AVIGILON™

H6A Camera Web Interface User Guide

Avigilon H6A, H6X, and H6XP IP Camera Models:

H6A-xxx
H6A-xxx-IR
H6X-xxx
H6X-xxx-IR

Copyright

Avigilon Corporation
avigilon.com

PDF-H6AWebUI-A

Revision: 1 - EN

20231018

Table of Contents

Introduction

Avigilon High Definition IP cameras include a web interface that allows you to view the live video and configure the camera through a web browser.

Before you access the web interface, make sure all the procedures described in the camera installation guide have been completed.

> **Tip:** Features and options are disabled if they are not supported by the camera.

System Requirements

The following browsers are recommended when accessing the web interface from any Windows, Mac, or mobile device:

- Mozilla Firefox version 96.0.2 (64-bit) or later
- Google Chrome™ version 97.0.4692.71 (64-bit, official build) or later
- Microsoft Edge version 97.0.1072.76 (64-bit, official build) or later

> **Note:** The web interface may work with older or unsupported browsers, but this has not been tested.

Other Web Interface Guides

Check out these other Web Interface Guides for other types of Avigilon cameras:

- **APD Sensor Web Interface Guide** — for Avigilon presence detectors.

Accessing the Camera Web Interface

After the camera has been installed, you need the camera's IP address to access the web interface. The IP address can be found in the following:

- The Avigilon Control Center (ACC) software — Open the Setup tab to see the details of the selected camera.
- Motorola Solutions' Camera Configuration Tool (CCT) — Go to the Network tab to see the details of the selected cameras.

Once you have the IP address, complete the following procedure to access the web interface:

Note: The web browser must be configured to accept cookies or the camera web interface will not function correctly.

1. On a computer with access to the same network as the camera, enter the camera's IP address into a web browser:

   http://*<camera IP address>*/

   For example: http://192.168.1.40/
2. You will automatically be prompted to enter your username and password to access the camera. If the device is in the factory default state and was manufactured after January 1, 2020, you will be asked to create a user with administrator privileges before the device will be operational. For more information, see *Creating the Initial User and Logging In* on page 1.

Creating the Initial User and Logging In

New cameras do not have a default username and password and will be in a factory default state.

Important: You must create a user with *administrator* privileges before the camera is operational.

When logging into the camera for the first time, you will be redirected to the Add User page to create an administrator user:

1. Enter a new **User Name** or keep the default `administrator` name.
2. Enter a new **Password** for the user. We recommend using a complex and unique password. Avoid using an empty password as they are not supported across all platforms and devices.
3. Confirm the new password.
4. For the first user, *Administrator* must be selected in the **Security Group** drop-down menu.
5. Click **Apply**. After creating the user, you will be asked to login.

Live View

After you log in, the first page you see is the Live View. The Live View contains an image panel that displays the live video stream.

Use the menu links in the top-left corner to navigate through the web interface. Click **Live View** any time to return to this page.

> **Tip:** Features and options are disabled if they are not supported by the camera.

Saving a Still Image

If you see the **Save Still to SD Card** button from the Live View page, the camera supports the ability to take snapshots of live video from the web interface.

To use this feature, the following settings are required for the camera:

- There is an SD card inserted in the camera. For more information, see the camera's installation guide. Saving an image to the SD card is not supported if you are using FIPS Level 3 encryption with a CryptR micro card inserted in the SD slot.
- The camera's onboard storage settings are enabled on the Storage page. For more information, see *Storage* on page 20.
- The camera's video format must be set to MJPEG in the Compression and Image Rate page. For more information, see *Compression and Image Rate* on page 12.

Once all the requirements have been met, you can click **Save Still to SD Card** and the image that is displayed in the Live View page is automatically saved to the SD card.

To download the snapshot, see *Downloading Recorded Video from the Web Interface* on page 21.

Setup

Note: Certain options are not displayed if they are not supported by the camera model you are using or if you do not have the required user permissions.

The factory default settings allow you to use the camera or encoder immediately after installation. If you have special requirements, you can customize the settings through the web interface. In the top-left menu area, click **Setup** to display all the available setup pages.

A **Restore Defaults** button is available on each setup page to restore the factory default settings.

Be aware that some settings are only available through the camera's web interface and cannot be changed in the network video management software.

General

When you select Setup, the first page you see is the General page. The General page allows you to set the camera's identity.

Tip: Features and options are disabled if they are not supported by the camera.

Note: If a camera with video analytics or unusual motion detection is physically moved or adjusted, or if the focus or zoom level is changed, reset the learning progress to provide accurate results. If the camera's image rate and compression or display settings are updated, the learning progress may reset automatically.

1. In the **Name** field, give the camera a meaningful name.
2. In the **Location** field, describe the camera's location.
3. Select the **Disable device status LEDs** check box to disable the LED indicators located on the camera.
4. From the **Mode** drop-down list, select the mode that the camera will operate in.

   This option is only displayed for higher bandwidth usage cameras.

   - **Full Feature** — This is the standard operating mode. Offers the full functionality of the camera.
   - **High Framerate** — The 2MP and 4MP camera models have a High Frame Rate mode, allowing these cameras to reach higher frame rates while disabling analytics.

Models	Features Impacted by High Framerate
2 MP H6A Cameras 2 MP H6X Cameras 4 MP H6A Cameras 4 MP H6X Cameras	◦ Increased maximum frame rate ◦ Analytics disabled

   - **No Smart Analytics** — This mode will disable smart analytics. This option is for deployments where camera based video analytics would interfere with other analytics integrations.
5. Select any of the Overlay Setting check boxes to display and stamp that information on the camera's video stream. The options are:
   - **Display Date**

     Selecting the Display Date check box also enables the **Date Format** drop-down list. From the list, choose the date format which will be used to display the date.
   - **Display Time**

- **Display GMT Offset**
- **Display Name**
- **Display Location**

6. In the Time Settings area, select how the camera keeps time.
    - If you prefer to manually set the camera's date and time, enter the time zone on this page.
    - Select the **Automatically adjust clock for Daylight Savings Time** check box, if required.
    - If you prefer to auto-synchronize the camera's date and time with an NTP server, configure the NTP server on the Network page.

      At the bottom of the page, you can click on the (Configure NTP Server) link to go to the Network page. For more information on configuring the NTP server, see *Network* below.

    CAUTION — The time setting must always be current or the ACC software will reject the video stream from the camera. To ensure that the time is always current you should do one of the following:
    - Set up NTP on the DHCP server used by the ACC software.
    - Use a valid public NTP server.
    - Manually set the correct time in the Time Settings fields.
7. Click **Apply** to save your settings.

Network

On the Network page, you can change how the camera connects to the server network and choose how the camera keeps time.

1. At the top of the page, select how the camera obtains an IP address:
    - **Obtain an IP address automatically**: select this option to connect to the network through an automatically assigned IP address.

      The IP address is obtained from a DHCP server. If it cannot obtain an address, the IP address will default to addresses in the 169.254.x.x range.
    - **Use the following IP address**: select this option to manually assign a static IP address.
        - **IP Address**: Enter the IP Address you want to use.
        - **Subnet Mask**: Enter the Subnet Mask you want to use.
        - **Default Gateway**: Enter the Default Gateway you want to use.
2. Select the **Disable setting static IP address through ARP/Ping method** check box to disable the ARP/Ping method of setting an IP address.
3. If the camera supports IPv6, select the **Enable IPv6** check box to configure the following settings.

> **Note:** Enabling IPv6 does not disable IPv4 settings.

a. Select the **Accept Router Advertisements** check box if using Stateless Address Auto-Configuration.

b. From the **DHCPv6 State** drop-down list, select one of the following:

- **Auto**: DHCPv6 state is determined by router advertisements (RA).

  > **Note:** The Accept Router Advertisements setting must be enabled for this setting to perform as expected.

- **Stateful**: the camera receives IP address, DNS and NTP information from the DHCPv6 server.
- **Stateless**: the camera only receives DNS and NTP information from the DHCPv6 server. It does not accept an IP address from the DHCPv6 server.
- **Off**: the camera does not communicate with the DHCPv6 server.

c. In the **Static IPv6 Addresses** field, enter the preferred IPv6 address. Click + for additional addresses.

To change the prefix length, enter the preferred IPv6 address using Classless Inter-Domain Routing (CIDR) notation. For example, `2001:db8::1/32` would indicate the address prefix is 32-bits long.

By default, the prefix length is set to `/64`.

> **Note:** The configured prefix length may not display correctly in the web interface, but the prefix used by the camera will be the configured length.

d. In the **Default Gateway** field, enter the Default Gateway you prefer to use. You can only assign a Default Gateway if RA is disabled.

The IPv6 addresses that can be used to access the camera are listed under the **Current IPv6 Addresses** area.

4. If you need to customize the hostname, enter it in the **Hostname** field.
5. In the DNS Lookup area, select how the camera will obtain a Domain Name System (DNS) server address.

- **Obtain DNS server address automatically**: select this option to automatically find a DNS server.
- **Use the following DNS server addresses**: select this option to manually set DNS server addresses. You can set up to three addresses:
  - **Preferred DNS server**: assign the address of the preferred DNS server in this field.
  - **Alternate DNS server 1**: (optional) assign the address of an alternate DNS server to this field. In the case that the preferred server is not available, the camera will attempt to connect to this server.

- **Alternate DNS server 2**: (optional) assign the address of another alternate DNS server to this field. In the case that both the preferred server and the first alternate server are unavailable, the camera will attempt to connect to this server.

6. In the Control Ports area, you can specify which control ports are used to access the camera. You can enter any port number between 1 and 65534. The default port numbers are:
   - **HTTP Port**: 80

     If you want to limit camera access to secure connections only, clear the **Enable HTTP connections** check box. HTTP Port access is enabled by default.
   - **HTTPS Port**: 443
   - **RTSP Port**: 554
   - **RTSP Replay Port**: 555
7. In the NTP Server area, indicate if you want the camera to use an NTP server to keep time.
   a. Select the NTP source to use for keeping time:
      - **Always use Avigilon Control Center NTP Server**. Select this option if you want the camera to keep time through the Avigilon Control Center™ software only.
      - **Always use external NTP server**. Select this option if you want to use an external NTP server only. Then configure the NTP server to use.
      - **Use Avigilon Control Center Server with a failover external NTP**. By default, Avigilon cameras keep time through the Avigilon Control Center software and will use an external NTP Server when not connected to an ACC server, if one is configured.

   b. If you are using an external NTP server, select how the server is configured:
      - **DHCP**.
      - **Manual**. Select this option and then enter the server address in the **NTP Server** field.
8. In the MTU area, set the Maximum Transmission Unit (MTU) size in bytes. Enter a number between the available range displayed on the right. You may want to lower the MTU size if your network connection is slow.
9. In the Ethernet Setting area, set the **Speed & Duplex** for your network connection. The Auto-negotiation (default) setting is the preferred setting for most cameras, and will negotiate the optimal speed and duplex setting for your network connection. If necessary, you can manually select the speed and duplex setting for your connection.
10. In the Security area, set the **Minimum TLS version** that the camera should use for encrypting the communication between camera and server and block older TLS versions that should not be used.

- **TLS 1.3** is recommended for increased security.

  > **Note:** Please verify that this is supported by your VMS before enabling this option.

- **TLS 1.2** can be selected if it is required for backwards compatibility.

  > **Note:** Some cameras may also have the **TLS 1.1** options, which can be selected if it is required for backwards compatibility.

11. Click **Apply** to save your settings.

Configuring 802.1x Port-Based Authentication

If your network switch requires 802.1x port-based authentication, you can set up the appropriate camera credentials so that the video stream is not blocked by the switch.

1. In the left-menu pane, select **Network > 802.1x**.
2. On the Configure 802.1x Profiles page, select the preferred authentication method. You can configure multiple profiles. Be aware that you can only enable one profile at a time.

   From the **EAP Method** drop-down list, select one of the following and complete the related fields:

   - Select **PEAP** for username and password authentication.
     - **Configuration Name:** give the profile a name.
     - **EAP Identity:** enter the username that will be used to authenticate the camera.
     - **Password:** enter the password that will be used to authenticate the camera.
   - Select **EAP-TLS** for certificate authentication.
     - **Configuration Name:** give the profile a name.
     - **EAP Identity:** enter the username that will be used to authenticate the camera.
     - **TLS Client Certificates:** select the PEM-encoded certificate file to authenticate the camera.
     - **Private Key:** select the PEM-encoded private key file to authenticate the camera.
     - **Private Key Password:** if the private key has a password, enter the password here.
     - Click **Upload Files** and the TLS client certificate and private key are uploaded to the camera. The uploaded files are used to generate a unique certificate to authenticate the camera. The unique certificate is displayed in the Uploaded Certificate field.
3. Click **Save Config** to save the authentication profile.

   If this is the first profile added to the camera, it is automatically enabled.

   Saved configurations are listed under **Saved 802.1x Configurations**.

Switching 802.1x Authentication Profiles

To use a different authentication profile, select the saved configuration then click **Enable**.

Deleting an 802.1x Authentication Profile

To delete one of the authentication profiles, select the saved configuration then click **Remove**.

Configuring SNMP

You can use the Simple Network Management Protocol (SNMP) to help manage cameras that are connected to the network. When SNMP is enabled, camera status information can be sent to an SNMP management station.

On the SNMP page, you can configure the camera's SNMP settings and choose the status information that is sent to the management station page. For more details on the status information or traps that will be sent, see the camera's Management Information Base (MIB) file on the Avigilon website: **http://avigilon.com/support-and-downloads**.

1. In the left-menu pane, select **Network** > **SNMP**.
2. On the SNMP page, select the **Enable SNMP** check box.
3. From the **Version** drop-down list, select the preferred SNMP version. Be aware that both versions can be configured, but only one can be enabled at a time:
    - **SNMP v2c**: Using SNMP v2c, you can make a request to the camera for status information through an SNMP Get request and receive trap notifications from the camera.

      In the **SNMP v2c Settings** area, select the **Enable Traps** check box to enable traps from the camera.

        a. **Read Community:** enter the read community name for the camera. The name is used to authenticate SNMP traffic. Only SNMP management stations with the same read community name will receive a response from the camera.

        b. **Trap Destination IP:** enter the IP address of the management station where the traps will be sent.

           In the Available Traps area, select the traps that will be sent:

            - **Temperature Alert:** a trap notification will be sent when the camera temperature rises above or falls below the supported threshold. A notification will also be sent when the camera temperature returns to normal.
            - **Camera Tampering:** a trap notification will be sent when the camera's video analytics detects a sudden scene change.
            - **Edge Storage Status:** a trap notification will be sent when the status of the SD card changes.

    - **SNMP v3:** Using SNMP v3, you can request status information through an SNMP Get request. SNMP v3 does not support traps.

      SNMP v3 offers greater security by allowing you to set a username and password for the camera. This camera uses SHA-1 type authentication and AES type encryption.

      In the SNMP v3 Settings area, complete the following:

a. **Username:** enter the username that the management station must use when sending the SNMP Get request to the camera.

b. **Password:** enter the password the management station must use with the chosen username.

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

IP Filter

On the IP Filter page, you can control which IP addresses are able to connect to your camera.

If enabled, you have the option to limit IP addresses in 2 ways:

- Deny Access to specific IP addresses or range of addresses.
- Allow Access only to specific IP addresses or range of addresses.

Important: If you choose to filter IP access using the **Allow Access** option, make sure that you configure the correct addresses to be allowed or you may be locked out of your camera.

1. In the left menu pane, select **Network > IP Filter**.
2. Select the **Enable IP Filter** checkbox to enable IP filtering.
3. At the top of the page, select how the camera should filter IP addresses:
    - **Allow Access**: select this option to only allow access to the specific IP address entries you will make below. Be sure that you add the correct IP address entries or you may be locked out of your camera.
    - **Deny Access**: select this option to deny access to the specific IP address entries you will make below. This is the default option.
4. Add all the IP Filter Entries that you would like to either deny or allow access:
    a. Click + to add an entry to the IP filter list.
    b. In the **IPv4, IPv6 or CIDR range** field that appears, enter the IPv4, IPv6 or CIDR range of IP addresses that you would like to filter.
    c. Continue to add more entries to the list until you have added all of the necessary IP addresses to be filtered.

    Tip: You can add up to 256 IP Filter Entries.
5. Click **Apply** to save your settings.

Note: If you have denied or not allowed access to the IP address you are currently using to connect to your camera, your web interface connection will close after you click Apply.

Security Settings

For greater network communication security, you can enable compliance with the Federal Information Processing Standard (FIPS) 140-2 Level 1 or Level 3 Security Requirements for Cryptographic Modules for server and camera communication.

Note:

- FIPS 140-2 Level 1 requires the purchase of a FIPS camera license.
- FIPS 140-2 Level 3 on cameras with an onboard TPM requires the purchase of a FIPS camera license.
- FIPS 140-2 Level 3 on cameras without an onboard TPM requires the purchase of a CRYPTR micro card. The CRYPTR card must be inserted into the camera's SD card slot before it can be enabled.

1. Go to the Security Settings page.
2. In the Encryption Engine drop-down list, select the type of encryption to use:
   - **OpenSSL** is the default option for encryption.
   - **FIPS 140-2** enables FIPS 140-2 level 1 encryption.
   - **NXP TPM** enables the onboard trusted platform module (TPM) to securely store your encryption keys. Only cameras that come with the onboard NXP TPM will display this option.
3. Click **Apply** to save your settings.

Important: Changing this setting on your camera will require your camera to reboot and you will lose the video stream for that time. Avigilon recommends that you apply this setting during non-critical operating times.

Compression and Image Rate

On the Compression and Image Rate page, you can change the camera's compression and image quality settings for sending video over the network. You can change the camera's compression and image quality settings separately for primary, secondary, and tertiary streams.

Note: If a camera with video analytics or unusual motion detection is physically moved or adjusted, or if the focus or zoom level is changed, reset the learning progress to provide accurate results. If the camera's image rate and compression or display settings are updated, the learning progress may reset automatically.

To enable easy access and lower bandwidth usage, the web interface only displays video in JPEG format. The settings on this page only affect the video transmitted to the network video management software.

Avigilon High Definition IP cameras have dual stream capabilities. If the camera's streaming format is set to H.264 or H.265, the camera's web interface can still display live video in JPEG format.

Note: The camera may automatically adjust compression quality in order to abide by the bandwidth cap specified.

1. In the **Format** drop-down list, select the preferred streaming format for displaying the camera video in the network video management software.

   If you are using the Onboard Storage feature, select **H.264** or **H.265**. For more information, see *Enabling Onboard Storage* on page 20.
2. In the **Max Image Rate** field, enter how many images per second you want the camera to stream over the network.
3. In the **Max Quality** drop-down list, select the desired image quality level.

   Image quality setting of 1 will produce the highest quality video and require the most bandwidth.
4. In the **Max Bitrate** field, enter the maximum bandwidth the camera can use.
5. In the **Primary Resolution** drop-down list, select the preferred image resolution.
6. In the **Min Keyframe Interval** field, enter the number of frames between each keyframe.
7. Click **Apply** to save your changes.

Enabling HDSM SmartCodec™ Technology Settings

HDSM SmartCodec technology operates by separating foreground objects and background areas, then reduces bandwidth by increasing compression to the background areas. In this way, maximum quality is retained for subjects of interest while reducing bandwidth for unchanging backgrounds.

Important: Adjusting the stream settings with HDSM enabled and connected to Avigilon Control Center (ACC) or Avigilon Unity Video (AUV) may cause undesired behavior in camera operation and missing recordings. Camera stream settings should only be configured in ACC or AUV.

Once enabled, the camera will automatically switch to idle scene mode settings when there are no motion events detected. A motion event is when the camera detects pixel motion in the scene. For more information, see *Motion Detection* on page 15.

The camera uses pixel change motion to detect foreground objects and therefore uses the standard Motion Detection sensitivity settings of the camera.

Note: Additionally, advanced settings can also be updated on the HDSM SmartCodec Advanced

Settings page. For more information, see *HDSM SmartCodec Technology Advanced Settings* on the next page.

1. Select the **Enable** check box to enable the HDSM SmartCodec features.
2. In the **Min Image Rate** field, enter how many images per second you want the camera to stream when there is no motion in the scene.
3. In the **Idle Keyframe interval** field, enter the number of frames between each keyframe (between 1 and 254) when there is no motion in the scene.
4. In the **Bandwidth Reduction** drop-down list, select one of the options:
    - **Low**
    - **Medium** (recommended)
    - **High**
    - **Custom**
5. Click **Apply** to save your changes.

Viewing the RTSP Stream URI

On the Compression and Image Rate page, you can also generate the camera's real time streaming protocol (RTSP) address. The RTSP Stream URI allows you to watch the camera's live video stream from any application that supports viewing RTSP streams, including many video players.

Note: You can only generate the RTSP stream address in the camera web interface.

1. If the Generate RTSP Stream URI button is not available, the RTSP stream URI is auto-generated.

    In the RTSP Stream URI area, the auto-generated URIs are displayed:

    - **Unicast** — select this option if you only plan to view the video stream from one video player at a time.
    - **Multicast** — select this option if you plan to view the video from more than one video player simultaneously.

        To view the RTSP stream:

        a. Copy and paste the generated address into your video player. DO NOT open the live video stream yet.

        b. Add your username and password to the beginning of the address in this format:

        rtsp://<username>:<password>@<generated RTSP Stream URI>/

        For example:
        `rtsp://admin:admin@192.168.1.79/defaultPrimary?streamType=u`

c. Open the live video stream.

2. To watch the camera's live video stream from an external video player, click **Generate RTSP Stream URI**.

   The generated address is displayed at the bottom of the RTSP Stream URI area.

Accessing the Still Image URI

On the Compression and Image Rate page, you can access the last still image frame that the camera recorded.

- To access the still image, click the URI link in the Still Image URI area.

The last recorded frame of video from the camera's secondary stream is displayed. You can choose to save or print the image directly from the browser.

HDSM SmartCodec Technology Advanced Settings

On the HDSM SmartCodec Technology Advanced Settings page you can select settings for both motion and idle scenes. Other HDSM SmartCodec technology settings can be selected under HDSM SmartCodec technology Settings on the Compression and Image Rate page. For more information, see *Enabling HDSM SmartCodec™ Technology Settings* on page 13.

1. In the left-menu pane, select **Compression and Image Rate** > **Advanced**.
2. In the **Background Quality** field in the **On Motion** section, enter the compression quality for the background (between the default of 6 and the lowest setting of 20).
3. In the **Post-motion delay** field in the **On Idle Scenes** section, enter the delay (in seconds) after motion has ended before the camera drops into idle scene settings (between 5 and 60).
4. In the **Image Rate** field in the **On Idle Scenes** section, enter the encoding frame rate (images per second) when there is no motion in the scene.
5. In the **Quality** field in the **On Idle Scenes** section, enter the compression quality when there is no motion in the scene (between 6 and 20).
6. In the **Max Bitrate** field in the **On Idle Scenes** section, enter the maximum number of kilobytes per second when there is no motion in the scene.
7. In the **Keyframe Interval** field in the **On Idle Scenes** section, enter the number of frames between each keyframe when there is no motion in the scene (between 1 and 254 frames).
8. Click **Apply** to save your changes.

Motion Detection

On the Motion Detection page, you can define the green motion detection areas in the camera's field of view. Motion detection is ignored in areas not highlighted in green.

To help you define motion sensitivity and threshold, motion is highlighted in red in the image panel.

Note: This motion detection setting configures pixel change detection in the camera's field of view. If you are configuring an Avigilon video analytics camera, you will need to configure the detailed analytics motion detection and other video analytics features through the Avigilon Control Center Client software. For more information, see the *Avigilon Control Center Client User Guide*.

1. Define the motion detection area.

   The entire field of view is highlighted for motion detection by default. To define the motion detection area, use any of the following tools:

   - Click **Clear All** to remove all motion detection areas on the video image.
   - Click **Set All** to set the motion detection area to span the entire video image.
   - To set a specific motion detection area, click **Select Area** then click and drag anywhere on the video image.
   - To clear a specific motion detection area, click **Clear Area** then click and drag over any motion detection area.
   - Use the **Zoom In** and **Zoom Out** buttons to locate specific areas in the video image.
2. In the **Sensitivity** field, enter a percentage number to define how much each pixel must change before it is considered in motion.

   The higher the sensitivity, the smaller the amount of pixel change is required before motion is detected.
3. In the **Threshold** field, enter a percentage number to define how many pixels must change before the image is considered to have motion.

   The higher the threshold, the higher the number of pixels must change before the image is considered to have motion.
4. If the camera is connected to a third-party video management system (VMS), check the **Enable Onvif MotionAlarm Event** check box.

   Once enabled, the H.264 camera can send motion alarm information to the VMS according to the appropriate ONVIF protocol.
5. Click **Apply** to save your changes.

Tamper Detection

On the Tamper Detection page, you can set how sensitive the camera is to tampering.

To set the options for tampering:

1. In the **Sensitivity** field, enter a number between 1 and 10 to define how sensitive the camera is to a sudden change in the scene. The higher the setting, the more sensitive the camera is to detect scene changes.

   Note: A sudden change in the scene is usually caused by someone unexpectedly moving the camera. Lower the setting if small changes in the scene, like moving shadows, trigger too many tampering events. If the camera is installed indoors and the scene is unlikely to change, you can increase this setting to capture more unusual events.

2. In the **Trigger Delay** field, enter the number of seconds (up to 30 seconds) that the tamper condition must persist in the scene before the tamper event is sent.
3. Click **Apply** to save your changes.

Analytics

On the Analytics page, you can enable the camera to send ONVIF compliant analytics metadata, such as ONVIF Profile M metadata, for cameras connected to a 3rd party VMS system. This option is disabled by default.

CAUTION — This option should only be enabled when you are connecting the camera to a 3rd party VMS system that requires sending analytics metadata from the camera to the VMS system.

When the camera is connected to an ACC system, analytics data is transmitted in a different format and enabling this option may degrade the camera video quality.

DO NOT enable this option if you are connecting your camera to an ACC system.

1. Select the **Enable ONVIF Compliant Analytics Metadata** check box to enable the camera to send ONVIF-compliant metadata to a 3rd party VMS system.
2. Click **Apply** to save your changes.

Audio Analytics

On the Audio Analytics page, you can enable and configure Audio Detection for different Audio Detection Events. This option is disabled by default.

Note: The camera's microphone is disabled by default and must be physically switched on for Audio Detection to work.

1. Select the **Enable Audio Detection** checkbox to enable the camera to detect Audio Detection Events.
2. Select a sound from the list:

   Note: The sounds listed under **Basic Sounds** are available without a premium license. The sounds listed under **Premium Sounds** are only available with a premium license. For more information, see *Licensing* on page 27.

   - Scream
   - Glass Break
   - Car Alarm
   - Fire Alarm
   - Dog Bark
   - Loud Noise
   - Ultrasound
   - Gunshot
3. Under Event Details, select the **Enabled** checkbox to enable Audio Detection Events.
4. Select a Sensitivity level from the drop-down list:
   - Low: a lower setting means it requires a lower confidence level to trigger an alarm.
   - Medium: a medium setting means it requires a medium confidence level to trigger an alarm.
   - High: a higher setting means it requires a higher confidence level to trigger an alarm.
5. Adjust Timeout by entering a value between 1 and 300 seconds. Timeout refers to the minimum interval of time after an audio event is detected before the system triggers an additional alarm.

   Important: During the Timeout interval, subsequent audio events, e.g., gunshots, will not trigger separate alarms.
6. Click **Apply** to save your changes.

Privacy Zones

On the Privacy Zones page, you can set privacy zones in the camera's field of view to block out areas that you do not want to see or record. You can also create removable privacy zones that are blurred instead of opaque. The removable privacy zones are only applied to the secondary and tertiary video streams. This allows for ACC group and privilege settings to define which users can view the primary stream without the removable privacy zones and which users can only view the streams with the blurred privacy zones. For more information, see *Setting a Removable Privacy Zone for Specific Users* on the next page.

The camera supports up to 64 privacy zones.

Setting a Privacy Zone

1. To add a privacy zone, click **Add**. A privacy zone box is added to the video image.
2. To define the privacy zone area, perform any of the following:
    a. Drag any side or corner of the box to resize the privacy zone. Privacy zones can only be rectangular in shape. Multiple privacy zones can be used to obscure other shapes.
    b. Click inside the box and drag to move the privacy zone.
3. To set the privacy zone as removable:
    a. Click the **Enable** checkbox in the **Removable Blur** settings.
    b. Use the **Blurriness** slider to define amount of blur in the privacy zones. All Blurriness settings will make the video from that zone completely obscured.

    > **Note:** Removable privacy zones have diagonal lines in them when configuring them on the Privacy Zones page to help tell them apart from regular privacy zones. When viewed in the Live View page or an ACC client, the zone will appear as a blurred gray rectangle.

4. Click **Apply** to save the privacy zone settings.

Deleting a Privacy Zone

Click the **X** at the top-right corner of the gray box to delete the privacy zone.

Setting a Removable Privacy Zone for Specific Users

This is only supported when connecting the camera to an ACC system. Removable privacy zones are only applied to the secondary and tertiary video streams so that ACC group and privilege settings can be used to define which users can view the primary stream without the privacy zones and which users can only view the streams with the blurred privacy zones.

> **Note:** The removable privacy zones will be applied to the secondary and tertiary video streams for any VMS the camera is connected to. Other VMS systems may have similar user privilege settings that can be used as a similar method to define which stream users can view. Check your VMS documentation for how to configure which streams users have access to view.

The ACC View high-resolution images group privilege gives users in that group access to the primary high-resolution stream of the cameras. This primary high-resolution stream will not have the removable privacy zones applied to it. This privilege should only be granted to administrators or similar users that might have a need to view the private areas of the image. General operators and other ACC users that don't have the View high-resolution images privilege will always have the removable privacy zones applied. See your ACC documentation for more information on setting up group privileges.

Keep the following limitations in mind when using removable privacy zones:

- ACC High Definition Stream Management (HDSM)™ will display primary, secondary, or tertiary streams based on the zoom level and viewing portal size when viewing live or recorded video. Make sure to remove the View high-resolution images privilege from ACC users that do not need to see the unblurred video.
- Certain ACC user groups can be granted Emergency Privilege Override which can be used to see the primary unblurred video stream. This feature logs each use of the emergency override, including the username and time of access, in the ACC event logs.
- When ACC operators with access to the primary stream play back recorded video in a small video panel, they will see the blurred privacy zone. The blurred zone will disappear when the privileged operator pauses or scrubs through video on the timeline. The privileged operator can also swithc to the full screen view and/or zoom in on the video to make HDSM display the unblurred primary stream.

Storage

On the Storage page, you can enable the camera's onboard storage feature and download recorded video directly from the camera. Onboard storage is available only on cameras equipped with an SD card or microSD card slot.

Important: SD card failures can cause the camera to continuously reboot. To prevent this, the SD card will be disabled if persistent failures are detected. For more information, see *SD Card Failures* on page 23.

Cameras that include an onboard TPM do not support the CryptR micro card and can only use the SD slots for onboard storage.

Note: For cameras with 2 microSD card slots, the camera will record video to SD cards in both slots. The total storage capacity of the system is the combined storage capacity of each of the two individual cards.

Enabling Onboard Storage

To use the camera's onboard storage feature, you must first insert an SD card into the camera. Refer to the camera's installation manual for the location of the SD card slot.

Tip: The SD card will record from the camera's highest resolution, non-tiled stream. In most cases, this will be the primary stream.

Note: For cameras with 2 microSD card slots, the camera will record video to SD cards in both slots. The total storage capacity of the system is the combined storage capacity of each of the two individual cards.

1. On the Storage page, select the **Enable Onboard Storage** check box.
2. By default, the camera is set to only record to the SD card when it is unable to communicate with the network video management server. If you prefer to have the camera record video to both the network video management server and to the SD card, clear the **Record only when server connection is interrupted** check box to disable the setting.
3. Select one of the following recording modes:
   - **Continuous:** the camera never stops recording to the SD card.
   - **On Motion:** the camera only records when there is motion in the scene.

     If you are configuring an Avigilon video analytics camera, the On Motion setting will record either pixel change in the scene or analytics motion events depending on how the camera is configured in the Avigilon Control Center Client software.

   The recorded video will be divided into files no more than five minutes in length or 100 MB in size.
4. On the Compression and Image Rate page, make sure the format is set to **H.264** or **H.265** to maximize the SD card recording capacity and performance.

ONVIF Profile G

ONVIF Profile G allows video management systems to retrieve video from a camera's onboard storage when there is a gap in the VMS video due to a network outage or similar event.

- Cameras with firmware versions 4.4.0.X or later will have ONVIF Profile G already enabled.
- **Note:** Enabling ONVIF Profile G will require reformatting the SD card. You will lose all footage currently recorded on the SD card. Ensure that you download any required video clips before enabling Profile G.

Onvif is a trademark of Onvif, Inc.

Downloading Recorded Video from the Web Interface

Listed in the Recordings section are all the videos that have been recorded to the SD card.

If you are using two SD cards you will have to select the SD card that you want to download video from. You may have to check both SD cards for the recording you want to download. The camera can record video to either SD card based on the remaining capacity of the SD cards.

It is recommended that you download recorded video from the web interface. However, if your bandwidth is

limited, you can choose to download the recorded video directly from the SD card. For more information, see *Downloading Recorded Video from the SD Card* below.

To download recorded video from the web interface, perform the following:

> **Tip:** If you are using two SD cards, select the SD card that you want to download the recording from.

1. On the Storage page, select the check box beside all the videos you want to download.

   To help you find the video you want, you can filter the videos by date and time. Select the **Filter** check box then select the time range.
2. Click **Download**.

The selected video files are automatically downloaded to your browser's default Downloads folder. If you are prompted by the browser, allow the download to occur.

> **Note:** Do not close your browser window until the download is complete or the file may not download correctly. This is important if you are downloading multiple video files because the files are downloaded one by one.

Downloading Recorded Video from the SD Card

If you do not have enough bandwidth to download recorded video directly from the web interface, you can choose to download the recorded video directly from the SD card.

To download recorded video directly from the SD card, perform the following:

1. In the Settings area, disable onboard storage by clearing the **Enable Onboard Storage** check box then click **Apply**.
2. Remove the SD card from the camera.
3. Insert the SD card into a card reader.
4. When the Windows AutoPlay dialog box appears, select **Open folder to view files**.
5. Open the Avigilon Camera Footage application.

   The Avigilon Camera Footage window lists all the video files that are stored in the SD card.
   - To download all the recorded videos, click **Download All**.
   - To download specific video, select the video files you want then click **Download Selected**.
6. When you are prompted, choose a location to save the video files.

   The files start downloading from the SD card and are saved to the selected location.
7. When you are ready, eject the SD card.
8. Insert the SD card back into the camera then select Enable Onboard Storage to begin recording to the SD card again.

Deleting Recorded Video

As the SD card becomes full, the camera automatically starts overwriting the oldest recorded video. You can also choose to manually delete video to make room for new recordings.

On the Storage page, you can choose to delete video in the following ways:

- To delete individual video files, select all of the files you want to delete from the Recordings list then click **Delete**.
- To delete all of the recorded video files, click **Format Card** to format the SD card.

SD Card Failures

SD card failures can cause the camera to continuously reboot and compromise the camera's reliability. To prevent this, the SD card will be disabled if persistent failures are detected.

Once an SD card has been disabled, the camera and web interface will notify you of the issue:

- The camera's video will overlay warning text on the video image: `SD Card Recording Disabled! Replace card to re-enable.`

  > **Note:** The video overlay message can be disabled on the camera's **Storage** page by clearing the **Enable video alert overlay on severe SD card failure** checkbox.

- The camera's Storage page will have a warning message when you select the page: `SD card slot was disabled due to card errors, please replace card.`

To re-enable the SD card, remove it from the SD card slot on the camera and replace it with a working SD card. A speed test will be run on the new card when it is inserted to determine if it will function without any issues.

You can also force the SD card to be re-enabled in the web interface by clicking **Force Re-Enabled SD Card Slot** on the **Storage** page.

> **Important:** Forcing the SD card to be re-enabled is not recommended unless you are sure there are no problems with the card. If the card continues to fail, it may cause the camera to enter a reboot loop and after continued persistent failures, the SD card will be disabled again.

Digital Inputs and Outputs

On the Digital Inputs and Outputs page, you can set up the external input and output devices that are connected to the camera. This option does not appear for cameras that do not support digital inputs and outputs.

1. To configure a digital input:
    a. In the Digital Inputs area, enter a name for the digital input in the **Name** field.
    b. Select the appropriate state from the **Circuit State** drop-down list. The options are:
        - **Normally Open**
        - **Normally Closed**

        Note: Some cameras can detect the circuit state of the digital inputs automatically and the input will trigger when a change in state is detected. For these cameras, the Circuit State setting will have no effect on the digital input function.

    c. Click **Apply** to save your changes.

        Once the digital input is connected to the camera, you will see the connection status in the **Circuit Current State** area. The status is typically *Open* or *Closed*.
2. To configure a digital output:
    a. In the Digital Outputs area, enter a name for the digital output in the **Name** field.
    b. Select the appropriate state from the **Circuit State** drop-down list.
    c. In the **Duration** field, enter how long the digital output is active for when triggered. You can enter any number between 100 and 86,400,000 milliseconds.
    d. Click **Trigger** to manually trigger the digital output from the web interface.
    e. Click **Apply** to save your changes.

Audio

Use the settings on the Audio page to adjust the audio quality of the camera.

For encoding the audio stream, you can choose from the Opus sound encoder, which produces high-quality sound, or the G.711 protocol sound encoder. Use the Opus encoder if you are using ACC software Release 6.10 or later (or a third-party video management system that supports the Opus protocol). Otherwise use the widely supported G.711 protocol.

1. In the Audio Settings section:
    a. In the **Encoding** field, specify the audio encoder to use:
        - **Opus**: Default high quality audio codec.
        - **G.711**: Supported on various platforms.
2. In the Device Speaker section, use the **Volume** slider to adjust the volume on the speaker (from 0 to 100).
3. In the Device Microphone section:
4. Click **Apply** to save your changes.

Users

On the Users page, you can add new users, edit existing users, and change passwords.

Adding a User

1. On the Users page, click **Add...**.
2. On the Add User page, enter a User Name and Password for the new user.
3. In the **Security Group** drop-down list, select the access permissions available to this new user.
    - **Administrator**: full access to all the available features in the camera web interface.
    - **Operator**: has access to the Live View but limited access to the Setup features. The user can access the General page, Image and Display page, Compression and Image Rate page, Motion Detection page, Privacy Zones page, Digital Inputs and Outputs page, Microphone page and the Speakers page. The new user can also configure onboard storage settings but cannot delete video recordings or format the SD card.
    - **User**: has access to the Live View, but cannot access any of the Setup pages.
4. Click **Apply** to add the user.

Editing Users and Passwords

1. On the Users page, select a user from the User Name (Security Group) list and click **Modify**.
2. To change the user's password, enter a new password for the user.
3. To change the user's security group, select a different group from the **Security Group** drop-down list.

    Note: You cannot change the security group for the administrator account.

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

Removing a User

Note: You cannot remove the default Administrator user unless there is another user with administrator privileges. The camera must always have at least one administrator user configured.

1. On the Users page, select a user from the User Name (Security Group) list.
2. Click **Remove**.

Keeping Usernames and Passwords After Firmware Revert

To add a layer of security to protect the camera from theft, you have the option of keeping the camera's

current usernames and passwords after a firmware revert.

If you have set your camera to use FIPS 140-2 encryption, we recommend that you do not choose to keep usernames and passwords after a firmware revert. The password and username is not stored in a FIPS 140-2 compliant manner and may affect your FIPS 140-2 compliance.

Normally if you restore the camera firmware back to the factory default settings, the camera returns to using the default username and password. When you enable this feature, the camera will continue to use the configured username and passwords, so the camera cannot connect to new servers without the appropriate credentials.

Important: Forgetting your own username or password after enabling this setting voids your warranty. The primary method of restoring the factory default username and password will be disabled.

1. At the bottom of the Users page, select the **Do not clear usernames or passwords on firmware revert** check box.
2. After you select the check box, the following popup message appears:

   Please store your administrator password in a safe place. Password recovery is not covered by warranty and loss of password voids your warranty.

3. Click **OK** if you agree to the feature limitations.

Always keep a copy of your password in a safe place to avoid losing access to your camera.

System

On the System page, you can manually upgrade the camera firmware, reboot the camera, and restore all of the camera's factory default settings.

- Click **Reboot** to restart the camera.
- Click **Restore** to revert the camera firmware back to the factory default settings.

  Tip: If you've enabled the feature that maintains your username and password after a firmware revert, make sure you have a written copy of your current usernames and passwords. For more information, see *Keeping Usernames and Passwords After Firmware Revert* on the previous page.

- To upgrade the camera firmware, see *Upgrading the Camera Firmware* below.

Upgrading the Camera Firmware

To manually upgrade the camera 's firmware:

1. Download the latest version of the firmware .bin file from the Avigilon website (avigilon.com/support) and complete the following steps:
2. On the System page, click Choose File to browse and locate the downloaded firmware file.
3. Click **Upgrade**. Wait until the camera upgrade is complete.

Licensing

On the Licensing page, you can use a license activation key to enable certain features.

> **Note:** For licensing support, visit https://www.avigilon.com/support.

1. Click **Add License...**
2. Enter a license activation key into the field.
3. Choose an activation method:
    - Automatic: use this option if the camera has Internet access.
    - Manual: use this option if the camera does not have Internet access.

Automatic Activation

Click **Activate Now** to activate your license.

Manual Activation

1. Click **Save File...** to generate an activation request file.
2. Upload the activation request file to our licensing website: https://licensing.avigilon.com/activate
   Your license file will be available for download.
3. Save the license file.
4. Click **Choose File...** and select the license file you saved in Step 3.

Device Log

The Device Log page allows you to view the camera's system logs and the camera access logs.

The most recent log event is always displayed first.

1. In the **Type** drop-down list, select one of the following:
    - **Access Logs** — Logs of users who have logged into the web interface.
    - **System Logs** — Logs of camera operations.
2. In the **Minimum Log Level** drop-down list, select the minimum level of log message you want to see:
    - **Error** — Sent when the camera encounters a serious error. These are the highest level log messages.
    - **Warning** — Sent when the camera encounters a minor error such as an invalid username and password.
    - **Info** — Status information sent by the camera. These are the lowest level log messages.
3. In the **Maximum Number of Logs** drop-down list, select the number of log messages you want displayed.
4. Click **Update**.

    The logs update to display the filtered information.

Disable WebUI

On the Disable WebUI page, you can disable the camera's web interface, including any non-ONVIF API calls. This will disable any access to the camera other than through the ACC Client or an ONVIF-compliant VMS.

Important: If you disable the web UI and non-ONVIF APIs, you will only be able to connect to the camera with the ACC Client or an ONVIF-compliant VMS.
The only way to reverse this setting is by doing a physical firmware revert on the camera. See the camera's installation guide for more information.

To disable the web UI and non-ONVIF APIs:

1. Select the **Disable non-ONVIF APIs** checkbox.
2. Click **Apply**.
3. Read the warning message that appears, and click **OK** if you want to proceed with this setting.

About

On the About page, you can find information about your camera such as the firmware version, serial number, and ONVIF conformance.

Checking a Camera's Power Source

For camera's with multiple power source options, it may be useful to check the About page to confirm which power source is currently connected.