AVIGILON

PTZ Camera Web Interface User Guide

Avigilon PTZ H4, H5 and H6 IP Camera Models:

H6A-PTZ-xx
H5A-PTZ-xx
H4PTZ-Dx
H5A-IRPTZ-DP
H5EXPTZ-xx-BO30
H5A-RGDPTZ
H4IRPTZ-DP

Copyright

Avigilon Corporation
avigilon.com

PDF-PTZWebUI-A

Revision: 4 - EN

20240206

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:

- **IP Camera Web Interface Guide** — for H5A cameras, H5SL cameras, and many more.
- **H6 Camera Web Interface User Guide** — for H6A cameras and H6X cameras.
- **Multi-Head Camera Web Interface Guide** — for dual head and multisensor cameras.
- **H4 and H5 Pro Camera Web Interface Guide** — for high resolution Pro cameras.
- **H5A Fisheye Camera Web Interface Guide** — for H5A fisheye cameras.
- **Video Intercom Web Interface Guide** — for H4 Video Intercoms.
- **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* below.

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.

Logging In

Cameras manufactured before January 1, 2020, have a default username and password you can use to log in.

You will automatically be prompted to enter your username and password to access the camera.

- If the camera 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 camera will be operational. Use these credentials when logging in.
- The default username for most cameras is `administrator` with no password.

> **Tip:** It is recommended that you add a password after your first login. For more information, see *Editing Users and Passwords* on page 41.

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.

The following sections describe the buttons that are displayed under the image panel if users have access to Pan-Tilt-Zoom (PTZ) controls. PTZ controls allow users to control the zoom, focus, and positioning of a camera. To give a user PTZ controls, see *Adding a User* on page 41.

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

Using the Camera Zoom and Focus Controls

- To zoom in, move the slider towards the right.
- To zoom out, move the slider towards the left.
- To focus towards zero:
  - Click **<<** to take a large step.
  - Click **<** to take a small step.
  - Click **0** to focus at zero.
- To focus towards infinity:
  - Click **>>** to take a large step.
  - Click **>** to take a small step.
  - Click **Inf** to focus at infinity.
- If the camera supports auto focusing, click **Auto Focus**.

Using Camera Presets

Users can save frequently used camera operations as presets on the Live View page.

> **Note:** Only users in the **Operator** and **Administrator** security groups can add or remove presets. For more information on security groups, see *Adding a User* on page 41.

The presets can also be configured in the ACC Client software through the PTZ controls.

Adding a Camera Preset

1. To add a preset, select the preset type from the drop-down list:
    - PTZ — used for zoom and focus configurations. This is the default preset type.
    - Wiper Single Shot — triggers a single back-and-forth wipe of the wiper blade.
    - Wiper On — turns on the wiper, which will run continuously back-and-forth until stopped by triggering the Wiper Off preset.
    - Washer Sequence — starts a sequence of operations: PTZ to the wiper position, spraying the washer, running the wiper, and returning to the starting PTZ position.
    - Wiper Off — used to turn the wiper off.
    - Switch to Day Mode — switches the camera to day mode.
    - Switch to Night Mode — switches the camera to night mode.
    - Switch to Auto Mode — switches the camera to auto mode.
2. Use the Pan, Tilt, Zoom, and focus controls to position the camera to a specific point in the video image if you are adding a PTZ preset.
3. Enter a name in the **Add Preset** field then click **Add**.

   The new preset will appear in the drop-down list of configured presets.

Moving the Camera to a Preset Position

To use a preset, select a configured preset from the **Presets** drop-down list and click **Go**.

Deleting a Preset

To delete a preset, select a preset from the drop-down list then click **Remove**.

Using the PTZ Camera Controls

If you are accessing an Avigilon PTZ dome camera, you can control the zoom, focus, and presets in the same way as other Avigilon High Definition H.264 IP cameras, but you also have access to other features that are specific to the PTZ camera.

1. To zoom the camera:
    - Besides using the Zoom slider, you can also click and drag to create a green box on the image panel to define the area you want to zoom in to see.
2. To move the camera:
    - Click anywhere on the image panel to center the camera to that point.
    - Or, click and drag your mouse from center to move the camera in that direction. The farther the arrow is from center, the faster the camera will move.
3. To perform a guard tour, select an option from the **Tours** drop-down list then click **Start**. To setup a tour, see *Creating PTZ Tours* on page 37.

4. To stop a guard tour, click **Stop**. You can pause a tour at any time just by using the other PTZ controls.
5. To digitally zoom using your mouse cursor:
    - Move your cursor to the area you want to zoom in on. Scrolling up using your mouse wheel will digitally zoom in and scrolling down with your mouse wheel will digitally zoom out.

Activating the IR PTZ Camera Washing Sequence

The Avigilon H4 IR PTZ camera offers optional wiper and washer components to clean the glass surface. The washing sequence can be started by clicking **Washer Sequence**. There is also an option to perform a single wipe which can be started by clicking **Single Wipe**. This may cause the camera's tilt position to move temporarily, the position will be restored once the wipe action is finished.

> **Note:** The camera can also report on low water levels for the washing tank. The optional sensor can be configured by attaching it to the digital input. In order for the washer to work correctly, the washer circuit must be connected to Digital Output 1 with the Circuit State set to Normally Open. For more information, see *Digital Inputs and Outputs* on page 35.

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 32.
- 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 26.

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 33.

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. Select the **Lens Distortion Correction** check box to enable an algorithm-based automatic correction of lens distortion. The camera will reboot when applying this setting.
5. 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.
   - **No Video Analytics** — This mode will disable smart analytics. This option is for deployments where camera based video analytics would interfere with other analytics integrations.
6. 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**
7. 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, the NTP server must be configured. Click on the (Configure NTP Server) link at the bottom of the page to be redirected to the Network page.

  For more information on configuring the NTP server, see Step 7 under *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.

8. 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. Ensure the **Accept Router Advertisements** check box is checked 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.
- Click — to remove an address.

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. PTZ Priority Mode is a feature that improves video latency by disabling network traffic shaping. Video latency is higher when network traffic shaping is enabled and packets are delayed to reduce network traffic spikes. Set the **Priority Mode** that best suits your system:

    > **Tip:** Network traffic spikes may result in packet loss.

    - **Controlled (Default)**. This default option will allow your ACC system to control the PTZ priority mode. When an ACC Client has the PTZ controls selected, PTZ priority mode will be enabled.
    - **Enabled**. Select this option to override ACC Client control and set PTZ priority mode to always be enabled. Select this option to improve video latency.
    - **Disabled**. Select this option to override ACC Client control and set PTZ priority mode to always be disabled. Select this option to use network traffic shaping to reduce traffic spikes.

12. 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.
     - **Authenticate Server**: check this box if you need to add a certificate.

- 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.

Configuring DSCP

Differentiated services or DiffServ is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks. DiffServ can, for example, be used to provide low-latency to critical network traffic, such as voice or streaming media, while providing simple best-effort service to non-critical services, such as web traffic or file transfers.

DiffServ uses a 6-bit differentiated services code point (DSCP) in the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes. The DS field replaces the outdated IPv4 TOS field. Each DSCP value represents a QoS class, also known as a behavior aggregate. DiffServ is a coarse-grained, class-based mechanism for traffic management.

On the DSCP page you can activate the DSCP feature, choose values for the traffic types listed below, and restore values to default.

1. In the left-menu pane, select **Network** > **DSCP**.
2. In the DSCP area, the **Activate feature** checkbox is selected by default. Clear the **Activate feature** checkbox and click **Apply** to disable DSCP.
3. In the **ONVIF protcol** drop-down menu, click to select one of the options:

a. DF (0)
b. CS2 (16) (This is the default option.)

4. In the **Web interface** drop-down menu, click to select one of the options:
    a. DF (0)
    b. AF21 (18) (This is the default option.)
5. In the **SNMP protocol** drop-down menu, click to select one of the options:
    a. DF (0)
    b. CS2 (16) (This is the default option.)
6. In the **Primary Stream** drop-down menu, click to select one of the options:
    a. CS3 (24)
    b. AF31 (26)
    c. CS4 (32)
    d. AF41 (34) (This is the default option.)
7. In the **Secondary Stream** drop-down menu, click to select one of the options:
    a. CS3 (24)
    b. AF31 (26)
    c. CS4 (32)
    d. AF41 (34) (This is the default option.)
8. In the **Tertiary Stream** drop-down menu, click to select one of the options:
    a. CS3 (24) (This is the default option.)
    b. AF33 (30)
9. In the **Replay Stream** drop-down menu, click to select one of the options:
    a. CS3 (24) (This is the default option.)
    b. AF33 (30)
    c. CS4 (32)
    d. AF43 (38)
10. Click **Apply** to save your changes.
11. Click **Restore Defaults** and then click **Apply** to restore the DSCP values to their default settings.

Note: In case of Primary, Secondary, Tertiary and Replay Stream, it is very important to prepare and setup stream traffic. In case of stream over TCP (one common socket with RTSP), the DSCP value will be taken from the Primary stream and propagated to the other streams. Setting up a stream over UDP enables the user to specify different DSCP values for all streams.

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. 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.
    b. Click + to add additional entries to the IP filter list and continue to add additional 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**.
6. Click **Restore Defaults** and then click **Apply** to restore the IP Filter to it's default settings.

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. In the left menu pane, select **Network** > **Security** to navigate 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.

Enabling SRTP Streaming

SRTP streaming allows the camera to stream via SRTP encryption to Video Management Systems that also support SRTP. To enable SRTP streaming, the camera must have the correct firmware installed.

Note: Using SRTP for third-party integrations may require additional steps. For information on configuring SRTP streaming when using third-party integrations, refer to the manufacturer's documentation.

Requirements

- SRTP streaming requires an HTTP connection.

  You can enable HTTP connections in your camera's web interface. For instructions, see *Network* on page 9.
- SRTP streaming requires an OpenSSL library connection and does not work with FIPS 140-2 or NXP TPM.

  You can change the encryption engine to use OpenSSL on the Security page in your camera's web interface. For instructions, see *Security Settings* on the previous page.
- SRTP streaming requires a Unicast and Multicast over UDP connection.

Managing Certificates

On the Certificates page, administrators can manage certificates. Certificates are used to authenticate devices and encrypt communication over the network.

In the Certificates area, you can view the following information:

- **Cert ID**: Used to uniquely identify the certificate.
- **Subject**: The entity a certificate belongs to: a machine, an individual, or an organization.
- **Issuer**: The entity that verified the information and signed the certificate.
- **Algorithm**: This contain a hashing algorithm and a digital signature algorithm.
- **Expiry Date**: The date when the certificate expires.
- **Type**: The type of certificate, i.e., trusted or not trusted.

Downloading Certificates

1. To download a Certificate, select it from the list.
2. Click the **Download** button.

   Certificates are downloaded as .pem files.

Removing Certificates

1. To remove a Certificate, click the **Remove** button.
2. Click the **OK** button.

Downloading Certificate Signing Requests

1. To download the Certificate Signing Request (CSR), click the download **CSR button** and enter the following information:
   - **Common Name**: The primary hostname of the server.
   - **Alternative Name**: The alternative values associated with the certificate, e.g., email address, IP addresses, URIs, DNS names.
   - **(Optional) Organization**: The name of the organization requesting the certificates.
2. Click the **Download** button to download the CSR.

Uploading Certificates

1. To upload a certificate, click **Upload Cert**.
    a. **Certificate**: click **Choose File** to upload a certificate.
    b. **Private key**: click **Choose File** to upload a private key.
    c. **Private key password**: enter the private key password.
2. Click the **Upload** button to upload the Cert.

Uploading CA Certificates

1. Click the **Upload** button to upload the certificate.
2. To upload a CA certificate, click **Upload CA Cert**.
    a. CA Certificate: click **Choose File** to upload a CA certificate.
    b. CA Certificate ID: enter the CA certificate ID.
3. Click the **Upload** button to upload the CA certificate.

Image and Display

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.

On the Image and Display page, you can control the camera's day/night and exposure settings.

The Image and Display page includes an image panel that displays the camera's live video stream. When you click **Apply** to save your changes, the video stream is updated to use the new settings.

Below the image panel, the following information is displayed on the right:

- Current Exposure
- Current Gain
- Current Iris
- Last Known Light Level

Many Avigilon High Definition IP cameras have electronic zoom and focus controls, and you can set the camera's zoom and focus through this page as well.

1. Use the **Zoom** slider to adjust the camera's zoom position.
    - To zoom in, move the slider towards the right.
    - To zoom out, move the slider towards the left.
2. To manually focus the camera, use the **Focus** buttons:
    - To focus towards zero:
        - Click **<<** to take a large step.
        - Click **<** to take a small step.
        - Click **0** to focus at zero.
    - To focus towards infinity:
        - Click **>>** to take a large step.
        - Click **>** to take a small step.
        - Click **Inf** to focus at infinity.
    - If available, click **Auto Focus** to let the camera focus itself.

      Note: Once the focus is manually set, it will not change.
3. If the camera becomes defocused while in monochrome mode at night, adjust the **IR Focus Offset** slider to compensate for the focus shift caused by the built-in or external IR illuminators.
4. To set how the camera compensates for the environmental lighting conditions, define the following settings:
    - **Day/Night Mode:** Use the Day/Night Mode drop-down list to set how the video image switches between day and night mode.
        - **Automatic**: When the light level is above the day/night threshold, the video image will be in color. When the light level goes below the day/night threshold, the camera will automatically open the IR cut filter and switch to monochrome mode. If IR illuminators are enabled, they also turn on.
        - Check the **Restore Automatic after Timeout** box to automatically restore the Day/Night mode to **Automatic** after a certain timeout period. The **Timeout** field can be assigned a value between 5s and 3600s for the timeout period.
        - Use the **Day/Night Threshold** slider to set the day/night threshold. Move the slider to select the light level when the camera switches between day mode and night mode. The slider is only available when the Day/Night Mode setting is set to **Automatic**.

          The slider may display one of the following values:
            - **Day/Night Threshold (EV):** The slider value is in Exposure Values (EV).

              In day mode, the last known light level is displayed under the image panel and is also shown as a blue bar on the Day/Night Threshold slider.
            - **Day/Night Threshold (gain dB):** The slider value is in decibels (dB).

> **Note:** In addition to the **Day/Night Threshold (gain dB)** slider, Rugged PTZ cameras will also have a **Night/Day Threshold (gain dB)** slider and don't have a **Hysteresis** setting. The Day/Night Threshold (gain dB) slider determines the light level at which the camera will switch from day mode to night mode. The Night/Day Threshold (gain dB) slider determines the light level at which the camera will switch from night mode to day mode. The separation between these 2 slider settings is used to avoid the hysteresis problems.

  - Use the **Hysteresis** setting to refine the threshold offset.
    - Choose **Low** when the camera should switch from day to night in scenes where the difference between light and dark levels are small.
    - Choose **High** when the camera should switch modes when the difference between light and dark levels are large.
    - The default value is **Medium**.
  - **Color**: The video image will always be in color.
  - **Monochrome**: The video image will always be monochrome.
  - **External**: The camera will open the IR cut filter and switch to monochrome mode based on the digital input circuit state.

> **Note:** The default digital input circuit state is configured on the Digital Inputs and Outputs page. For more information, see *Digital Inputs and Outputs* on page 35.

- **Day/Night Delay (seconds)**: Set the delay time, in seconds, before the Day/Night mode switch is made once the set threshold is reached.
- **Enable IR LED in Night Mode:** You can manually enable or disable the IR illuminators that are installed on the camera. If unchecked, the IR LEDs will not turn on in Night mode.
- **Enable White Light LED:** For Rugged PTZ cameras with the white light LED illuminator accessory installed, use this checkbox to manually enable or disable the white light illuminator.
- **Toggle IR Filter with Illuminator:** For Rugged PTZ cameras with the white light LED illuminator accessory installed, use this checkbox to set the behavior of the IR cut filter when the white light LED is on. When this option is enabled, the default option, the IR cut filter will behave as normal and be in color mode in a light environment and night mode in a dark environment. When this option is disabled, the camera will remain in day mode at night and rely on the white light to illuminate the scene.
- **Enable Adaptive IR Compensation:** You can enable automatic infrared adjustments through Adaptive IR Compensation. This allows the camera to automatically adjust the video image for saturation caused by IR illumination.

- **Show Auto Contrast ROI:** Enabling this option allows you view and select the region of interest. The contrast is automatically adjusted based on the selected region.
- **Enable Night Visibility Check:** You can manually enable or disable the night visibility check on a camera. The night visibility check, when enabled, performs a periodic test switching between day/night mode to check if there is sufficient light level to switch from night mode to day mode. When disabled, the camera will use a less optimal method to determine if the light level is sufficient to switch to day mode.

  > **Note:** Disabling the night visibility check could delay the camera from transitioning between night and day modes and make the transition time less optimal. For example, the camera stays in night mode 30 minutes longer than it needs to.

- **Rugged PTZ Cameras Only**

  Use the **Narrow Illuminator** drop-down menu to configure how the narrow beam of the Rugged PTZ's white light LED illuminator will function:

  - **Always On:** Sets the white light LED illuminator to always use the narrow beam. This setting is recommended for Rugged PTZ cameras that are mostly used for viewing distant scenes.
  - **Always Off:** Sets the white light LED illuminator to disable the narrow beam and to always use the wide beam. This setting is recommended for Rugged PTZ cameras that are mostly used for viewing nearby scenes.
  - **At Zoom Level:** Sets the white light LED illuminator to switch between the wide and narrow beams at a specific zoom setting. Use this setting to have the Rugged PTZ camera switch to the white light LED's narrow beam when the camera zooms in to the scene by the zoom level that is specified in the **Zoom Step (0-100)** field.

    > **Tip:** You can zoom the Rugged PTZ camera to the zoom level that you want the narrow white light LED beam to turn on and then click **Current** to input that zoom level into the field.

5. To adjust the exposure of the image, adjust the Exposure Settings:
   - **Flicker Control:** If your video image flickers because of fluorescent lights around the camera, you can reduce the effects of the light by setting the Flicker Control to the same frequency as your lights. Generally, Europe is **50Hz** and North America is **60Hz**.

     > **Note:** Resetting this control will stop the video stream for a few seconds.

   - **Enable Wide Dynamic Range:** You can enable automatic color adjustments through Wide Dynamic Range (WDR). This allows the camera to adjust the video image to accommodate scenes where bright light and dark shadow are clearly visible.

- **Exposure:** You can allow the camera to control the exposure by selecting **Automatic**, or you can set a specific exposure rate.

  > **Note:** Increasing the manual exposure time may affect the image rate.

- **Exposure Offset:** This is an advanced setting that allows you to compensate for unusual lighting conditions by setting an exposure offset value. Negative values result in a persistently darker image, and positive values result in a persistently brighter image.
- **Maximum Exposure:** You can limit the automatic exposure setting by selecting a maximum exposure level. The Maximum Exposure drop-down list is only available when the Exposure setting is set to Automatic.

  By setting a maximum exposure level for low-light situations, you can control the camera's exposure time to let in the maximum amount of light without creating blurry images.
- **Priority:** You can set **Max Image Rate** or **Exposure** as the priority.
  - When set to **Max Image Rate**, the camera will maintain the set image rate as the priority and will not adjust the exposure beyond what can be recorded for the set image rate.
  - When set to **Exposure** the camera will maintain the exposure setting as the priority, and will override the set image rate to achieve the best image possible.
- **Maximum Iris:** You can limit the largest iris opening the lens will use by setting a maximum iris opening. This value is an f-number. It is also given in EV relative to the widest possible opening of the lens. This setting is only available when the **Iris** setting is set to **Automatic**.

  The iris opening also affects how much of the scene is in focus. The smallest f-number (0 EV) sets the iris to the widest possible opening. This allows the most light into the camera, but places less of the scene in focus. Larger f-numbers (negative EV) result in a smaller maximum opening, placing more of the scene in focus. The camera will automatically correct for the decreased light by using a higher gain or a longer exposure time.
- **Preferred Iris:** You can set an ideal iris opening to give a well-exposed and well-focused image in the most frequent lighting conditions. This value is an f-number. It is also given in EV relative to the widest possible opening of the lens. This setting is only available when the **Iris** setting is set to **Automatic**.

  > **Note:** The Preferred Iris value must be less than or the same as the Maximum Iris value.

  The smallest f-number (0 EV) sets the iris to the widest possible opening. This allows the most light into the camera, but places less of the scene in focus. Larger f-numbers (negative EV) result in smaller openings, placing more of the scene in focus. The camera will automatically correct for the decreased light by using a higher gain or a longer exposure time.
- **Backlight Compensation:** If your scene has areas of intense light that cause the overall image to be too dark, you can enable Backlight Compensation to achieve a well-exposed image.
- **Iris:** You can allow the camera to control the iris by selecting **Automatic**, or you can manually set it to **Open** or **Closed**.

- **Maximum Gain:** You can limit the automatic gain setting by selecting a maximum gain level.

  By setting the maximum gain level for low-light situations, you can maximize the detail of an image without creating excessive noise in the images.
- **Equalization:** This setting allows you to adjust the camera image to equalize the color difference between warm and cold objects. A lower value will make the warm objects more noticable. Increasing the value will result in a more balanced video image.

6. If you are configuring a PTZ dome camera, you can define additional settings in the Advanced Filters area.
   - **Enable Digital Defog:** If your PTZ dome camera is installed in a foggy environment, select this check box to increase the video contrast to help make objects more visible in the scene. From the **Defog Level** drop-down list, select one of the available options: **Low**, **Medium**, **High**. To disable Digital Defog, uncheck the box.
   - **Enable Image Stabilization:** If your PTZ dome camera is mounted to a pole or other surface that may be prone to shaking or vibrations, select this check box to enable the camera's built-in image stabilization feature.

     Note: On H5A-PTZ cameras, enabling Image Stabilization will reduce the zoom capability from 36x to 30x zoom.
7. Click **Apply** to save your changes.

Adjustments

On the Adjustments page, you can control the video image color, contrast, and brightness settings.

The Adjustments page also includes an image panel that displays the camera's live video stream. When you click **Apply** to save your changes, the video stream is updated.

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

1. In the left menu pane, select **Image and Display** > **Adjustments**.
2. Adjust the video image as required.

   You can either use a preset configuration, or you can create your own custom configuration. Use the **Preset** drop-down list to select the preferred configuration:

   a. **Avigilon:** This preset provides the recommended balance of brightness and color for video surveillance.

   b. **Standard:** This preset is configured for general day/night changes in an indoor or outdoor scene.

   c. **Vivid:** This preset provides increased color and brightness for a more saturated image.

d. **Custom:** Select this option to manually adjust the following image settings:

> **Note:** The Brightness and Contrast settings are disabled if Wide Dynamic Range is enabled.

- **Saturation:** You can adjust the video's color saturation by entering a percentage number.

  0 creates a black and white image, while 100 creates intense color images.
- **Sharpness:** You can adjust the video's sharpness by entering a percentage number.

  0 applies the least amount of sharpening, while 100 applies the most sharpening to make the edges of objects more visible.
- **Brightness:** You can adjust the video's brightness by entering a percentage number.

  0 creates a dark image, while 100 creates a light-filled image.
- **Contrast:** You can adjust the video's contrast by entering a percentage number.

  0 applies the least amount of contrast, while 100 applies the most contrast between objects in the image.

3. Use the **White Balance** drop-down list to select how the white balance settings are controlled:
   - **Automatic**: The camera will automatically control the white balance.
   - **Custom**: Manually set the **Red** and **Blue** levels.

   Dominant Color Compensation (if available): This option enables an alternate auto white balance algorithm which should be used when a large area in the field of view contains one color. For example, a camera that is overlooking a grass field. For this example, the Dominant Color Compensation white balance mode will improve the white balance to a more neutral color.
4. Move the **Temporal Filter Strength** slider slightly to the left or right to adjust the amount of noise vs. blur in the scene. A temporal filter reduces image noise by averaging the noise over several frames.

   > **Tip:** Start by making small adjustments only because applying excessive changes may degrade the overall image quality.

   If the image looks noisy, move the slider to the right to reduce the amount of noise in the scene and decrease the bandwidth used.

   If the image looks blurry, move the slider to the left to reduce the amount of blur in the scene and increase the bandwidth used.

   By default, the slider is set to the middle, or 50.

   > **Note:** On H4 IR PTZ cameras, the default value is set to 80. On H6A PTZ cameras, the default value is set to 60.
5. Click **Apply** to save your changes.

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 multi 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.

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.

Follow these steps for each of the primary, secondary, and tertiary streams to change the compression and image quality settings for each stream.

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 32.

2. In the **Max Image Rate** field, enter how many images per second you want the camera to stream over the network.

   Note: Adjusting the image rate across the 30 fps boundary will stop the video stream for a few seconds.

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.

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 29.

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 the previous page.

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 Configuration

On the Analytics page, you can configure Self Learning Analytics.

1. Select the **Enable Self Learning** checkbox to enable self learning analytics.
2. Select the **Suspend Self Learning** checkbox to temporarily disable self learning analytics.
3. Click the **Reset Self Learning** button to reset self learning.

   > **Important:** This action can not be undone.

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

Extended Settings

On the Extended Settings page, you can configure ONVIF Settings.

1. Select the **Enable Multi-Packet XML Documents** checkbox to enable multi-packet XML documents to reduce metadata size. Only for Video Management systems that support multi-packet XML documents.
2. Select the **Enable Analytics Options Requests** checkbox to enable the GetAnalyticsModuleOptions and GetRuleOptions Requests.
3. Select the **Enable Analytics XML Metadata** checkbox to send analytics metadata in the XML metadata stream.
4. Select the **Enable Run-Length Encoding of Motion Mask** checkbox to enable run-length encoding of the motion mask. Only for Video Management Systems that do not require an un-encoded mask.
5. Select the **Enable Supplemental Events** checkbox to send supplemental events not defined by ONVIF that may be useful to some Video Management Systems.
6. Select the **Enable Singleton Analytics Events** checkbox to send singleton Analytics events instead of property events.
7. 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.

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.

   Note: For Avigilon H4 PTZ cameras, the privacy zone may shift slightly when the camera performs an e-flip. If this is a concern, we recommend drawing a slightly larger privacy zone or disabling e-flip for that camera. For more information on disabling e-flip, see *Defining PTZ Limits* on page 39.

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. 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. Alternatively, you can select the privacy zone you want to delete from the list and click **Remove**.

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 35.

If you are using a CryptR micro card in the camera's SD slot for FIPS level 3 encryption, you will not be able to use onboard storage in the SD card slot. For camera's with 2 microSD slots you can only use the slots for either storage or the CryptR micro card, both options cannot be used at the same time.

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.
- Cameras with firmware older than 4.4.0.X will have the option to **Enable ONVIF Profile G** when they upgrade their firmware.

  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.

If you are using a CryptR micro card in the camera's SD slot for FIPS level 3 encryption, you will not be able to use onboard storage in the SD card slot. For camera's with 2 microSD slots you can only use the slots for either storage or the CryptR micro card, both options cannot be used at the same time.

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. The **Type** drop-down list is used for cameras that can have the day/night mode triggered by an external light detector. You will only see this option on cameras that support this feature. If the digital input will be used to control the day/night settings, select **Force IRCF** in the Type drop-down list.

        For day/night switching controlled by an external digital input, the **External** option must be selected as the **Day/Night Mode**. For more information on configuring the day/night mode, see *Image and Display* on page 19.

    d. 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. Check the **IRCF to Out** box to allow the camera's IR Cut Filter to control the external output.

        This feature is typically used when the camera is connected to an external IR illuminator. Once enabled, the IR illuminator is turned on when the camera's IR Cut Filter is in monochrome mode.

    d. 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.
    e. Click **Trigger** to manually trigger the digital output from the web interface.
    f. Click **Apply** to save your changes.

Washer

On the Washer page, you can activate the washer and wiper sequence to clean the window on H5A Rugged PTZ cameras and H5A Explosion- Protected PTZ and bullet cameras. The washer function is supported if these cameras have the optional washer installed. See the table below for the camera and washer models that support the washer function.

Camera Model	Camera Part Number	Washer Part Number
H5A Rugged PTZ	H5A-RGDPTZ-DP36	AVWASPT0V5L5M00 / AVWASPT0V23L11M00 / AVWASPT1V23L30M00 / AVWASPT3V23L30M00
H5A Explosion-Protected PTZ	H5EXPTZ-x0-BO30	AVGEX-WASEX2T4AT / AVGEX-WASEX2T4IN / AVGEX-WASEX2T4KC / AVGEX-WASEX2T4GOR
H5A Explosion-Protected Bullet camera	H5EX-xx-BO1	

To activate the washing sequence:

Note: On H5A Rugged PTZ and H5A Explosion-Protected PTZ cameras, you will need to configure a PTZ preset position where the glass viewing window is angled so that it is directly in front of the washer nozzle. For more information on setting up PTZ presets, see *Using Camera Presets* on page 4.

1. Click **Washer** on the left menu pane.

   Select the **Enable Washer** checkbox.
2. In the **Washer Location** drop-down list, select the PTZ preset position that has been configured to position the glass window of the PTZ camera in front of the washer's nozzle.
3. Set the **Wiper On Delay** to control the amount of time between the washer spray starting and the wiper function starting.
4. Set the time that the washer will spray in the **Washer Period** field.
5. Set the time that the wiper function will continue in the **Wiper Off Delay** field.
6. Click **Apply** to save your settings.

Tip: We recommend your washing sequence is set up so the Wiper On Delay is at least 4 seconds to give the washer time to spray the window. The Wiper Off Delay should be at least 8 seconds longer than the Washer Period to give the wiper time to clean the window after the spray has stopped.

PTZ Camera

Avigilon H4 PTZ cameras use many of the same settings as other High Definition IP cameras. The following settings are only available to PTZ cameras.

Creating PTZ Tours

For PTZ cameras, you have the option of running Tours from the Live View page. Tours allow the PTZ camera

to automatically move between a series of preset positions, and can be set to pause at each preset for a specific amount of time for video monitoring.

> **Note:** All the required presets must be added before a new tour can be created. For more information, see *Using Camera Presets* on page 4.

To create a tour, complete the following:

1. From the left-menu pane, select **PTZ Tours**.
2. Click **Create New Tour**.

   The New Tour dialog is displayed.
3. In the **Name** field, give the tour a name.
4. In the **Mode** drop-down list, select one of the following:
   - **Sequential:** the PTZ camera will go to each preset in the set order.
   - **Random:** the PTZ camera will go to each preset in random order.
5. Select the **Set as default tour** check box if you want this tour to run automatically.
   - The Default Tour Idle Start Time (Minutes) field is now enabled, enter the amount of time the PTZ camera must be idle for before this tour automatically begins.
6. In the **Tour Pause Duration (Minutes)** field, enter the amount of time before the tour repeats. Tours repeat until manually stopped, or until other PTZ controls are used.
7. To add a preset, click **Add Preset** and a preset is added to the list.
   a. In the Preset column, select a preset from the drop-down list.
   b. In the Move Speed column, enter a percentage of the maximum speed defined on the PTZ Limits page. This option sets how fast you want the PTZ camera to move to this preset. The Move Speed is 80% by default.
   c. In the View Time column, enter the amount of time you want the PTZ camera to stay at this preset position. The view time is 10 seconds by default.
   d. Continue until all the presets for this tour have been added.
8. To remove a preset, click the **(x)** icon to the far right of the preset.
9. To re-order a preset, click the up and down arrows or click and drag the left edge of the preset through the list.
10. Click **Apply** to save the tour.

Editing PTZ Tours

1. From the left menu pane, select **PTZ Tours**.
2. Click **Edit** beside the tour that you want to edit.
3. Make the changes you need.

4. To undo the changes that you've made, click **Discard Changes**.
5. Click **Apply** to save your changes.
6. To delete the tour, click **Delete Tour**. Click **OK** when the confirmation dialog box appears.

Defining PTZ Limits

Depending on where the PTZ camera is installed, you may want to limit the movement and zoom of the camera so that obstructions are never in view. For example, if the PTZ camera is installed close to the side of a building, you can set the limits so that the PTZ camera cannot move to show the wall it is installed against.

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

1. From the left menu pane, click **PTZ Limits**.
2. To limit the maximum movement range, you can do one of the following:
   - In the image panel, move the PTZ camera as far left as you want to display then click the **From** icon for the Pan Limit. Move the camera to the farthest point to the right and click the **To** icon. Repeat this procedure for the Tilt Limit, only move the camera up and down. For information about moving the PTZ camera, see *Using the PTZ Camera Controls* on page 5.
   - Below the image panel, you can set the Pan and Tilt Limit by adjusting the position of the two black dots on each circle. The gray area shows the set degree of movement. The Pan Limit sets the horizontal movement range and the Tilt Limit sets the vertical movement range.

     The blue arrow helps you identify where the camera is currently pointing.
3. To set the **Lens Zoom Limit**, enter a maximum zoom level. Enter a number between the available range displayed on the right.
4. To set the **Preset Speed Limit**, enter a maximum number of degrees per second to limit the speed that the camera is permitted to move to each preset location. Enter a number between the available range displayed on the right.
5. To set the **Pan/Tilt Speed Limit**, enter a maximum number of degrees per second to limit the speed that the camera moves when you manually control its mechanical pan and tilt. Enter a number between the available range displayed on the right.
6. To allow the camera to automatically correct the video image when the camera tilts more than 90°, select the **Enable E-Flip** check box. When this option is disabled, the video image is upside down when the camera tilts more than 90°.
7. To enable Digital Zoom, select **On**.
8. Click **Apply** to save your settings.

Enabling the PTZ Compass Overlay

Avigilon PTZ cameras that support the PTZ Compass overlay feature can have the camera's direction overlayed on the video image. The direction displayed is based on the position of the camera. The compass overlay information may be useful for PTZ cameras that are mounted in an outdoor environment.

To enable and calibrate the PTZ compass overlay:

1. From the left-menu pane, select **PTZ Compass**.
2. Check the **Enable Compass Overlay** checkbox.

   The first time you enable the compass feature you will also have to calibrate the compass direction:

   a. After enabling the compass overlay, the text *Compass uninitialized* will appear in the upper-left corner of the camera's video stream.

   b. Use the PTZ controls to point the camera in one of the cardinal directions: East, West, North or South. Try to be as exact as possible.

   c. Once the you are satisfied with the direction you have pointed the camera, click the corresponding **Set** button in the **Compass Calibration** area.

      For example, click **Set East** if you pointed the camera to the East point. The overlay text on the image would now change to *90.00° E*.

   d. If you made an error in the compass calibration setting, click **Uninitialize Compass** and start over moving the camera and calibrating the direction.
3. Once the compass direction has been calibrated, you can enable and disable the compass overlay by checking and unchecking **Enable Compass Overlay**. The compass feature will retain the direction calibration and does not have to be re-calibrated every time you enable the overlay.

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:
   a. Use the **Line in Gain** setting to adjust output of the microphone that is built into the camera.
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, including PTZ controls.
    - **Operator**: has access to the Live View and PTZ controls 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 and optional PTZ controls, but cannot access any of the Setup pages. To enable the PTZ controls, select the Use PTZ Controls check box.
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.

- To upgrade the camera firmware, see *Upgrading the Camera Firmware* below.
- Click **Download** to Download Bug Report.
- Click **Reboot** to restart the camera.
- Click **Restore** to revert the camera firmware back to the factory default settings.
- Click **Soft Reset** to reset the camera to factory default settings, except for network 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.

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.

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.
   - **Kernel Logs (debug)** — Logs of debug messages.
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.
   - **Debug** — troubleshooting information sent by the camera to aid in diagnosing issues.
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.

Cameras that have been connected to use seamless power failover will show both power sources. For these cameras, the Aux power source is the priority power source.

Troubleshooting

Video Does Not Display After Powering the Camera

> **Note:** The following troubleshooting case only applies to H4 IR PTZ cameras that are powered up in a cold environment of -10°C to -40°C (14°F to -40°F) or lower. Properly powering the camera at this lower temperature requires 95 W PoE or an auxiliary power supply.

Up to a 60 minute startup delay may be necessary to warm up the camera when powering up in a cold environment below -10°C (14°F). During this cold start delay, video will not display and errors may be generated in ACC. If you are viewing video in the web interface you will see a blue screen and message about being in cold start mode. Video transmission will start and the errors will stop once the camera has warmed up.