppool.org

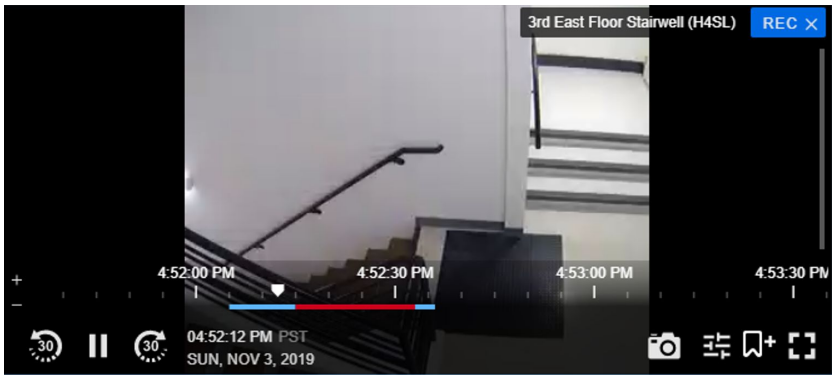
ACS Web Client ScreenShots

Views Tab



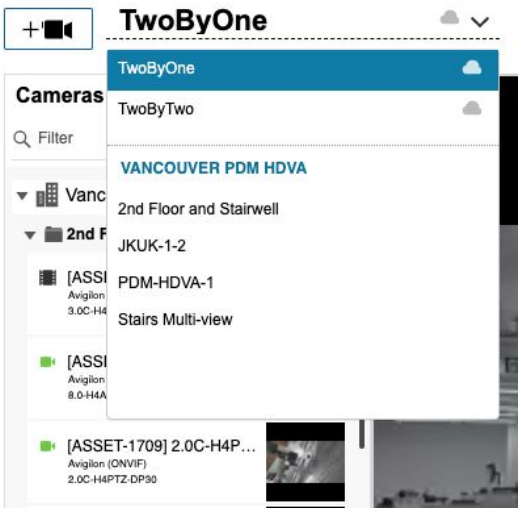
Views Tab - Recorded Video

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

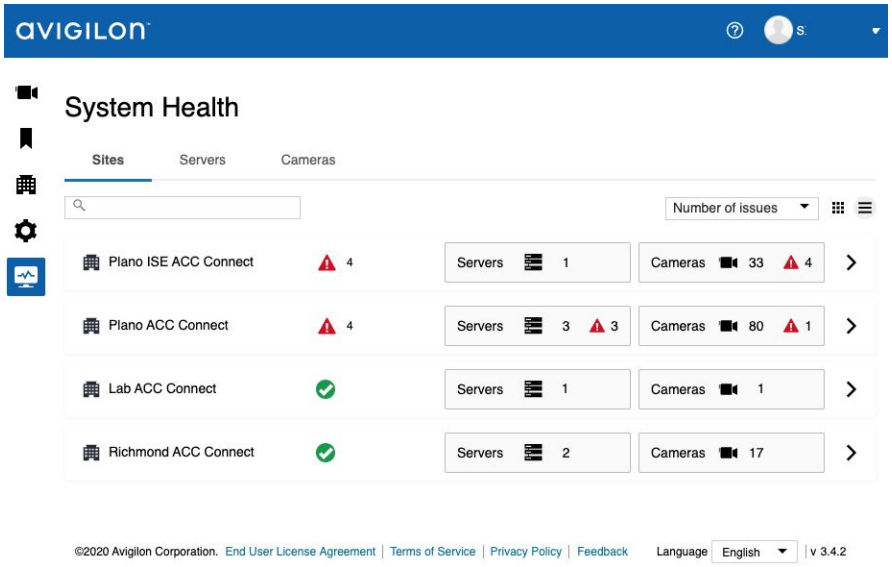


Views Tab - Recall saved views

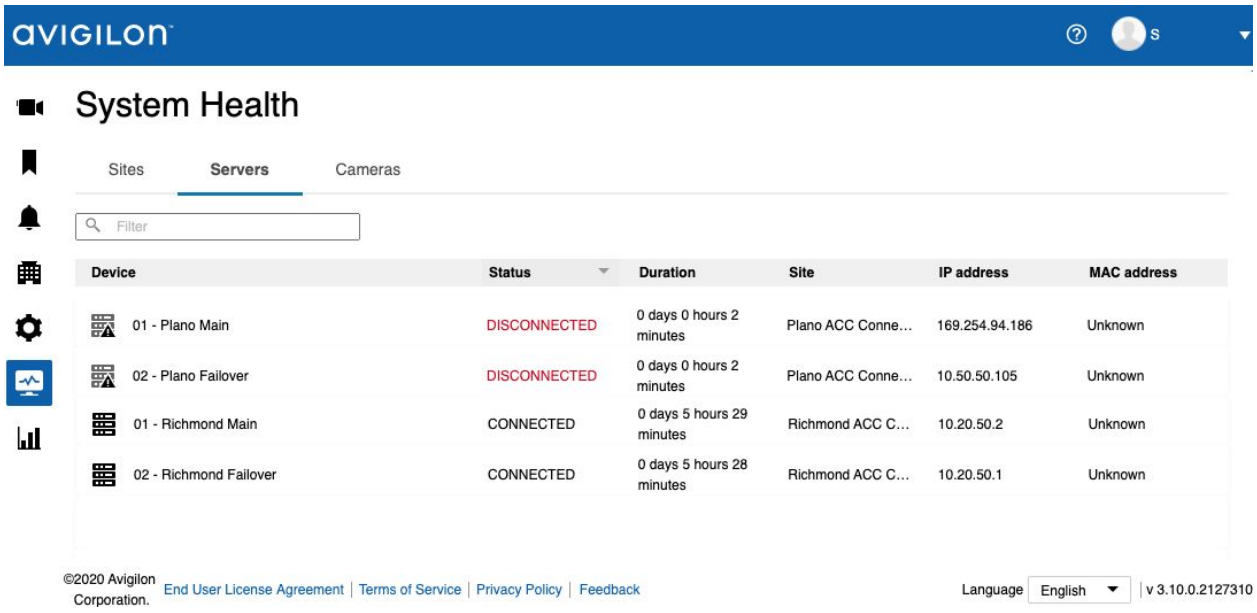
Saved View from ACC server or create new personal views saved to ACS servers



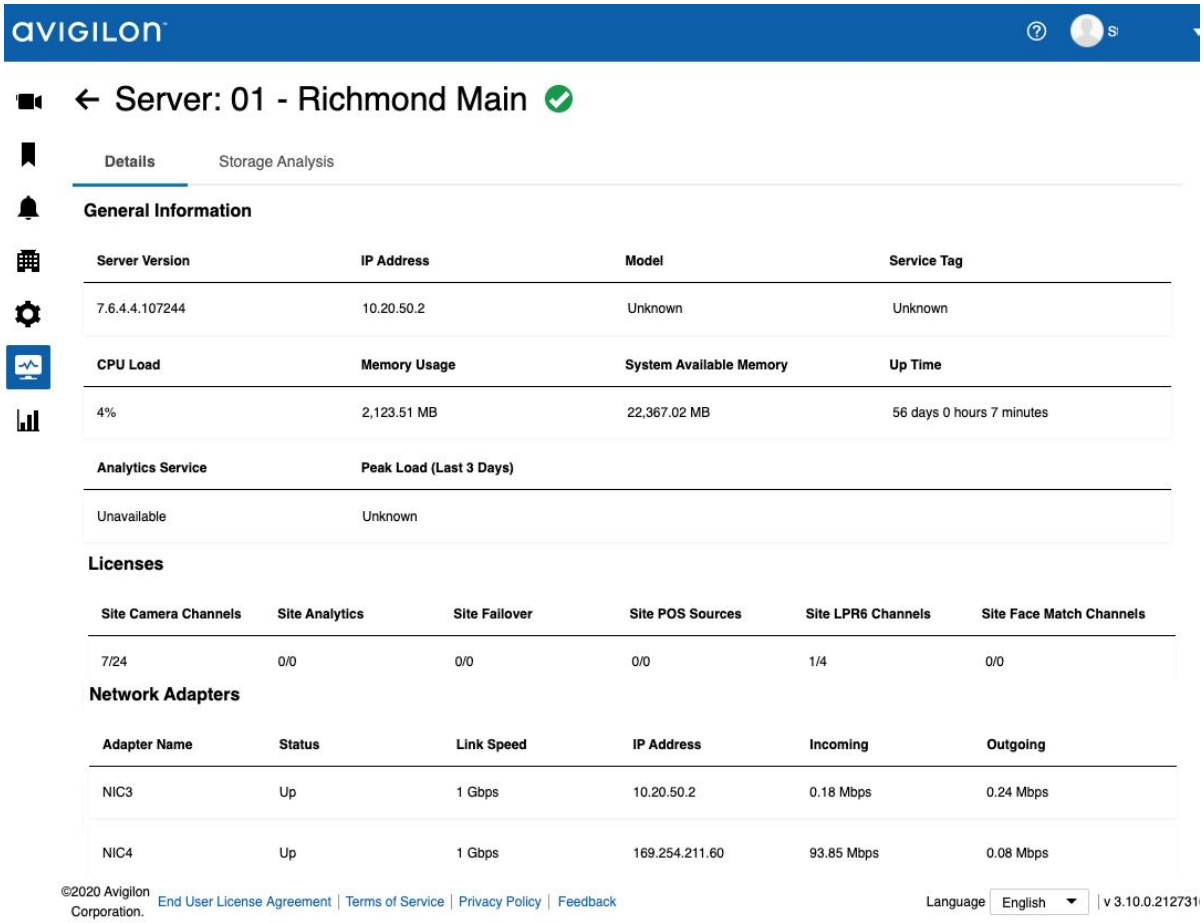
System Health Monitoring Site Summary



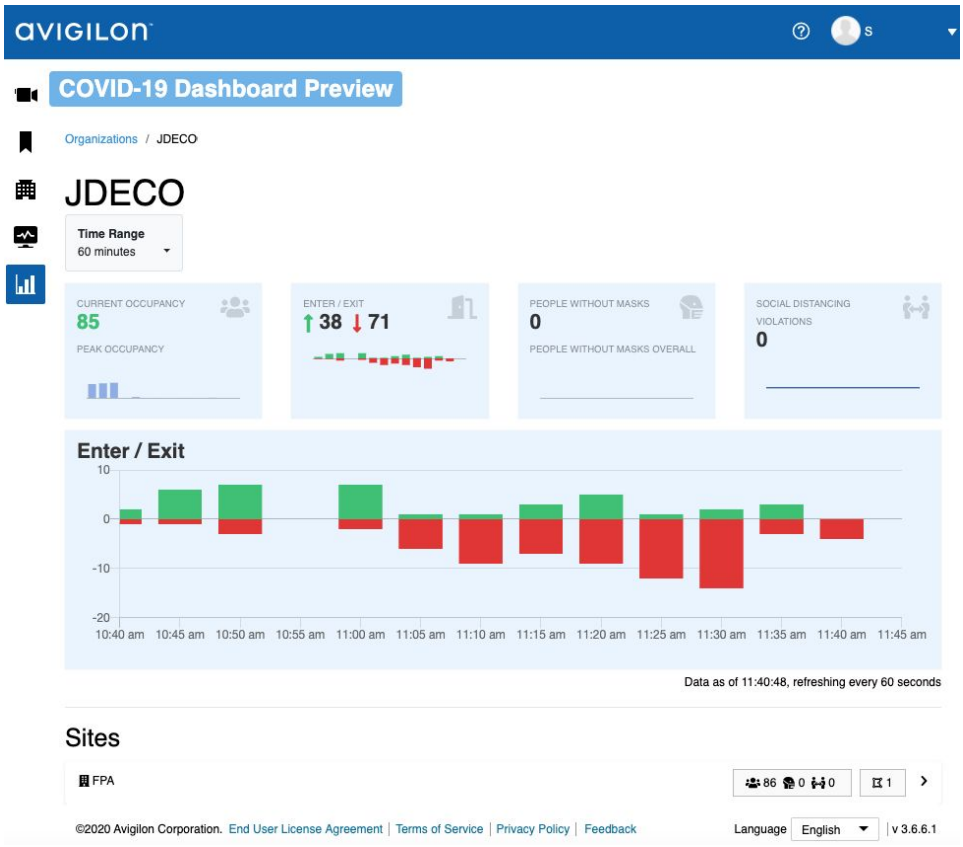
System Health Monitoring Server Summary



System Health Monitoring Server Details



Reports - COVID-19 Response Dashboard



EST. 1988 dts SOLUTIONS

HEAD OFFICE:
01480 407740
hello@dts.solutions
dts.solutions
@dts_solutionsuk
Barham House, Barford Rd,
St.Neots,
Cambridgeshire,
PE19 6YQ