

Video Intercom Web Interface User Guide

Avigilon H4 Video Intercom Camera Model:

H4VI-RO1-IR

Copyright

© 2016 - 2022, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, HDSM SmartCodec, AVIGILON CONTROL CENTER, ACC, ACCESS CONTROL MANAGER, and ACM are trademarks of Avigilon Corporation. Android is a trademark of Google LLC. Apple, Safari and Mac are trademarks of Apple Inc, registered in the US and other countries. Firefox is a registered trademark of the Mozilla Foundation in the US and other countries. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark. Covered by one or more claims of the patents listed at patentlist.hevcadvance.com.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

PDF-VIWebUI-A

Revision: 2 - EN

20220824

Table of Contents

Introduction	1
System Requirements	1
Other Web Interface Guides	1
Accessing the Camera Web Interface	2
Creating the Initial User and Logging In	2
Logging In	3
Live View	4
Saving a Still Image	4
Setup	5
General	6
Network	7
Configuring 802.1x Port-Based Authentication	9
Switching 802.1X Authentication Profiles	10
Deleting an 802.1X Authentication Profile	10
Configuring SNMP	10
IP Filter	11
Advanced Settings	12
Image and Display	14
Adjustments	18
Compression and Image Rate	19
Enabling HDSM SmartCodec™ Technology Settings	20
Viewing the RTSP Stream URI	21
Accessing the Still Image URI	22
HDSM SmartCodec Technology Advanced Settings	22
Motion Detection	22
Tamper Detection	23
Tamper Detection Switch	24
Analytics	24
Privacy Zones	25
Setting a Privacy Zone	25
Deleting a Privacy Zone	25
Storage	25
Enabling Onboard Storage	26
ONVIF Profile G	26
Downloading Recorded Video from the Web Interface	27

Downloading Recorded Video from the SD Card	27
Deleting Recorded Video	28
SD Card Failures	28
Digital Inputs and Outputs	29
Microphone	30
Speaker	30
Intercom	31
SIP Peer to Peer Configuration	31
SIP Server Configuration	32
SIP Network Settings	33
DTMF Supported Standards	33
Configuring DTMF Codes	33
Adding a DTMF Code	34
Modifying a DTMF Code	34
Deleting a DTMF Code	34
SIP Video Settings	34
Audio	35
Users	36
Adding a User	37
Editing Users and Passwords	37
Removing a User	37
Keeping Usernames and Passwords After Firmware Revert	37
System	38
Upgrading the Camera Firmware	38
Device Log	39
Disable WebUI	39

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.
- [PTZ Camera Web Interface Guide](#) — for pan, tilt, and zoom 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.
- [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.
- Avigilon Camera Configuration Tool — 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

Cameras manufactured after January 1, 2020, 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.

Tip: Cameras manufactured before January 1, 2020, have a default username and password you can use to log in. For more information, see *Logging In* on the next page.

If the camera is in the factory default state, 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. It is recommended to use a secure and complex password.
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

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 37.

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 25.
- 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 19.

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 27.

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 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**
5. 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* on the next page.

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.
6. 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.

Note: You can only set the HTTPS port, the RTSP port, and the NTP Server in the camera web interface.

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 1.2** is recommended for increased security.
 - **TLS 1.1** 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.
 - **IR Illuminator Status:** a trap notification will be sent when the status of the H4 multisensor camera's IR LED ring 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**.

Advanced 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 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 Advanced 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 Secure Element** enables the onboard trusted platform module (TPM) to securely store your encryption keys. Only cameras that come with the onboard NXP Secure Element TPM will display this option.
 - **CRYPTR micro** enables the installed CRYPTR card to securely store your keys, meeting FIPS 140-2 level 3 requirements.

Important: Switching the setting to CRYPTR micro will cause the camera to generate a new key and self-signed certificate. Some certificate and key management may be required when you enable this setting. If your previous keys were signed by a certificate authority (CA), the newly generated keys will also need to be signed by the CA to keep the connection to your camera secure. The Camera Configuration Tool (CCT) can be used to generate a Certificate Signing Request (CSR) from the camera and to upload the signed certificate back to the camera. For more information, see the *Camera Configuration Tool User Guide*.

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.

Once CRYPTR encryption is enabled, you can access the **CryptR Log** page by selecting it in the side menu. When the CRYPTR micro's internal audit log reaches 80% capacity, entries are automatically pulled from the CRYPTR micro, logged to the camera's syslog, and the CRYPTR micro's audit log is cleared out. The **CryptR Log** page will only show entries that haven't been logged to the camera's syslog yet.

Note: If the CRYPTR micro card is ejected or becomes unusable while it is inserted in the camera and enabled, the camera will restart in FIPS 140-2 mode. If the card is re-inserted into the camera, CRYPTR micro will need to be re-selected as the Encryption Engine to continue using the CryptR micro card to store your keys.

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 out, move the slider towards the right.
 - To zoom in, 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).
- 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

- **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:** You can manually enable or disable the IR illuminators that are installed on the camera.
- **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.

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, change the Backlight Compensation value until you 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 noticeable. Increasing the value will result in a more balanced video image.
- **Color Palette:** You can change how information captured from thermal cameras is represented by selecting a Color Palette. You can choose one of the following options:
 - WhiteHot - Grayscale. White represents hot, black represents cold.
 - BlackHot - Grayscale. Black represents hot, white represents cold.
 - Rainbow - Multicolor. Red represents hot, blue represents cold.

6. 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.

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.

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 H.264 IP cameras have dual stream capabilities. If the camera's streaming format is set to H.264, 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 26.

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 **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 22.

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 page 22.

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 20.

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.

Tamper Detection Switch

Cameras with a tamper detection switch can detect attempts to dismount the device. When the tamper detection switch is activated, an event notification is forwarded to the ACC system and alarms can be triggered to alert operators.

In addition, if the Video Intercom camera is connected to the optional Safety Relay (H4VI-AC-RELY1), the event triggers the Safety Relay to go into its lock-out state. In this state, the Safety Relay persists in a lockout mode and keeps the door securely locked, only permitting exiting from the secure side. After a lockout, the clear button on the Safety Relay must be pressed to restore normal operation. For more information about the Safety Relay, see the *Safety Relay Installation Guide*.

If the ACC system is integrated with the Avigilon Access Control Manager (ACM) software, the event is forwarded to the ACM™ software and processed according to its configuration.

In the Tamper Detection Switch sub section, you can view the tamper switch status and configure the Safety Relay behavior.

1. The Status field reports the state of the tamper detection switch:
 - **No Tamper:** The tamper detection switch is in its normal operating state.
 - **Tamper Detected:** The tamper detection switch has been activated (or the camera is not properly installed). If the camera is connected to a Safety Relay, lockout mode is activated, keeping the door securely locked, only permitting exiting from the secure side.
 - **Disabled:** Tamper detection switch is not enabled on the camera.
2. Check **Enable Tamper Detection Switch** if you want the camera to send notifications when the tamper detection switch is activated. This option is enabled by default.
 - Notifications received by a Safety Relay connected to the camera will activate the lockout mode, keeping the door securely locked, only permitting exiting from the secure side.
 - Notifications received by the ACC system integrated with an ACM system are forwarded to the ACM system for processing according to its configuration.
3. Check **Trigger Tamper Detection Switch On Video Tamper** if you want sudden changes in the camera's view to be treated by the ACC system as though the tamper detection switch has been activated. This option is disabled by default.
4. Click **Apply** to save your changes.

CAUTION — After the Safety Relay enters the lock-out state, the clear button on the Safety Relay must be manually pressed to restore normal operation. Since video tampering is more prone to false events than physical tampering, this option is disabled by default.

Analytics

On the Analytics page, you can enable the camera to send ONVIF compliant analytics 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.

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.
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.

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 28.

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.

Note: For cameras with 2 microSD card slots, you will only be able to configure the microSD card that is inserted first, in either card slot. The second microSD card slot is reserved for future features.

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, you will only be able to configure the microSD card that is inserted first, in either card slot. The second microSD card slot is reserved for future features.

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 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:

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 14.

- 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.

Microphone

If a microphone is supported by the camera and is connected to the camera, you can adjust the gain on the Microphone page. The higher the gain setting, the higher the microphone volume.

- Enter a number between the available range displayed on the right then click **Apply**.

If you are configuring an Avigilon Fisheye camera, there are two fields available:

1. **Internal Microphone Gain** — configures the gain for the microphone that is built into the camera.
2. **External Source Gain** — configures the gain for any microphone that is connected to the audio input.
3. In either field, enter a number between the available range displayed on the right then click **Apply**.

Speaker

If a speaker is supported by the camera and is connected to the camera, you can adjust the volume on the Speakers page.

- Enter a number between 0 and 100 to set the speaker volume then click **Apply**.

Intercom

Use the settings on the Intercom page to setup the SIP connection for the Video Intercom. You can configure your Video Intercom to work with SIP or your VMS. If you are using SIP, you can configure for:

- **SIP Peer to Peer calling.** Used for configuring the Video Intercom to make a direct SIP call to a specific SIP phone. For more information, see *SIP Peer to Peer Configuration* below.
- **SIP/PBX Server calling.** Used to register the Video Intercom on the PBX server as one of the extensions, and then use the PBX server as a proxy for making calls to a SIP phone. For more information, see *SIP Server Configuration* on the next page.

If you want to use your Video Intercom with your ACC system, select **VMS** as the **Intercom Call Destination** and configure your Video Intercom settings on the Audio page and in the ACC Client. For more information, see *Audio* on page 35, and the *ACC Client User Guide*. The codec, volume and microphone settings on the Audio page will also affect SIP configurations.

Important: If any SIP configuration setting is changed while a call is ongoing, that call will be dropped when the changes are applied.

SIP Peer to Peer Configuration

SIP peer to peer calling configuration is a simple setup for locations that want to have the same SIP phone always answer calls from the Video Intercom, such as a security desk phone.

1. Select **SIP** as the **Intercom Call Destination**.
2. Configure the following SIP Peer To Peer Call Settings:
 - **Display Name:** Enter the name for the Video Intercom that will be displayed when calling the SIP phone. This field is optional and can be left empty.
 - **SIP Call Destination:** Enter the domain address of the SIP phone that the Video Intercom will dial. This must be a valid IPv4, IPv6, or DNS name.
 - **SIP Call Destination Port:** Enter the UDP port number of the SIP phone that the Video Intercom will dial. This must be a valid port number between 1 and 65534. The default port is 5060.

Note: Ports 1-1024 are reserved IP ports. SIP ports should be outside of this reserved range and also should not use any ports used by the ACC system.

- **Allow Incoming SIP Calls:** Enable this option to turn on SIP call auto-answering for the Video Intercom. With this option enabled, any SIP phone can make a call to the Video Intercom IP address or domain address to talk through the Video Intercom even if the visitor has not pressed the call button.
3. Click **Apply** to save your changes.

When a SIP phone user receives a call, they can answer the call and speak to the visitor or redirect the call to another SIP phone before answering the call. If the call is answered, you will no longer be able to redirect the call. If the visitor is approved to enter, the user can use their DTMF code to grant door access. For more information, see *Configuring DTMF Codes* on the next page.

SIP Server Configuration

SIP server configuration allows for more flexibility on setting up Video Intercom SIP calling. SIP servers are also called PBX servers. You can use the PBX server to set up call redirecting if the main SIP number is busy, as well as other options that are available from connecting to the PBX server. If the operator that usually answers a Video Intercom call is away, the extension can easily be changed to call another phone in the PBX domain.

Note: To use the Video Intercom with your PBX server, your server administrator will have to add and register the Video Intercom device to the PBX server. The username, authentication ID, and other information from the PBX server will be required when configuring the SIP Server Settings.

A PBX, or SIP, server usually includes proxy, registrar, and redirect functionality. Proxies route the calls and provide additional logic to incoming calls. Registrars accept SIP device registration requests and act as a location service for the SIP domain. Redirect servers redirect the client to contact an alternative SIP address.

1. Select **SIP** as the **Intercom Call Destination**.
2. Select the **PBX mode** checkbox.
3. Configure the following SIP Peer To Peer Call Settings:
 - **Display Name:** Enter the name for the Video Intercom that will be displayed when calling the SIP phone. This field is optional and can be left empty.
 - **Allow Incoming SIP Calls:** Enable this option to turn on SIP call auto-answering for the Video Intercom. With this option enabled, any SIP phone extension can make a call to the Video Intercom extension through the PBX server to talk through the Video Intercom even if the visitor has not pressed the call button.
4. Configure the following SIP Server Settings:
 - **SIP Server:** Enter the domain address of the SIP server used as registrar, proxy, and redirect server. This must be a valid IPv4, IPv6, or DNS name.
 - **SIP Server Port:** Enter the UDP port number that will be used to communicate with the SIP server. This must be a valid port number between 1 and 65534. The default port is 5060.

Note: Ports 1-1024 are reserved IP ports. SIP ports should be outside of this reserved range and also should not use any ports used by the ACC system.

- **SIP Username:** Enter the username that is configured for the Video Intercom in the PBX server. This field cannot be left empty.

- **Authentication ID:** Enter the username/ID that is used by the PBX registrar to authenticate the Video Intercom. This field cannot be left empty.
- **Password:** Enter the password that is used to authenticate the Video Intercom. This field is optional and can be left empty.
- **Domain:** Enter the domain name that the Video Intercom will register to. Typically this will be the same as the SIP server, but if your SIP server handles multiple domains, this will need to be confirmed. This must be a valid IPv4, IPv6, or DNS name.
- **Registration Duration:** Enter the time period, in seconds, that the Video Intercom will wait before re-registering with the SIP server. This must be a value greater than 0.

Tip: The Registration Status field shows the current registration status of the Video Intercom. If the Video Intercom is not successfully registered with the SIP server, the status will display the reason for unsuccessful registration.

- **PBX Call Destination:** Enter the extension number that the Video Intercom will use when a visitor makes a call. This field cannot be left empty.

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

When a SIP phone user receives a call, they can answer the call and speak to the visitor. If the visitor is approved to enter, the user can use their DTMF code to grant door access. For more information, see *Configuring DTMF Codes* below.

SIP Network Settings

You can modify the **SIP Port** and **RTP Base Port** values or use the default values. These both must be a valid port number between 1 and 65534. The SIP Port and RTP Base Port cannot be the same port, and cannot be the same as other camera ports assigned to the Video Intercom.

The RTP Base Port is the first port in a 2-port range, so make sure the input RTP Base Port and RTP Base Port+1 are not already in use.

DTMF Supported Standards

Select the checkbox for SIP info and/or RTC 2833 to have your DTMF codes supported by one or both of those standards. The default is to have both standards selected.

Configuring DTMF Codes

To use the Video Intercom with a SIP configuration, you will need to use the DTMF Codes page to setup the dual-tone multi-frequency signaling that will be used grant door access through the Video Intercom. DTMF uses the tones from the buttons on the phone to send the signal to the Video Intercom for access to be granted.

Tip: The DTMF codes will trigger output #1 on the Video Intercom for granting access. See the *H4VI Video Intercom Installation Guide* for more information on setting up the digital outputs.

Multiple DTMF codes can be added for cases where there are multiple operators and auditing of which operator granted access may be needed. The Video Intercom Device Log will contain a record of the DTMF codes that have been used. For more information, see *Device Log* on page 39.

Adding a DTMF Code

Note: If you have more than one DTMF code, please note that no 2 DTMF sequences are allowed to share a similar substring of a sequence.

For example, if one user has a DTMF sequence of *123*, then a second user cannot be configured to use a DTMF sequence containing *123*. For this example, sequences like *12345* or *21234* are considered invalid.

1. Click **Add** on the DTMF Codes page.
2. In the Add DTMF page, enter a **Name** for the DTMF code you are adding.
3. Enter the DTMF **Sequence**. This is the number sequence that operators enter on their SIP phone to grant door access.

Tip: DTMF sequences can consist of the numbers 0–9, #, or *. DTMF sequences should be at least 3 digits or longer.

4. Select which output the DTMF code will activate in the Triggers field. You can select **Output 1**, **Output 2**, or both. The output(s) you select will be triggered on the video intercom when the DTMF code is input during an intercom call.
5. Click **Apply** to save your DTMF code.

The new DTMF name and sequence will be listed on the DTMF Codes page.

Modifying a DTMF Code

You can change the name or sequence of a DTMF code by selecting it and clicking **Modify**. Make your changes and click **Apply** to save them.

Deleting a DTMF Code

To delete one or more DTMF codes, select them from the list and click **Delete**.

SIP Video Settings

SIP video will automatically be included with your SIP calls at the default settings if the phone and PBX server

supports video. Use the SIP Video Settings page to configure the settings for the video that will be displayed during SIP calls.

Note: SIP video calls also require you to have configured the SIP audio call settings. For more information, see *Intercom* on page 31.

The SIP video stream is only supported in the H.264 Format.

1. In the **Max Image Rate** field, enter how many images per second you want the camera to stream over the SIP call.
2. 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.
3. In the **Max Bitrate** field, enter the maximum bandwidth the SIP video can use.
4. In the **SIP Video Resolution** drop-down list, select the preferred image resolution.

Note: The SIP video call resolution cannot be set higher than 1920x1080. The only available resolutions to select will be equal to or less than 1920x1080. If the primary stream resolution is reduced to a lower resolution than the SIP Video Resolution setting, the SIP resolution will be automatically reduced at the same time.

5. In the **Min Keyframe Interval** field, enter the minimum number of frames between each keyframe.
6. In the video image, click and drag the SIP video zone so that it covers the area of the video image that you want to display during a SIP call.
Changing the SIP Video Resolution setting will change the size and shape of the SIP video zone.
7. Click **Apply** to save your SIP video settings.

Audio

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

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.

Echo cancellation and noise reduction are built into the Video Intercom. Echo cancellation removes the speaker output signal from the microphone signal, which prevents the operator at the other end from hearing an echo of their own voice. Noise reduction removes background noise from the microphone signal, and you can set the sensitivity to background noise. You can also set the speaker volume and the microphone output levels.

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.
 - b. Clear the **Echo Cancellation & Processing** check box to disable all audio processing, including echo cancellation, noise reduction, and auto gain control. This is enabled by default.
 - c. In the **Noise Reduction** field specify the noise reduction strength to apply to reduce background noise.

The default level of 7 is suitable for a moderately noisy environment, while a value in the range 1 to 3 is suitable for quiet indoor environments with little background noise.

In a noisy environment, strange-sounding background noise usually indicates that the **Noise Reduction** setting is too low. In this case, increase the value of this setting. Audio quality may be affected at settings higher than the default.

When set to **Off**, noise reduction is disabled completely.
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 **Output Level** slider to adjust the output of the microphone. The default level is 0 dB, and you can reduce the output level by as much as 40 dB . This volume level is applied after auto gain control and other processing. Lower the output level to match the volume from the Video Intercom to other devices.
 - b. Check **Auto Gain Control** to maintain the microphone output level to be as constant as possible. The microphone signal is increased when someone is talking quietly, and decreased when someone is talking loudly into the microphone. This keeps the resulting volume level constant for the operator.
 - c. There is a Microphone Muting drop-down menu for the Video Intercom that regulates the microphone's behavior in the ACC Client. For other cameras this option is not available.

Use the **Microphone Muting** drop-down menu to set the microphone's behavior. The default setting is **Never Mute**.

 - **Never Mute**: Allows the ACC Client users to always listen to audio from the camera at any time.
 - **Always Mute**: Prevents the ACC Client users from listening to audio from the camera. This may be required by some local privacy laws. When an intercom call is initiated, the ring tone will be muted and only the pop-up dialog will appear in the ACC Client.
 - **Unmute Only During Call**: Allows the ACC Client users to always listen to audio from the camera when an intercom call is in progress.
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.

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](https://www.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.
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.