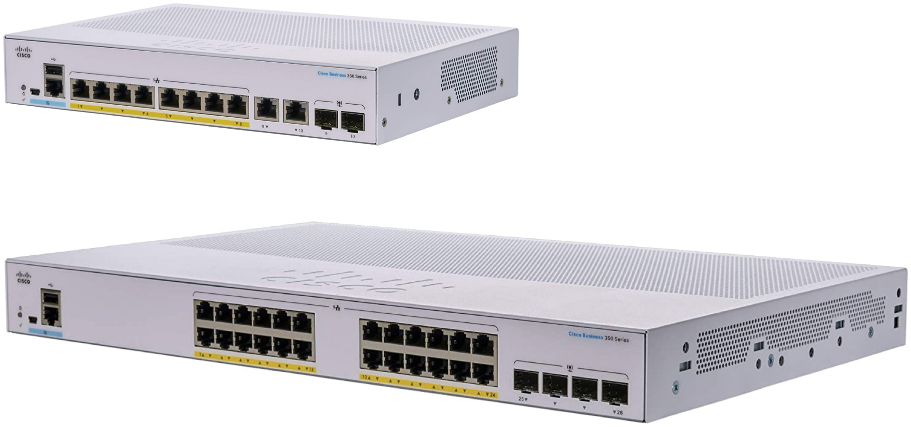
avigilon™



User Guide

8- and 24-Port Managed PoE Switches

CBS350-8FP-E-2G and CBS350-24FP-4G-xx

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-PoESwitch-A

Revision: 1 - EN

20220329

Safety and Regulatory Information

For safety and regulatory information, refer to the *Quick Start Guide* included with the switch.

Table of Contents

Introduction

Avigilon provides two network switches (manufactured by Cisco®) that can easily integrate into a video security system and connect many camera feeds to your security workstations and recording appliances. With only minimal configuration, these switches can be efficiently deployed into your video security network.

Before deploying these switches into your video security network, carefully read this guide, and any documentation referenced within it. This guide assumes that these PoE switches are connected with no change to their default settings. Provide this guide to the owner of the equipment for future use.

This guide provides configuration information for deploying the 8-port and 24-port managed PoE switches from Avigilon into a video security network using the Avigilon Control Center (ACC) video management system, Avigilon Network Video Recorders (NVRs), and Avigilon Appliances. It provides guidelines for connecting the switches and using their switch management applications.

Advanced configurations and installation recommendations can be found in the complete *Cisco Business 350 Series Switches Administration Guide*.

Configuring 8- and 24-Port Managed PoE Switches

The managed PoE switch can be managed over your IP network using the web-based interface, or by using the command-line interface through the console port. Using the console port requires advanced user skills and is only supported on certain models. In this guide we will only cover the web-based interface configuration.

The following table shows the default settings used when configuring your switch for the first time.

Parameter	Default Value
Username	cisco
Password	cisco
IP address	192.165.0.254/24

Configuring Your Switch Using the Web-based Interface

To access the managed PoE switch using the web-based interface, you must know the IP address that the managed PoE switch is using. The managed PoE switch uses the factory default IP address of 192.168.1.254, with a subnet of /24. When the managed PoE switch is using the factory default IP address, the System LED flashes continuously. When the managed PoE switch is using a DHCP server-assigned IP address or an administrator has configured a static IP address, the System LED is a steady green (DHCP is enabled by default).

Tip: Access to the managed PoE switch will be lost if its IP address is changed, either by a DHCP server or manually while tou are configuring the managed PoE switch through its web-based interface. . You must enter the new IP address that the managed PoE switch is using into your browser to reconnect to the web-based interface.

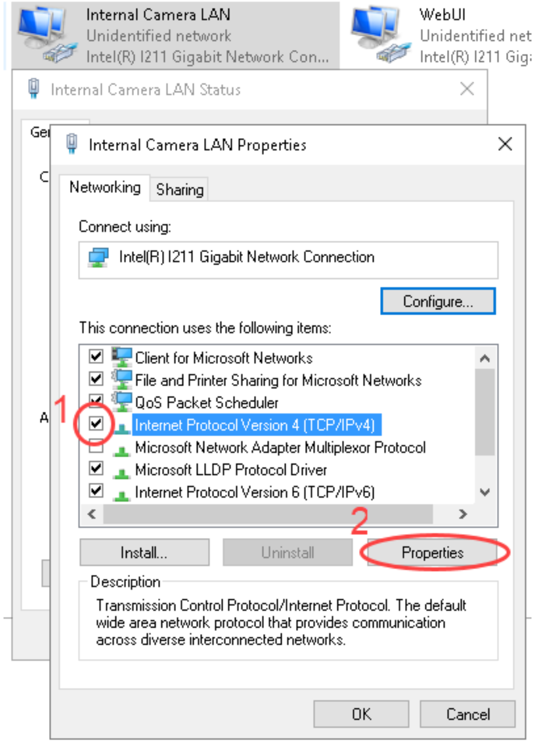
Accessing the Managed PoE Switch Web-based Interface

To access the web-based management interface on the managed PoE switch, you need to connect a computer to any PoE port on the switch, and configure the Network Interface Connection (NIC) on the computer to communicate with the switch on the local private network.

Note: If the IP address is assigned by DHCP, make sure that your DHCP server is running and can be reached from the switch and the computer. You may need to disconnect and reconnect the switch for it to discover its new IP addresses from the DHCP server.

After connecting the computer to the switch, complete the following steps on the computer:

1. Click **Start** > **Windows System** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
2. Click **Change adapter settings** from the left navigation menu. The Network Connections window is displayed.
3. Double-click on the icon for the NIC connected to the managed PoE switch to open the Status dialog box.
4. Click the **Properties** button open the Properties dialog box.



Internal Camera LAN
Unidentified network
Intel(R) I211 Gigabit Network Con...

WebUI
Unidentified net
Intel(R) I211 Gig

Internal Camera LAN Status

Internal Camera LAN Properties

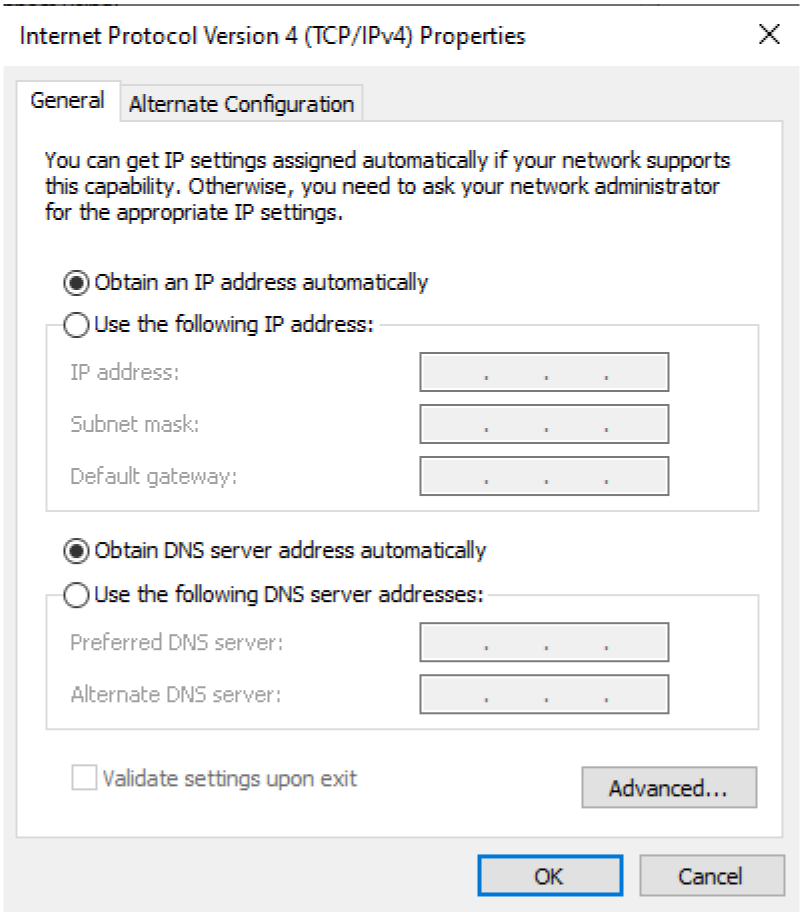
Connect using:
Intel(R) I211 Gigabit Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Click to select the **Internet Protocol Version 4 (TCP/IPv4)** checkbox and then click the **Properties** button to open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

6. If the IP address is not otained automatically using DHCP:
    a. Click to select **Use the following IP address**.
    b. Specify an IP address in the private IP address range for this connection with a subnet mask of 255.255.255.0. An address in a discrete range of normally unallocated addresses is recommended; for example, 198.168.1.20.
7. Open a web browser window, type the switch IP address in the address bar and press **Enter**. For example, http://192.168.1.254.
8. When the login page appears, choose the language that you prefer to use in the web-based interface and enter the username and password.
    - The default username is cisco.
    - The default password is cisco.
    - Usernames and passwords are both case sensitive.
9. Click **Log In**.

    If you have logged on for the first time with the default username and password:

   a. The Change username and Password page opens. The rules for constructing a new password are displayed.
   b. Enter a new username and password and confirm.

      Note: Password complexity is enabled by default. The password must comply with the default complexity rules.

   c. Click **Apply**.

10. The Getting Started page opens. You are now ready to configure the managed PoE switch.

Important: Make sure that any configuration changes made are saved before exiting from the web-based interface by clicking on the **Save** icon. Exiting before you save your configuration results in all changes being lost.

Basic or Advanced Display Mode

The managed PoE switch web-based GUI includes hundreds of configuration and display pages. These pages are divided into the following display modes:

- Basic—Basic subset of configuration options.

  Advanced—Full set of configuration options are available .

When switching from one mode to another, any configuration which was made on the page without Apply, is deleted. After connecting the computer to the switch, complete the following steps on the computer:

Configuration Wizards

This chapter contains the following sections:

- Getting Started Wizard
- VLAN Configuration Wizard
- ACL Configuration Wizard

Getting Started Wizard

The Getting Started Wizard will assist you in the initial configuration of the device.

1. In **Configuration Wizards** > **Getting Started Wizard**, click **Launch Wizard**.
2. Click **Launch Wizard** and **Next**.
3. Enter the fields in the General Information tab:
    - System Location — Enter the physical location of the device.
    - System Contact — Enter the name of a contact person.
    - Host Name — Select the host name of this device:
        - Use Default — The default hostname (System Name) of the device is: switch 123456, where 123456 represents the last three bytes of the device MAC address in hex format.
        - User Defined — Enter the hostname. Use only letters, digits, and hyphens. Host names cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).
4. Click **Next**.
5. Enter the fields in the IP Settings tab:
    - Interface — Select the IP interface for the system.
    - IP Interface Source — Select one of the following options:
    - DHCP — Select for the device to receive its IP address from a DHCP server.
    - Static — This is the recommended option for most of the applications. Select to enter the details of the static IP address of the device manually:
        - IP Address — Enter the IP address of the interface.
        - Network Mask — Enter the subnet mask for this address.
        - Default Gateway — Enter the default gateway IP address.
        - DNS Server — Enter the IP address of the DNS server.
6. **Click Next.**

7. Enter the fields in the User Account tab:
    - Username — Enter a new user name between 0 and 20 characters. UTF-8 characters are not permitted.
    - Password — Enter a password (UTF-8 characters are not permitted).
    - Confirm Password — Enter the password again.
    - Password Strength — Displays the strength of password.
    - Keep current username and password — Select to keep current username and password.
8. Click **Next**.
9. Enter the fields in the Time Settings tab:
    - Clock Source — Select one of the following:
        - Manual Settings—Select to enter the device system time. If this is selected, enter the Date and Time.
        - Default SNTP Servers—Select to use the default SNTP servers.

        > **Note:** The default SNTP servers are defined by name, thus DNS must be configured and operational. Manual SNTP Server—Select and enter the IP address of an SNTP server.
10. Click **Next** to view a summary of the configuration that you entered.
11. Click **Apply** to save the configuration data.

VLAN Configuration Wizard

VLANs are used to segment network traffic and isolate broadcast domains. Segmentation of a network helps to increase security, reliability, and efficiency of a network. In the context of the Avigilon Control Center end to end solution,VLANs are recommended to be used to isolate ACC Server incoming traffic (recordings) from ACC Server outgoing traffic (playback). Cameras should reside on the recordings VLANs not accessible by the remote monitoring workstation that should only access the ACC server through the monitoring VLAN.

VLANs consist in ports that are configured as Trunk and ports that are configured as Access:

- Trunk Ports - carry the traffic of more than one VLAN and are used to exchange traffic between more than one managed PoE switches having more than one VLAN configured.
- Access Ports - assigned to a single VLAN. The frames that arrive on an access port are assumed to be part of the access VLAN. This port type is configured on switch ports that are connected to devices such as cameras or the recorder.

> **Note:** Note: By default, all switch ports are assigned VLAN 1 and VLAN 1 cannot be modified or deleted prior to having other VLANs configured on the managed PoE switch.

The VLAN Configuration Wizard will assist you in configuring the VLANs. Each time you run this wizard, you can configure the port memberships in a single VLAN.

1. In **Configuration Wizards** > **VLAN Configuration Wizard**, click **Launch Wizard**.
2. Click **Launch Wizard** and **Next**.
3. Select the ports that are to be configured as trunk ports (by clicking with mouse on the required ports in the graphical display). Ports that are already configured as Trunk ports are pre-selected.
4. Click **Next**.
5. Enter the fields:
    - VLAN ID — Select the VLAN you want to configure. You can select either an existing VLAN or New VLAN.
        - New VLAN ID — Enter the VLAN ID of a new VLAN.
        - VLAN Name — Optionally, enter VLAN name.
6. Select the trunk ports that are to be configured as untagged members of the VLAN (by clicking with mouse on the required ports in the graphical display). The trunk ports that are not selected in this step become tagged members of the VLAN.
7. Click Next.
8. Select the ports that are to be the access ports of the VLAN. Access ports of a VLAN are untagged members of the VLAN. (by clicking with mouse on the required ports in the graphical display).
9. Click **Next** to see the summary of the information that you entered.
10. Click **Apply**.

ACL Configuration Wizard

An access control list (ACL) is an ordered list of rules used to filter network traffic. Using ACLs helps to increase security, reliability, and efficiency of a network. Each rule states what traffic is permitted or what's denied. When a packet attempts to enter or leave the managed PoE switch, it's tested against each rule in the list — from first to last. If the packet matches a rule, its outcome is determined by the conditions of the statement: If the first rule the packet matches is a permit statement, it's permitted; if it's a deny statement, it's denied.

The ACL Configuration Wizard will assist you when creating a new ACL, or editing an existing ACL. To add or modify an existing ACL, complete the following steps:

1. In **Configuration Wizards** > **ACL Configuration Wizard**, click **Launch Wizard**.
2. To create a new ACL, click **Next**. To edit an existing ACL, choose it from the ACL drop-down list and then click **Next**.
3. Enter the fields:
    - ACL Name — Enter the name of a new ACL.
    - ACL Type — Select the type of ACL: IPv4 or MAC.
4. Click Next.
5. Enter the fields:

- Action on match — Select one of the options:
  - Permit Traffic — Forward packets that meet the ACL criteria.
  - Deny Traffic — Drop packets that meet the ACL criteria.
  - Shutdown Interface — Drop packets that meet the ACL criteria, and disable the port from where the packets received.

6. For a MAC-based ACL, enter the fields:

Source MAC Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses
Source MAC Value	Enter the MAC address to which the source MAC address is to be matched and its mask (if relevant)
Source MAC Wildcard Mask	Select Any if all destination addresses are acceptable or User defined to enter a destination
Destination MAC Address	Select Any if all destination addresses are acceptable or User defined to enter a destination
Destination MAC Value	Enter the MAC address to which the destination MAC address is to be matched and its mask (if relevant)
Destination MAC Wildcard Mask	Enter the mask to define a range of MAC addresses. Note that this mask is different from other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value
Time Range Name	If Time Range is selected, select the time range to be used

7. For a IPv4-based ACL, enter the fields:

Protocol	Select one of the following options to create an ACL based on a specific protocol: • Any (IP) — Accept all IP protocols packets • TCP — Accept Transmission Control Protocols packets • UDP — Accept User Datagram Protocols packets • ICMP — Accept ICMP Protocols packets IGMP — Accept IGMP Protocols packets
Source Port for TCP/UDP	Select a port from the drop-down list
Destination Port for TCP/UDP	Select a port from the drop-down list
Source IP Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses
Source IP Value	Enter the IP address to which the source IP address is to be matched
Source IP Wildcard Mask	Enter the mask to define a range of IP addresses. Note that this mask is different from other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value
Destination IP Address	Enter the IP address to which the source IP address is to be matched

Destination IP Wildcard Mask	Enter the mask to define a range of IP addresses. Note that this mask is different from other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value.
Time Range Name	If Time Range is selected, select the time range to be used

8. Click **Next**.
9. Confirm that you want the ACL and ACE to be created.

   The details of the ACL rule are displayed. You can click Add another rule to this ACL to add another rule.
10. Click **Next** and enter the ACL Binding information:
    - Binding Type — Select one of the following options to bind the ACL:
    - Physical interfaces only — Bind the ACL to a port. In this case, click a port or ports on which to bind the ACL.
    - VLANs only — Bind the ACL to a VLAN. Enter the list of VLANs in the Enter the list of VLANs you want to bind the ACL to.
    - No binding — Do not bind the ACL.
11. Click **Apply**.

Enhancing Security and Customizing the Managed PoE Switch

The follow setting can be configured to further secure and customize your deployment.:

- Port security — Configure each port to allow access only to cameras or devices with specific MAC addresses. Unknown devices (those with MAC addresses not known to the switch) are automatically blocked. For more information, see Port Security below.
- Limiting power per port — If you have a mixture of cameras with different power requirements, you can configure the maximum limit of power used by individual PoE ports. This allows you to divert power to a single port that draws more power, such as a port connected to an IR PTZ camera. For more information, see PoE Power Limiting on the next page.

Port Security

After you have connected a camera or device to a specific physical interface and VLAN, secure the MAC address on the interface. After it is secured, a port allows access only to cameras or devices with specific MAC addresses. Unknown devices (those with MAC addresses not known to the switch) are automatically blocked.

To secure a port:

1. Click **Security** > **Port Security**.
2. Select an interface to be modified, and click **Edit**.
3. Enter the parameters.
   - **Interface**—Select the interface name.
   - **Interface Status**—Select to lock the port.
   - **Learning Mode**—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the Interface Status field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. From the options, select **Classic Lock**. The port is locked immediately, regardless of the number of addresses that have already been learned.
   - **Max No. of Addresses Allowed**—The number 0 indicates that only static addresses are supported on the interface.
   - **Action on Violation**—Select **Discard** to discard packets from any unlearned source.
4. Click **Apply**. Port security is modified, and the Running Configuration file is updated.

Note: For detailed information, refer to *Port Security*, in the *Security* chapter of the *Cisco Business 350 Series Switches Administration Guide*.

PoE Power Limiting

If you have a mixture of cameras with different power requirements, you can configure the maximum amount of power supplied to individual PoE ports. This allows you to divert power to a single port that draws more power, such as a port connected to an IR PTZ camera. You can allocate up to 60W on select ports and up to 30W on all other ports on the 24-port switch. You can allocate up to 30W on any port on the 8-port switch. You can adjust the power allocated to each port up to these maximums, as long as the total power allocated to all ports does not exceed the total power that the switch can supply. The total power available on the 8-port switch is 124W and on the 24-port port it is 382W.

To configure PoE on the device and monitor current power usage:

1. Click **Port Management** > **PoE** > **Properties**.
2. From the **Power Mode** options, select **Port Limit**.
3. Click **Apply**.

To configure PoE port limit settings:

1. Click **Port Management** > **PoE** > **Settings**.
2. Select a port and click **Edit**.
3. Enter the necessary power settings for the port in the fields that are displayed.
4. Click **Apply**. The PoE settings for the port are written to the Running Configuration file.

Note: For detailed information, refer to *PoE Properties*, in the *PoE* section in the *Port Management* chapter of the *Cisco Business 350 Series Switches Administration Guide*.

Restoring Factory Default Settings

To restore the managed PoE switch to factory default settings, use the Reset button to reboot or reset the switch and do the following:

- To reboot the switch, press and hold the **Reset** button for less than ten seconds.
- To restore the switch to its factory default settings:
  1. Disconnect the switch from the network or disable all DHCP servers on your network.
  2. With the power on, press and hold the **Reset** button for more than ten seconds.