avigilon™
TRUSTED SECURITY SOLUTIONS™

Web Interface User Guide

Avigilon Presence Detector™ Device

APD-S1-D

Avigilon Corporation
avigilon.com

PDF-DeviceWebUI-A

Revision: 1 - EN

20171016

Table of Contents

Introduction

Avigilon devices include a web interface that allows you to view the device status and configure the device through a web browser.

Before you access the web interface, make sure you complete all the procedures described in the device installation guide.

NOTE: Features and options are disabled and are not displayed if they are not supported by the device.

System Requirements

The web interface can be accessed from any Windows, Mac or mobile device using one of the following browsers:

- Microsoft Internet Explorer version 7.0 or later
- Mozilla Firefox version 3.6 or later
- Google Chrome version 8.0 or later
- Apple Safari version 5.0 or later
- Android™ 2.2 (Froyo) or later browsers
- Apple iOS version 5.0 or later browsers

Accessing the Device Web Interface

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

- Avigilon Control Center (ACC) software — Open the device Setup tab to see the details of the selected device .

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 device web interface will not function correctly.

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

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

   For example: http://192.168.1.40/

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

   The default username for most devices is `administrator` with no password.

   It is recommended that you add a password after your first login. For more information, see *Editing Users and Passwords* on page 9.

Live View

After you log in, the first page you see is the Live View. The Live View contains an indicator that displays the status of the APD™ device.

There are three states that can be displayed here: No Presence, Presence or Initializing. If the Status is No Presence then the time indicator shows the time passed since presence was last detected. If the Status is Presence the time indicator shows how long someone has been present, and if the status is initializing then the time indicator shows how long the device has been initializing.

When the status is Presence, then the upper right corner displays the line-of-sight distance to the closest moving object being detected. This is very useful information when doing a walk test to set the sensor's range setting and detection area.

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.

NOTE: Features and options are disabled and are not displayed if they are not supported by the device.

Setup

NOTE: Options are disabled and are not displayed if they are not supported by the device or if you do not have the required user permissions.

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

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

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

General

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

NOTE: Features and options are disabled and are not displayed if they are not supported by the device.

1. In the **Name** field, give the device a meaningful name.
2. In the **Location** field, describe the device's location.
3. Select the **Disable device status LEDs** check box to disable the LED indicators located on the device.
4. In the Time Settings area, select how the device keeps time.
    - If you prefer to manually set the device'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 device's date and time with an NTP server, configure the NTP server on the Networkpage.

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

Network

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

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

1. At the top of the page, select how the device 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 you need to customize the hostname, enter it in the **Hostname** field.
4. In the DNS Lookup area, select how the device 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 device 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 device will attempt to connect to this server.
5. In the Control Ports area, you can specify which control ports are used to access the device. You can enter any port number between 1 and 65534. The default port numbers are:
    - **HTTP Port**: 80

      If you want to limit device 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
6. In the NTP Server area, decide if you want the device to use a Network Time Protocol (NTP) server to keep time.

   By default, Avigilon devices keep time through external Avigilon Control Center™ software.
    - Select the **Use NTP server when not connected to an external Avigilon Control Center Server** check box to allow the device to keep time through an NTP server. You also have the option to manually set the device's time on the General page. For more information, see *General* on the previous page.
    - **DHCP:** select this option to automatically use an NTP server on the network.
    - **Manual:** select this option to manually enter a specific NTP server address in the **NTP Server** field.

7. 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.
8. Click **Apply** when you are done.

Configuring 802.1x Port Based Authentication

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

1. In the left menu pane, select **Network > 802.1X** page link.
2. On the Configure 802.1X Profiles page, select the preferred authentication method. You can configure multiple. 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 device.
     - **Password:** enter the password that will be used to authenticate the device.
   - 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 device.
     - **TLS Client Certificates:** select the PEM-encoded certificate file to authenticate the device.
     - **Private Key:** select the PEM-encoded private key file to authenticate the device.
     - **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 device. The uploaded files are used to generate a unique certificate to authenticate the device. 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 device, it is automatically enabled.

   Saved configurations are listed under **Saved 802.1X Configurations**.
4. To use a different authentication profile, select the saved configuration then click **Enable**.
5. 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 devices that are connected to the network. When SNMP is enabled, device status information can be sent to an SNMP management station.

On the SNMP page, you can configure the device's SNMP settings and choose the status information that is sent to the management station page. For more details on what status information or traps that will be sent, see the device'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, 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 request the device for status information through an SNMP Get request and receive trap notifications from the device.

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

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

        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 device temperature rises above or falls below the supported threshold. A notification will also be sent when the device temperature returns to normal.

    - **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 device. This deviceuses 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 device.

        b. **Password:** enter the password the management station must use with the chosen username.
4. Click **Apply** to save your changes.

Presence Detection

NOTE: Features and options are disabled and are not displayed if they are not supported by the device.

On the Presence Detection page, you can view the current status of the Avigilon Presence Detector Sensor, configure the detection settings, and enable and disable the device's range test mode.

The Presence Detection panel displays the same information as the Live View. Below this panel are the configurable settings for the device.

1. In the Configuration section, you can set:
    - Dwell Alarm Time:—The number of minutes a person must be present before an alarm event is forwarded to the ACC software.
    - Sensitivity:—Enter the threshold for the amount of change from the background model needed to determine presence in the zone for fine movement on a scale of 0 to 9 . The default setting is 7. It is unlikely you will need to change sensitivity.

      The higher the sensitivity the less movement needed to activate the sensor. In general, increasing sensitivity will lead to more detections but may lead to increased number of false positives. Decreasing sensitivity can reduce the number of false positives but may lead to a false negatives.
    - Detection Range: — Move the slider to adjust the outer range of the detection area, the line-of-sight distance from the Avigilon Presence Detector Sensor to the person being detected.
2. Use range-test mode to test the outer range of the detection area, which is the area for detecting larger movement. Range-test mode is not as sensitive to fine movement, such as respiration, as is the normal mode. It is intended to be used for installation purposes only.

   To activate Range-Test Mode, click the **Enter** button. The button is changed to **Exit** and the status changes to Enabled.

   While the device is in Range-Test Mode, reinitializing after applying a change to the Detection Range setting takes about 30 seconds, rather than the 2 minutes it takes in normal mode.

   Click the **Exit** button to leave Range-Test Mode. Reinitializing on exit takes 2 minutes.

   NOTE: The device automatically exits Range-Test Mode (and reinitializes) after one hour of configuration inactivity.
3. Click **Apply** to save your changes.

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 device. This option does not appear for devices 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 in the **Circuit State** drop down list. The options are:
        - **Normally Open**
        - **Normally Closed**
    c. Click **Apply** to save your changes.

       Once the digital input is connected to the device, 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 in the **Circuit State** drop down list.
    c. In the **Duration** field, enter how long the digital output is active for when triggered. You can enter any number between 100 and 3,600,000 milliseconds.
    d. Click **Trigger** to manually trigger the digital output from the web interface.
    e. Click **Apply** to save your changes.

    NOTE: The ACC Client software can be used to configure rules that automatically trigger digital output on various conditions, such as presence or dwell alarm events. Triggering the digital input or output from this panel is intended to help with installation. For information on configuring rules in the ACC Client software, see the *Avigilon Control Center Standard Client User Guide* or the *Avigilon Control Center Enterprise Client User Guide*.

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 username 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 device web interface.
    - **Operator:** has access to the Live View but limited access to the Setup features. The user can access the General page, Presence Detection page and the Digital Inputs and Outputs page.
    - **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 (Administrator)` user.

1. On the Users page, select a user from the list.
2. Click **Remove**.

Keeping Usernames and Passwords After Firmware Revert

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

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

Important: If you forget your own username or password after enabling this setting, your device warranty becomes void because you have disabled the primary method of restoring the factory default username and password.

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 may void your warranty.

   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 device.

System

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

- Click **Reboot** to restart the device.
- Click **Restore** to revert the device 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* above.
- To upgrade the device firmware, see *Upgrading the Device Firmware* below.

Upgrading the Device Firmware

To manually upgrade the device's firmware:

1. Download the latest version of the firmware .bin file from the Avigilon website (**http://avigilon.com/support-and-downloads/for-cameras-and-hardware/firmware-updates-and-downloads/**) and complete the following steps:
2. On the System page, browse and locate the downloaded firmware file.
3. Click **Upgrade**. Wait until the device upgrade is complete.

Device Log

The Device Log page allows you to view the device's system logs and the device 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 device 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 device encounters a serious error. These are the highest level log messages.
    - **Warning** — Sent when the device encounters a minor error such as an invalid username and password.
    - **Info** — Status information sent by the device. 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.