AVIGILON™

Pro Camera Web Interface User Guide

Avigilon H4 and H5 Pro IP Camera Models:

H5PRO-B

H4PRO-B

MOTOROLA SOLUTIONS

© 2024, Avigilon Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Avigilon Corporation or its licensors.

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-PRO-WebUI
Revision: 1 – EN
2024-10-28



Table of Contents

Pro Camera Web Interface User Guide v
Web Interface System Requirements v
Accessing the Camera Web Interface vi
Creating the Initial User and Logging In vi
Logging In vii
Live View viii
Saving a Still Image viii
Setup ix
General x
Network xii
Configuring 802.1x Port-Based Authentication xiv
Switching 802.1x Authentication Profiles xv
Deleting an 802.1x Authentication Profile xv
Configuring SNMP xv
IP Filter xvi
Security Settings xvi
Managing Certificates xviii
Downloading Certificates xviii
Removing Certificates xviii
Downloading Certificate Signing Requests xviii
Uploading Certificates xix
Uploading CA Certificates xix
Creating Certificates xix
Image and Display xx
Adjustments xxiii
Compression and Image Rate xxv
Enabling HDSM SmartCodec™ Technology Settings xxvi
Viewing the RTSP Stream URI xxvi
Configure Multicast Streaming xxvii
Accessing the Still Image URI xxvii
HDSM SmartCodec Technology Advanced Settings xxvii
Streaming Settings xxviii
Motion Detection xxviii
Tamper Detection xxix
Analytics Configuration xxix
Create Analytic Events xxix
Classified Object Motion Detection xxix

Create a Motion Analytic Event xxx
Configure Self Learning Analytics xxxi
Suspend Self Learning xxxii
Reset Self Learning xxxii
Extended Settings xxxii
Privacy Zones xxxiii
Setting a Privacy Zone xxxiii
Deleting a Privacy Zone xxxiii
Storage xxxiii
Enabling Onboard Storage xxxiv
Enable SD Card Encryption xxxiv
ONVIF Profile G xxxv
Downloading Recorded Video from the Web Interface xxxv
Downloading Recorded Video from the SD Card xxxvi
Deleting Recorded Video xxxvi
SD Card Failures xxxvi
Digital Inputs and Outputs xxxvii
Audio xxxviii
Users xxxviii
Adding a User xxxix
Editing Users and Passwords xxxix
Removing a User xxxix
Keeping Usernames and Passwords After Firmware Revert xxxix
Camera Automation xli
Create and Manage Camera Rules xli
Manage Sequences and Email Actions xli
Create and Manage Sequences xlii
Create and Manage Email Actions xlii
Configure SMTP Server Information xlii
Edit SMTP Server Information xliii
Add Email xliii
System xliii
Upgrading the Camera Firmware xliv
Device Log xliv
Disable WebUI xliv
About Page xlv
Checking a Camera's Power Source xlv
More Information & Support xlvi

Pro Camera Web Interface User Guide

You can use the camera web interface to check the camera's status and image quality, edit camera settings, manage features and upgrade firmware.

Make sure you have completed the installation procedure and added the camera to the network before you try to access the web interface.

The supported features depend on the specific camera model. The features outlined in this guide apply to the following camera models:

H5PRO-B	H4PRO-B

Web Interface 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.

Accessing the Camera Web Interface

You can access the camera web interface using the camera's IP address. The IP address is assigned automatically once the camera is discovered on the network using either CCT, Unity Video or ACC. Make sure the computer you are using to access the web interface is connected to the same network as the camera you are trying to access.

The IP address is assigned automatically once the camera is discovered on the network using either CCT, Unity Video or ACC. You can find the IP address in the following places:

- Avigilon Unity Video or ACC – navigate to Site Setup and select the camera. Click Network Settings and chose how to obtain an IP address.
- Camera Configuration Tool – select the camera and navigate to the Network tab.

Follow these steps to access the web interface:

1. Find the camera's IP address.
2. Copy and paste the IP address into a web browser: http://*<device IP address>*/. Example: http://192.168.1.40/

   NOTE

   The web browser must be configured to accept cookies or the camera web interface will not function correctly.
3. Enter the username and password to log into 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 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.
- The default username for HD Pro and H3A cameras is `admin` and the default password is `admin`.



TIP

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

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 xxxiii.
- 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 xxv.

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 xxxv.

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. ### H5 Pro 40 MP and 61 MP Cameras Only

   Select the **Enable ONVIF compatibility** check box to enable your H5 Pro camera to use ONVIF® to connect to a third party VMS. ONVIF compatibility is required to connect to a third party VMS.

   > **IMPORTANT**
   >
   > Enabling ONVIF compatibility on a 40 MP or 61 MP H5 Pro camera will limit the resolution to 32 MP. The 32 MP video stream will be used by the 3rd party VMS and by the SD card if onboard storage is enabled. Disable the Enable ONVIF compatibility option to view the higher resolution options that are available. Connect your H5 Pro camera to an ACC system to enjoy the full resolution of your camera.

   Onvif is a trademark of Onvif, Inc.
5. ### H4 Pro Cameras Only

   Select the **Enable ONVIF compatibility** check box to enable ONVIF features on your H4 Pro camera.

   > **NOTE**
   >
   > The **Enable ONVIF compatibility** check box will not appear when configuring cameras that already have ONVIF enabled. New cameras have ONVIF enabled by default. Older cameras may have this check box appear after upgrading the camera firmware. Once the **Enable ONVIF compatibility** check box is enabled, you will be unable to disable ONVIF compatibility. If the camera is connected to the ACC system prior to enabling this feature, you will need to disconnect and then re-connect the camera to your ACC system.

6. From the **Mode** drop-down list, select the mode that the camera will operate in. The camera will reboot after you change the camera mode.
   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. This mode will disable H.265 on 26 MP H5 Pro cameras.
   - **High Framerate** – This mode will use the maximum image rate possible but will disable self-learning video analytics, Unusual Motion Detection (UMD), and tamper detection on the camera.
     On 26 MP H5 Pro cameras, the High Framerate mode will disable self-learning video analytics and Unusual Motion Detection (UMD). Tamper detection is not supported on H5 Pro cameras.

Models	Features Impacted by High Framerate
26 MP H5 Pro Cameras: 26C-H5PRO-B	◦ Self-learning video analytics disabled ◦ Unusual Motion Detection (UMD) disabled ◦ H.265 (H.265 is disabled in **Full Feature** mode)

   - **No Video Analytics** – This mode will disable video analytics. This option is for deployments where camera-based video analytics would interfere with other analytics integrations.
7. 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**
8. Use the **Font Size** field to make the font larger or smaller. The default font size is 24. You can make the font as small as 12 or as large as 120.
9. 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* 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.
10. 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. 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.

3. Uncheck the **Enable WS Discovery Protocol** checkbox to turn off the WS Discovery protocol. This option is enabled by default.
   WS Discovery is used to scan and find cameras on the same network. This is required when using the Camera Configuration Tool and certain Video Management Systems. You can turn off WS Discovery after installation as a security precaution.
4. If you need to customize the hostname, enter it in the **Hostname** field.
5. In the DNS Lookup area, select how the camera will obtain a Domain Name System (DNS) server address.
   - **Obtain DNS server address automatically**: select this option to automatically find a DNS server.
   - **Use the following DNS server addresses**: select this option to manually set DNS server addresses. You can set up to three addresses:
     - **Preferred DNS server**: assign the address of the preferred DNS server in this field.
     - **Alternate DNS server 1**: (optional) assign the address of an alternate DNS server to this field. In the case that the preferred server is not available, the camera will attempt to connect to this server.
     - **Alternate DNS server 2**: (optional) assign the address of another alternate DNS server to this field. In the case that both the preferred server and the first alternate server are unavailable, the camera will attempt to connect to this server.
6. In the Control Ports area, you can specify which control ports are used to access the camera. You can enter any port number between 1 and 65534. The default port numbers are:
   - **HTTP Port**: 80
     If you want to limit camera access to secure connections only, clear the **Enable HTTP connections** check box. HTTP Port access is enabled by default.
   - **HTTPS Port**: 443
   - **RTSP Port**: 554
   - **RTSP Replay Port**: 555
7. In the NTP Server area, indicate if you want the camera to use an NTP server to keep time.
   a. Select the NTP source to use for keeping time:
      - **Always use Avigilon Control Center NTP Server**. Select this option if you want the camera to keep time through the Avigilon Control Center™ software only.
      - **Always use external NTP server**. Select this option if you want to use an external NTP server only. Then configure the NTP server to use.
      - **Use Avigilon Control Center Server with a failover external NTP**. By default, Avigilon cameras keep time through the Avigilon Control Center software and will use an external NTP Server when not connected to an ACC server, if one is configured.
   b. If you are using an external NTP server, select how the server is configured:
      - **DHCP**.
      - **Manual**. Select this option and then enter the server address in the **NTP Server** field.
8. In the MTU area, set the Maximum Transmission Unit (MTU) size in bytes. Enter a number between the available range displayed on the right. You may want to lower the MTU size if your network connection is slow.

9. In the Ethernet Setting area, set the **Speed & Duplex** for your network connection. The Auto-negotiation (default) setting is the preferred setting for most cameras, and will negotiate the optimal speed and duplex setting for your network connection. If necessary, you can manually select the speed and duplex setting for your connection.
10. In the Security area, set the **Minimum TLS version** that the camera should use for encrypting the communication between camera and server and block older TLS versions that should not be used.
    - **TLS 1.3** is recommended for increased security.

      NOTE

      Please verify that this is supported by your VMS before enabling this option.

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

      NOTE

      Some cameras may also have the **TLS 1.1** options, which can be selected if it is required for backwards compatibility.
11. Click **Apply** to save your settings.

Configuring 802.1x Port-Based Authentication

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

1. In the left-menu pane, select **Network > 802.1x**.
2. On the Configure 802.1x Profiles page, select the preferred authentication method. You can configure multiple profiles. Be aware that you can only enable one profile at a time.
   From the **EAP Method** drop-down list, select one of the following and complete the related fields:
    - Select **PEAP** for username and password authentication.
        - **Configuration Name:** give the profile a name.
        - **EAP Identity:** enter the username that will be used to authenticate the camera.
        - **Password:** enter the password that will be used to authenticate the camera.
        - **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.

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.
   - **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.

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. This field is required.
   - *Subject Alternative Name (DNS)*: The alternative values associated with the certificate, e.g., email address, IP addresses, URIs, DNS names.
   - *Organizational Unit*: The name of the unit within the organization that is requesting the certificates.
   - *Organization*: The name of the organization requesting the certificates.
   - *Locality*: The geographic locality of the organization.
   - *State or Province*: The State (United States) or Province (Canada) associated with the organization.
   - *Country*: The Country where the organization is located.
2. Click the **Download** button to download the CSR file.

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.

Creating Certificates

1. In the *Valid Not Before* field, enter the date that the certificate becomes valid in the format: mm/dd/yyy. This field is required.



NOTE

You can also click the calendar icon to select a date using the calendar view.

2. In the *Valid Not After* field, enter the date that the certificate is no longer valid in the format: mm/dd/yyyy. This field is required.
3. Enter the following information:
    - *Common Name*: The primary hostname of the server. This field is required.
    - *Subject Alternative Name (DNS)*: The alternative values associated with the certificate, e.g., email address, IP addresses, URIs, DNS names.
    - *Organizational Unit*: The name of the unit within the organization that is requesting the certificates.
    - *Organization*: The name of the organization requesting the certificates.
    - *Locality*: The geographic locality of the organization.
    - *State or Province*: The State (United States) or Province (Canada) associated with the organization.
    - *Country*: The Country where the organization is located.
4. Click the **Create** button.
5. Click the **Make Active** button.
6. Click the **OK** button in the pop-up message.



IMPORTANT

If you activate the new certificate other certificates will be deactivated, and the page will be reloaded.

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).
     - 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 xxxvii.
   - **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 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, 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. 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. 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 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 xxxiv.
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.

   If the camera is operating in High Framerate mode, then the maximum image rate is increased. For more information on the High Framerate mode, see *General* on page x.
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

You can enable and configure HDSM SmartCodec settings on the *Video Configuration* page. HDSM SmartCodec helps isolate objects from the background areas. This reduces the camera's bandwidth usage by concentrating on the subjects of interest.

HDSM SmartCodec is turned off by default.



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 feature.
2. Enabling HDSM SmartCodec will turn on Idle Scene Mode. Uncheck the **Idle Scene Mode** checkbox to turn off this feature.
3. 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.
4. 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.
5. In the **Bandwidth Reduction** drop-down list, select one of the options:
    - **Low**
    - **Medium** (recommended)
    - **High**
    - **Custom**
6. 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.

Configure Multicast Streaming

Multicast streaming delivers a continuous stream of footage to multiple endpoints simultaneously. Cameras with multiple streams can stream to the multiple endpoints using different IP addresses and port numbers.

You can configure the primary, secondary and tertiary streams separately in the *Multicast* area on the *Compression and Image Rate* page of the camera web interface.

Follow these steps to configure multicast streaming settings for the streams as required:

1. Enter the IP address in the **Address** field.
2. Enter the port number in the **Port** field.
3. Enter a value between 1 and 255 seconds in the **Time To Live** field.

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.

Streaming Settings

On the *Streaming Settings* page, you can set the ONVIF Media Profile and configure Profile Settings.

1. Select an **ONVIF Media Profile** from the **Profiles** drop-down menu.
2. Select a profile from the **Video Source** drop-down menu.
3. Select a profile from the **Video Encoder** drop-down menu.
4. Select a profile from the **Audio Source** drop-down menu.
5. To enable **Metadata**, select metadata0 from the drop-down menu.
6. To disable **Metadata**, select None.
7. Click the **Apply** button to apply 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 AvigilonControl Center Client software. For more information, see the *AvigilonControl 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.
5. Once enabled, the H.264 camera can send motion alarm information to the VMS according to the appropriate ONVIF protocol.
6. 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 create analytic events and enable, suspend and reset self-learning analytics. You can also change the the analytics scene mode to optimize camera analytics.

Create Analytic Events

You can edit the Classified Motion Detection event and create motion analytic events on the *Analytics* page.

Classified Object Motion Detection

Once Classified Object Motion Detection is enabled, you can configure the rule and adjust the inclusion area. The inclusion area is shown as the green box overlaying the camera field of view. You can also add and arrange inclusion areas to make sure that the site is fully monitored.

1. Click **Edit** next to Classified Object Motion Detection in the *Events* area.
2. The default rule name is Smart Motion Rule. You can not edit the name of the rule.
3. Select one or more object types from the list of options: At least one object type is required.
    - Person
    - Vehicle
        - Car
        - Bus
        - Bicycle
        - Motorcycle
        - Pickup
        - Truck
        - Large
        - Truck
        - Van
4. Click and drag the slider to adjust the **Sensitivity** level. Lowering the sensitivity increases the chances of false negatives.
5. Use the up and down arrows to set the **Threshold Time** required to trigger an alarm.
6. Objects within the Inclusion area for longer than the threshold time will trigger an alarm.
7. Use the up and down arrows to set the **Timeout** before another alarm is triggered.
8. Click and drag the middle of the green square on the screen to move the inclusion area.
9. Click and drag the points to reshape the inclusion area.
10. Click **Add Exclusion Area** to add a new exclusion area.
11. Click **Reset Inclusion Area** to reset the size and shape of the inclusion area.
12. Select an Inclusion Area and click **Delete Exclusion Area** if you want to delete it.

    NOTE

    At least one Inclusion area is required.
13. Click **Save**.

Create a Motion Analytic Event

You can create Motion Analytic Events on the *Analytics* page. Motions Events trigger alarms when a certain activity occurs in the inclusion area. You can also add and arrange inclusion areas to make sure that the site is fully monitored.

1. Click **Add Event** in the Events area.
2. Enter a name for the Event in the Name field.
3. You can uncheck the **Enabled** checkbox if you want to enable it at a later time. The Enabled checkbox should remain checked if you want the event to be enabled immediately.
4. Select an activity type from the list:

- Objects in area
- Object loitering
- Objects crossing beam
- Object appears or enters area
- Object not present in area
- Objects enter area
- Objects leave area
- Object stops in area
- Direction violated

5. Select one or more object types from the list of options: At least one object type is required.
   - Person
   - Vehicle
   - Car
   - Bus
   - Bicycle
   - Motorcycle
   - Pickup
   - Truck
   - Large
   - Truck
   - Van
6. Click and drag the slider to adjust the **Sensitivity** level. Lowering the sensitivity increases the chances of false negatives.
7. Use the up and down arrows to set the **No. of Objects** required to trigger an alarm.
8. Use the up and down arrows to set the **Threshold Time** required to trigger an alarm.
9. Objects within the Inclusion area for longer than the threshold time will trigger an alarm.
10. Use the up and down arrows to set the **Timeout** before another alarm is triggered.
11. Click and drag the middle of the green square on the screen to move the inclusion area.
12. Click and drag the points to reshape the inclusion area.
13. Click **Add Exclusion Area** to add a new exclusion area.
14. Click **Reset Inclusion Area** to reset the size and shape of the inclusion area.
15. Select an Inclusion Area and click **Delete Exclusion Area** if you want to delete it.

    NOTE

    At least one Inclusion area is required.
16. Click **Save**.

Configure Self Learning Analytics

You can configure Self Learning Analytics on the *Analytics* page. The camera will perform self adjustments based on the activity in the field of view. This can significantly improve the accuracy of classified object detection.

Self-learning will progress based on activity detected in the field of view. Scenes with less activity will require staging during the learning phase. One example of staging would involve having a person walk through the field of view during learning.

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.

Suspend Self Learning

You can now stop the self-learning video analytics from continuing to learn the scene so that the camera continues to recognize objects correctly based on previous learnings and does not degrade its detection of objects when left to operate in sparse scenes.

The following scenarios are examples of when self learning should be suspended:

- People or vehicles are not expected in the device's field of view.
- Objects move at different heights. For example, overhead pedestrian bridges, train platforms, hills and underpasses.
- The device is in Indoor Overhead mode. Self learning is not used, even if enabled. All detected objects are classified as people.

Reset Self Learning

When the learning progress is reset, all learning data is cleared and the device needs to re-learn the scene. This prevents missed and false detections based on old data.

> **NOTE**
>
> Always reset Self Learning after a camera is physically moved or adjusted, or if the focus or zoom level is changed.

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.
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 xxxvi.

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. Select the **Enable Recordings Retention** checkbox to enable the camera to store recordings for a set amount of time, from a minimum of 5 minutes to a maximum of 2 years. You can assign the number of days, hours and minutes that the recordings will be stored.
5. 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.

Enable SD Card Encryption

You can enable SD card encryption to encrypt the video files as a security precaution.

IMPORTANT

Enabling or disabling encryption will format all inserted cards and erase all files on them.

1. Select the **Card Encryption** checkbox in the *Onboard Storage* area to enable card encryption.
2. Click the **Apply** button.

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* on the next page.

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 xx.

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.

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.
    - **Operator**: has access to the Live View but limited access to the Setup features. The user can access the General page, Image and Display page, Compression and Image Rate page, Motion Detection page, Privacy Zones page, Digital Inputs and Outputs page, Microphone page and the Speakers page. The new user can also configure onboard storage settings but cannot delete video recordings or format the SD card.
    - **User**: has access to the Live View, but cannot access any of the Setup pages.
4. Click **Apply** to add the user.

Editing Users and Passwords

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

    NOTE

    You cannot change the security group for the administrator account.
4. Click **Apply** to save your changes.

Removing a User

NOTE

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

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

Keeping Usernames and Passwords After Firmware Revert

To add a layer of security to protect the camera from theft, you have the option of keeping the camera's current usernames and passwords after a firmware revert.

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

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

IMPORTANT

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

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

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

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

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

Camera Automation

You can create rules and assign actions to automate camera functions and responses on the *Automation* page.

Create and Manage Camera Rules

On the *Rules* tab, you can review the list of defined rules or create a new rule.

Follow these steps to create a new rule:

1. Click the **Add Rule** button.
2. Under *When the following trigger happens*, select the **Analytics** option if you want to create an Analytics rule and then select one of the following Analytics types:
    - Smart Motion Rule – when the camera detects a specific motion event, e.g., classified objects in the scene. You can select from the list of motion rules you created on the *Analytics* page. See *Create a Motion Analytic Event* on page xxx for instructions.
    - Camera Tampering Rule – when the camera detects a person tampering with the camera itself.
    - Motion Detector – when the camera detects motion in the scene.
3. Alternatively, select the **SystemStatus** option if you want to create a system status rule and select the **SystemBooted** option. This rule triggers an action when the camera reboots.
4. You can click the **Simulate Trigger** button to test any rules that you have already defined using that trigger.
5. Under *And the following condition is true*, select an option:
    - Always – the rule will perform the action every time the selected trigger occurs.
    - Never – the rule will never perform the action, even if the selected trigger occurs. This can be used to temporarily disable a rule.
6. Under *Then perform this action*, select one of the following action types:
    - Email – sends an email when the selected trigger occurs and the condition is true.
    - Sequence – initiates a sequence of actions when the selected trigger occurs and the condition is true.
7. If you chose Email, select from the list of available email actions. If the email action you want isn't listed, you can create a new one by selecting **Add New** and filling out the form as described in the section titled *Create and Manage Sequences* under *Manage Sequences and Email Actions* below.
8. If you chose Sequence, select from the list of available sequence actions. If the sequence you want isn't listed, you can create a new one by selecting **Add New** and filling out the form as described in the section titled *Create and Manage Email Actions* under *Manage Sequences and Email Actions* below.
9. You can click the **Test Action** button to test the action.
10. Enter a Rule Name.
11. Click the **Save** button. The rule will be added to the *Defined Rules* list.
12. Click the ✎ icon to edit a rule.
13. Click the ⊗ icon to delete a rule.

Manage Sequences and Email Actions

On the *Actions* tab, you can create and configure the sequences or email actions that are used for the camera rules. This is helpful if you want to create reusable action types or edit the actions in one place.

IMPORTANT

Any changes you make to an action will affect all of the camera rules using it.

Create and Manage Sequences

You can click the **Sequence** button to review, edit, delete or add new sequences. The new sequence will appear on the *Sequence* list. You can use these sequences when creating rules.

Follow these steps to create a new sequence:

1. Click the **Add Sequence** button.
2. On the *Add Sequence* page, enter the following information:
    - Sequence Name – enter a descriptive name for the sequence action. This name is shown on the Add Rule page.
    - Wait before – enter the number of milliseconds you want the sequence to wait before performing the action.
    - Then perform this action – select an action type and choose the action rule. If you select Email as the action type, see Step 5 for instructions on how to add a new email action.
3. Click **Test** to test the sequence.
4. Click **Save**.

Create and Manage Email Actions

You can click the **Email** button to create, edit, delete or test email actions. You can also configure SMTP server information for the email actions.

IMPORTANT

Any changes you make to the SMTP server information will affect any rules that are already using that email.

Configure SMTP Server Information

If you are adding the SMTP server for the first time, the button is labeled **Configure SMTP** and the **Add Email** button is disabled and greyed out. See *Edit SMTP Server Information* on the next page for instructions on how to edit SMTP server information for existing SMTP configurations.

Follow these steps to configure SMTP Server information for the first time:

1. Click the **Configure SMTP** button.
2. Enter the following information:
    a. Enter the SMTP Server URL.
    b. Enter the Username on the server url you provided.
    c. Enter User password or app password for the username.
    d. Enter an email address for the sender's email.
3. Click **Save**.

Edit SMTP Server Information

Once an SMTP server has been configured, the **Configure SMTP** button changes to **Edit SMTP**, and the **Add Email** button becomes enabled.

Follow these steps to edit the SMTP Server information:

1. Click the **Edit SMTP** button.
2. Enter the following information:
    a. Enter the SMTP Server URL.
    b. Enter the Username on the server url you provided.
    c. Enter User password or app password for the username.
    d. Enter an email address for the sender's email.
3. Click **Save**.

Add Email

Follow these steps to create a new email action:

1. Click the **Add Email** button.
2. Enter a name for the Email Action.
3. Enter a recipient email address in the **Email To** field.
4. You can enter another email address in the **Email Cc** field, if required.
5. Enter the text that you want to use for the email's subject line in the **Email Subject** field.
6. Enter the text that you want the email to contain into the **Email Body** section.
7. Click **Save**.

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* on the next page.
- 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 page xxxix.

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 Page

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.

More Information & Support

For additional product documentation and software and firmware upgrades, visit support.avigilon.com.

Technical Support

Contact Avigilon Technical Support at support.avigilon.com/s/contactsupport.