NETGEAR ENTERPRISE

Audio Video User Manual

AV Line of Fully Managed Switches M4250 Series

Model: M4250

202-12937-01
May 2026

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/enterprise.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/enterprise.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

Where permitted by law, by using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions and if you do not agree, return the device to your place of purchase within your return period.

This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra building connection only.

Trademarks

© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-12937-01	May 2026	We revised the following section: • Overview of preconfigured AV profile templates
202-12148-12	January 2026	We added the following sections: • Access the NETGEAR support pages • Change view to the Main UI We revised the following sections: • Overview of preconfigured AV profile templates
202-12148-11	November 2025	We revised the following sections: • Overview of preconfigured AV profile templates

Publication Part Number	Publish Date	Comments
		• Add a description for one or more interfaces • Configure and assign a custom network profile • Display detailed information about the physical ports and LAGs In addition, we revised all procedures to advise that the default web browser protocol is HTTPS.
202-12148-10	July 2025	We added multiple new templates to the Overview of preconfigured AV profile templates section.
202-12148-09	June 2025	We revised the following sections: • How Insight and the AV UI interact with each other • Overview of preconfigured AV profile templates We updated the AV UI password requirements throughout the document.
202-12148-08	December 2024	We added multiple new templates to Overview of preconfigured AV profile templates. We added Add one or more ports as untagged ports to a network profile. We revised the chapter Port Configuration and also added the following sections to the chapter: • Configure STP and CST settings for one or more interfaces • Configure autonegotiation or speed and duplex mode for one or more interfaces • Configure broadband storm control for one or more interfaces We updated Set the STP network redundancy for the switch to document support for custom STP priority settings.
202-12148-07	September 2024	We added multiple new templates to Overview of preconfigured AV profile templates. We changed Use an AV profile template to configure and assign a network profile because PTP residency time stamping is now configured *per profile* rather than globally for the switch.
		We added the following sections: • Use the Kramer AV profile template to configure and assign a network profile • Use the Shure Split Audio and Control Network AV profile

Publication Part Number	Publish Date	Comments
		template to configure and assign a network profile • Configure and assign a custom network profile • Manually set Trunk mode on one or more ports
		We removed the QoS configuration options from Create a custom AV profile template and Change a custom AV profile template. QoS is now set automatically. We removed information about licenses, which are no longer required for the audio video bridging (AVB) feature.
202-12148-06	October 2022	We added new templates for Shure, and support for Extron NAV and Wyrestorm products to Overview of preconfigured AV profile templates.
202-12148-05	May 2022	We changed Supported Switches.
202-12148-04	December 2021	We added the following chapters: • Multicast • Port Configuration
		We added the following sections in existing chapters: • Log in to the AV UI using the management interface default IP address • Log in to the AV UI over the OOB port • About audio video bridging • About PTP residency time stamping • Configure the IGMP querier for a network profile • Display the total PoE consumption for the switch and the PoE information for the ports • Management interface IP address, including Set a fixed IP address or change the management VLAN for the management interface and Enable the DHCP client for the management interface • OOB port IP address, including Set a fixed IP address for the OOB port and Enable the DHCP client for the OOB port • Display or clear the port statistics • Access the CLI through the terminal in the AV UI
		We changed the following sections: Overview of preconfigured AV profile templates Set the STP network redundancy for the switch

Publication Part Number	Publish Date	Comments
		We made other minor changes throughout the manual.
202-12148-03	March 2021	We added the following chapters: • Security • Diagnostics and Troubleshooting
		We added the following sections to existing chapters: • Auto-Trunk overview • Enable or disable Auto-Trunks • Auto-LAG overview • Enable or disable Auto-LAGs • Configure the hash mode for Auto-LAGs • Save the running configuration • Download the running configuration • Restore the configuration. • Set the STP network redundancy for the switch • Display the status of the ports and switch • Display the neighboring devices
		We changed the following sections: • Supported Switches • Use an AV profile template to configure and assign a network profile • Create a custom AV profile template • Manage PoE port settings • Save the running configuration
202-12148-02	November 2020	We added the following chapters: • Link Aggregation • Power over Ethernet
		We added a DHCP server option to Use an AV profile template to configure and assign a network profile.
202-12148-01	September 2020	First publication.

Contents

Copyright © 2026 NETGEAR

Copyright © 2026 NETGEAR

Copyright © 2026 NETGEAR

Getting Started with the AV UI

This user manual is for the AV Line of Fully Managed Switches M4250 Series and covers all M4250 switch models.

This chapter provides an overview of how you can use your switch and access the audio-video (AV) user interface (UI), in short AV UI.

The chapter contains the following sections:

NOTE: For more information about the topics that are covered in this manual, visit the support website at netgear.com/support/.

NOTE: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. You can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Supported Switches

This AV user manual is for the NETGEAR AV Line of Fully Managed Switches M4250 Series models. For a list of M4250 switch models, visit kb.netgear.com/000064904.

Available publications

You can download the following publications for the AV Line of Fully Managed Switches M4250 Series by visiting netgear.com/support/download.

- Installation guide
- Hardware installation guide
- Main user manual
- Audio-video user manual (this manual)
- Software administration manual
- CLI command reference manual

- Frequently Asked Questions
- Data sheet

AV UI overview

Your switch contains an embedded web server and management software for managing and monitoring the switch. The switch functions as a simple switch without the management software. However, you can use the management software to configure many advanced features that can improve audio-video (AV) flows, switch efficiency, and overall network performance.

The switch software includes a set of comprehensive management features for configuring and monitoring the switch through one of the following methods:

- Audio-video user interface (AV UI), either over an Ethernet network port or over the out-of-band (OOB) port (also referred to as the service port).
- Main user interface (main UI), either over an Ethernet network port or over the OOB port.
- Simple Network Management Protocol (SNMP)
- Command-line interface (CLI)

Each of the standards-based management methods allows you to configure and monitor the components of the switch. The method you use to manage the system depends on your network size and requirements, and on your preference.

This manual describes how to use the AV UI to manage and monitor the switch. The AV UI is a web-based management tool that lets you configure and manage audio-video and other types of network profiles remotely using a standard web browser.

NOTE: To configure *all* available switch features, including VLANs, QoS, and ACLs, use the main UI.

Use a web browser to log in to the AV UI

If this is the first time that you log in to the switch and you must use the default IP address of the switch, see the information in the installation guide. You can use a web browser to access the switch and log in. You must be able to ping the IP address of the management interface or out-of-band (OOB) port from your computer for web access to be available.

NOTE: The first time that you log in as an admin user to either the AV UI or the main UI, no password is required (that is, the password is blank). After you log in for the first time, you are required to specify a local device password that you must use each subsequent time that you log in to either the AV UI or the main UI. (Using the main UI, you can change the password again.)

Log in to the AV UI using the management interface default IP address

Any Ethernet interface can function as the management interface.

To use the default IP address of the management interface to access the switch over the AV UI:

1. Prepare your computer with a static IP address in the 169.254.0.0 subnet with subnet mask 255.255.0.0.
   For example, use 169.254.100.201 for your computer.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet network port on the switch.
3. Launch a web browser.
4. Enter **https://169.254.100.100** in the web browser address field:
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
5. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

Log in to the AV UI over the OOB port

You can configure network information on the IPv4 service port, also referred to as the out-of-band (OOB) port. The OOB port is a dedicated Ethernet port for out-of-band management of the switch. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

By default, no IP address is set for the OOB port, but its DHCP client is enabled so that the port can receive an IP address from a DHCP server in your network.

If the OOB port does not receive an IP address from a DHCP server in your network, the IP address for the port is set to 192.168.0.239 with 255.255.255.0 as the subnet mask. The same occurs if you connect the OOB port directly to a computer and reboot the switch.

For information about setting a fixed IP address for the OOB port, see Set a fixed IP address for the OOB port on page 100.

To use IP address 192.168.0.239 of the OOB port to access the switch over the AV UI:

1. Prepare your computer with a static IP address in the 192.168.0.0 subnet with subnet mask 255.255.255.0.
   For example, use 192.168.0.201 and 255.255.255.0 for your computer.
2. Connect an Ethernet cable from an Ethernet port on your computer to the OOB port on the switch.
3. Reboot the switch so that the OOB port is set to its default IP address.
4. Launch a web browser.
5. Enter **https://192.168.0.239** in the web browser address field:
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
6. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

Log in to the AV UI with a known IP address

If you did not assign a static IP address to the switch but let a DHCP server in your network assign an IP address to switch, determine the IP address by accessing the DHCP server or by using an IP scanner utility.

The procedures in this manual assume that you know the IP address of your switch.

To use a known IP address to access the switch over the AV UI:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

How Insight and the AV UI interact with each other

If you manage the switch using the NETGEAR Insight Cloud Portal or Insight app, you can *also* still use the AV UI to manage the switch. That is, these management methods are not mutually exclusive but complement each other. Changes to Insight are synchronized to the AV UI, and the other way around, changes to the AV UI are synchronized to Insight.

NOTE: Synchronization between the AV UI and Insight might take up to 15 minutes. During the synchronization period, do not make the same changes on both the AV UI and Insight or conflicting changes on the AV UI and Insight.

By default, NETGEAR Insight is enabled but inactive if you do not configure and use it. If Insight is inactive, changes to the main UI are not synchronized to Insight. You cannot use the AV UI to disable Insight. However, if you do not configure and use Insight, it is effectively disabled.

NOTE: NETGEAR Insight and the Engage Controller application are mutually exclusive. To change the management mode of the switch from Insight to the Engage Controller, or the other way around, reset the switch to factory default settings.

Limitations

NETGEAR Insight does not support AV profile templates and associated network profiles, which you can configure in the AV UI. In addition, Insight does not support port priority settings for PoE ports, which is a feature that you can configure in the AV UI.

Save the running configuration to the startup configuration

After you make changes on a page of the AV UI and click the **Apply** button (or, in some windows, the **Save** button), your changes are saved for the current session but are not retained when you restart the switch. That is, your running configuration is not saved to the startup configuration (the startup-config file), which means that it is not yet permanently saved.

For information about saving your current changes (your running configuration) to the startup configuration, see Save the running configuration on page 92.

Register your switch

To qualify for product updates and product warranty, we encourage you to register your product.

Registration confirms that your email alerts work, lowers technical support resolution time, and ensures your shipping address accuracy. We would also like to incorporate your feedback into future product development. We never sell or rent your email address and you can opt out of communications.

To register your switch with NETGEAR:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. At the top of page, from the **Question/Help** menu, select **Register**.
   The NETGEAR Account Login page displays. If the page does not display, visit the following website:

   my.netgear.com/registration/login.aspx

5. Enter your NETGEAR account email address and password and click the **NETGEAR Sign In** button.
   If you did not yet create a NETGEAR account, click the **Create an account** link, follow the directions onscreen to create an account, and then register the switch with your NETGEAR email address and password.

Access the NETGEAR support pages

You can navigate to the NETGEAR support and community pages from the AV UI.

To access the support or community page:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Do one of the following:
   - **Access the support page**: At the top of page, from the **Question/Help** menu, select **Support**.

     The NETGEAR Support page displays.
   - **Access the community page**: At the top of page, from the **Question/Help** menu, select **Community**.

     The NETGEAR Community page displays.

Change view to the Main UI

You can navigate to the Main UI from the AV UI.

To change your view from the AV UI to the Main UI:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. At the top of page, from the **Question/Help** menu, select **Main UI**.
   The NETGEAR Account Login page displays.

Audio-Video Profile Templates and Network Profiles

The switch provides preconfigured audio-video (AV) profile templates that you can configure and assign to switch ports and VLANs, thereby creating network profiles.

You can also set up your own AV profile templates.

These are the essential differences between an AV profile template and a network profile:

- **AV profile template**: A preconfigured or custom template with QoS, multicast, or PTP settings, or a combination of these settings, that you can apply to multiple network profiles.
- **Network profile**: An AV profile template that you configured and assigned to one or more switch ports, to a VLAN, and as an option, to a specific IP address.

The chapter contains the following sections:

Overview of preconfigured AV profile templates

An AV profile template integrates NETGEAR proprietary settings, allowing you to optimize specific audio and video environments. You can use an AV profile template to create one or multiple network profiles. For example, you might use the same AV profile template to set up three network profiles for different areas at the same physical location: one network profile for the lobby, one for the theater, and one for the patio.

The switch provides the following preconfigured AV profile templates:

- **Allen & Heath gigaACE/GX**: Use this template to connect two audio devices from Allen & Heath in a Layer 2 VLAN only, across one or multiple switches. The supported protocols include gigaACE and GX.
- **AJA AV Network**: Use this template to connect AJA Dante AV systems for quick auto-detection and for ease of configuration..
- **Audio AES67**: Use this template to connect the switch to connect IP Audio AES67 InterComm devices and their controller. By default, this profile enables PTP TC.

- **AUDAC Audio and Control Network**: Use this template to connect AUDAC devices and AUDAC devices requiring separation of audio and control traffic into different VLANs. This profile is compatible with Dante and AES67. By default, this profile enables PTP TC.
- **Audio Audio-Technica**: Use this template to connect Audio-Technica Commercial Audio microphones, speakers, digital mixers, and wireless systems.
- **Audio Basalte Multiroom**: Use this template to connect IP Basalte Plano, Aalto, and Ceilo Speaker systems and controllers.
- **Audio Genelec Smart IP**: Use this template to connect Genelec Smart IP active PoE+ loudspeakers and various control systems.
- **Audio Dante**: Use this template to connect the switch to Dante audio devices and their controller. This template can support products such as Audinate, AED, Biamp, Bose, Genelec, Harman, RTS, Sennheiser, Shure, Trinnov Audio, and Waves. By default, this profile enables PTP TC.
- **Audio Q-SYS**: Use this template to connect the switch to IP Audio Q-SYS devices and their controller.
- **Audio Soundgrid**: Use this template to connect the switch to IP Audio SoundGrid devices and their controllers.
- **Audio Video AVB**: Use this template to connect the switch to IP audio devices that support Audio Video Bridging (AVB). This profile does not support PTP TC.
- **Audio Video AVB MILAN**: Use this template to connect the switch to IP Audio Video AVB MILAN devices and their controller.
- **Audio Video AVB MILAN with Dante PTPv1 PTPv2 or AES67**: Use this template to connect IP Audio Video AVB and Dante or AES67 devices and their respective controllers in the same VLAN. MTU is 1500 by default and PTP-TC is not configurable on that VLAN.
- **Avid S6L**: Use this template to connect the switch to Avid VENUE | S6L Live Sound Ethernet AVB ports “A” or “B” devices. This profile is supported on all M4250 Series and M4250 Series switches that support AVB and is supported on VLAN 1 (the default VLAN profile) only. Only one VLAN can exist on the switch when you use this profile. No other VLAN IDs are accepted.

  By default, this profile enables Redundancy Mode A. This means the switch with mode A is the grandmaster clock and the switch with mode B is the grandmaster clock backup.
- **AVoIP Lightware AV Network**: Use this template to connect Lightware AVoIP endpoints and their control devices from the UBEX product family.
- **BirdDog AV Network**: Use this template to connect BirdDog AV systems for quick auto-detection and for ease of configuration. By default, this profile enables PTP TC.
- **BluOS AV**: Use this template to connect BluOS AV systems for quick auto-detection and for ease of configuration.
- **Blustream Multicast**: Use this template to connect Blustream Multicast Video over IP products, including those that feature Dante / AES67.
- **Crestron DigitalMedia AV Network**: Use this template to connect the switch to Crestron DM

NVX (video), Crestron DM NAX (audio), Creston cameras (NDI), computers, computers, and other Crestron Control network devices.

- **Data**: Use this template to connect the switch to computers and other control network devices. CobraNet is supported in a VLAN other than VLAN 1. This profile does not support PTP TC.
- **Default**: Use this template as the default VLAN 1 profile. You can overwrite this profile with another profile on VLAN 1 after initial switch configuration. The default profile automatically applies after a factory reset. This profile does not support PTP TC.
- **DICENTIS Conference system profile**: Use this template to connect the switch to DICENTIS Conference system equipment with RPVSTP and IGMP support. By default, this profile enables PTP TC.
- **ETC Lighting**: Use this template to connect the switch to ETC Lighting and control devices. This profile does not support PTP TC.
- **G&D KVM-over-IP**: Use this template to connect the switch to Guntermann & Drunck KVM-over-IP Solutions devices. By default, this profile does not support PTP TC. However, you can manually enable PTP settings.
- **HARMAN Professional AV Network**: Use this template on the switch to connect HARMAN Professional product lines together. This profile does not support PTP TC.
- **Kramer AV**: Use this template to connect Kramer AV over IP solutions for audio and video distribution over up to four different VLANs (video, control, audio, and aux).
- **Lighting**: Use this template to connect the switch to streaming ACN (sACN), Art-Net, and MA-NET3 lighting devices for controlling lighting equipments. This profile does not support PTP TC.
- **Nice Home Management**: Use this template to connect the switch to Nice Home Management systems, including IPD Dante with either unicast or multicast configurations. Auto-Provision automatically detects Nice devices on a factory-default switch by matching their MAC OUI (F8:57:2E) and creates a Nice network profile on VLAN 1 across all switch ports. When the switch is in factory default mode, Auto-Provision is enabled by default.

  By default, this profile enables PTP TC.
- **NUCLEUS Converged AV Network**: Use this template to connect the switch to EvertzAV NUCLEUS Session Manager and UXP gateways on a single converged network. This profile does not support PTP TC.
- **Pharos Lighting Control**: Use this template to connect the switch to Pharos Control devices. This profile does not support PTP TC.
- **Pharos Lighting Data**: Use this template to connect the switch to Pharos Lighting devices. This profile does not support PTP TC.
- **Poly StudioNet Modular Room**: Use this template to connect the switch to HP Poly StudioNet Modular Room peripherals. You can create multiple instances of this profile on a switch and it can coexist with other profiles on a switch. You can configure this profile on all switch models.

By default, this profile enables PTP TC.

- **Shure Converged Audio and Control Network**: Use this template to connect the switch to Shure devices requiring audio and control traffic on a single VLAN. Compatible with Dante, AES67, QSYS, and Biamp Dante devices. By default, this profile enables PTP TC.
- **Shure Split Audio and Control Network**: Use this template to connect the switch to Shure devices requiring separation of audio and control traffic into different VLANs. Compatible with Dante, AES67, QSYS, and Biamp Dante devices.
- **Sennheiser TeamConnect Bar S - Single Domain Mode**: Use this template to connect the switch to a Sennheiser TeamConnect Bar S device in single domain mode. By default, this profile enables PTP TC.
- **Sonos**: Use this template to connect the switch to a Sonos smart home sound system. This profile does not support PTP TC.
- **Telos Alliance / Livewire+ AES67**: Use this template to connect Telos Alliance Livewire+ products and other products that are AES67 compliant. By default, this profile enables PTP TC.
- **Unite Audio**: Use this template to connect to Glidenet audio streaming products for PCM, multichannel, ultra high definition, and compressed bit-perfect audio over networks.
- **Video**: Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

  This profile does not support PTP TC.
- **URC Automation**: Use this template to connect the switch to URC Automation HDA devices and their controllers. This profile is supported on all M4250 Series and M4350 Series switches that support AVB.
- **Video**: Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

  This profile does not support PTP TC.
- **Video NDI4**: Use this template to connect the switch to video devices and cameras that support Network Device Interface (NDI) version 4 with multi-TCP (mTCP) transport. This template can support products from companies such as AVer, Avonic, BirdDog, Bolin, Canon, JVC, Kiloview, Lumens, Magewell, Ross, Panasonic, PTZOptics, Sony, and Vizrt, as well as products from other companies.

  This profile does not support PTP TC.
- **Video NDI5 / NDI6 with Dante, Q-Sys or AES67 audio**: Use this template to connect the

switch to video devices and cameras that support NDI version 5 or version 6 with Reliable User Datagram Protocol (RUDP). Audio Dante, Q-SYS, or AES67 is supported at the same time in the same VLAN. This template can support products from companies such as AVer, Avonic, BirdDog, Bolin, Canon, JVC, Kiloview, Lumens, Magewell, Ross, Panasonic, PTZOptics, Sony, and Vizrt, as well as products from other companies.

- **Video with AES67 audio**: Use this template to connect the switch to IP video devices and their controllers when AES67 audio is supported in the same VLAN. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

  By default, this profile enables PTP TC.
- **Video with Dante audio**: Use this template to connect the switch to IP video devices and their controllers when Dante audio is supported in the same VLAN. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.
- **Video with Q-SYS audio**: Use this template to connect the switch to IP video devices and their controllers when Q-SYS audio is supported in the same VLAN. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

  The MTU for the packet is 1,500 bytes. For Jumbo Frames, use another profile template such as Video with AES67 audio or Dante.
- **Visionary AV Network**: Use this template to connect the switch to Visionary AV systems for quick auto-detection and for ease of configuration. This profile does not support PTP TC.
- **Visionary Advanced Multi-Domain**: Use this template to configure video, audio, and expansion together. This profile does not support PTP TC.

About audio video bridging

802.1AS timing and synchronization is an audio video bridging (AVB) feature.

The IEEE 802.1AS standard specifies the protocol and procedures used to ensure that the QoS requirements are guaranteed for time-sensitive applications, such as audio and video.

The IEEE 1588 Precision Time Protocol (PTP) forms the basis of the IEEE 802.1AS standard. PTP specifies a precise clock synchronization protocol that relies on time-stamped packets.

As of firmware version 13.0.4.17, a license is no longer required for the AVB feature.

About PTP residency time stamping

Precision Time Protocol (PTP, IEEE 1588) is a protocol that enables precise synchronization of clocks with a sub-microsecond accuracy across a packet-based network. PTP version 2 (PTPv2) lets network devices of different precision and resolution synchronize to a grandmaster clock through an exchange of packets across the network.

The switch supports a PTP end-to-end transparent clock that is used in the *PTP residency time stamping* feature. Most network profiles support PTP residency time stamping. Whether the feature is available, enabled by default, or disabled by default, depends on the network profile. For more information, see Overview of preconfigured AV profile templates on page 10.

You can enable or disable PTP residency time stamping per network profile (see Use an AV profile template to configure and assign a network profile on page 17).

NOTE: Another feature that the switch supports, 802.1AS (audio video bridging, or AVB), is incompatible with PTP residency time stamping. For more information, see About audio video bridging on page 14 and the information below.

Network profiles

You can use either a preconfigured AV profile template (for example, Audio Dante) or a custom AV profile template that you created to set up one or multiple network profiles.

Change the Default VLAN profile

The default network profile is the Default VLAN profile, which uses the Data AV profile template and VLAN 1. All ports are untagged members of VLAN 1. You can change the AV profile template and the member ports. For each port, you can either remove the port from VLAN 1 or change the port to a tagged port.

To change the Default VLAN profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the Default VLAN, click the **3 dots** icon and select **Edit**.
   The Edit Profile Default window displays.
6. Select the ports to which the profile must apply.
   By default, all ports are selected as untagged ports for the profile. That is, each port is marked with a green icon.

   To configure ports, do the following:
   - **Change a port to a tagged port**: Click the port once. The port is marked with a T icon (for tagged).
   - **Remove a port from the profile**: Click the port twice to remove it from the profile. The port is not marked with a green icon or T icon.
7. To change the AV profile template, from the **Profile Template** menu, select another template.
   The default AV profile template is the Data template.
8. To change the color for the Default VLAN for visual representation, click the box in the **Color** field, and select a color.
   The profile color displays in the AV UI to identify the profile assigned to the Default VLAN.
9. Click the **Apply** button.
   Your settings are saved. The window closes. The Network Profiles page displays again.
10. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Use an AV profile template to configure and assign a network profile

When you configure a network profile, you must enable or disable PTP residency time stamping (depending on whether the profile supports this feature), give the profile a name and assign it to a VLAN, and add a unique color for visual representation. As an option, you can assign a specific VLAN IP address to the profile and use the profile as a DHCP server.

To use an AV profile template to configure and assign a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Profile Templates table, to the right of the AV profile template that you want to use, do one of the following:
   - **Preconfigured AV profile template**: Click the **gear** icon.
   - **Custom AV profile template**: Click the **3 dots** icon and select **Configure**.

   The Profile Configure window displays.
6. Select the ports to add them to or exclude them from the VLAN to which the network profile must apply:
   - **Untagged port**: Click the port once. The port is added as an untagged port and is marked with a green icon. To untag all ports, click the **Untag all** button.
   - **Tagged port**: Click the port twice. The port is added as a tagged port and is marked with a T icon (for tagged). To tag all ports, click the **Tag all** button.
   - **Excluded port**: Do not click the port. The port is excluded and is not marked with a green icon or T icon. To exclude all ports, click the **Remove all** button.

7. Depending on the AV profile template that you select in the previous step, below the graphical display of the switch, you can enable or disable PTP residency time stamping (TC) for the profile (for more information, see About PTP residency time stamping on page 15):
   - **Enable PTP residency time stamping**: Turn on the toggle so that it displays green and is positioned to the right.
   - **Disable PTP residency time stamping**: Turn off the toggle so that it displays gray and is positioned to the left.
8. In the **Profile Name** field, enter a name for the profile.

   NOTE: You cannot change the selection from the **Profile Template** menu.
9. In the **VLAN ID** field, type the VLAN ID to which traffic of the profile must be assigned.
10. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
    The profile color displays in the AV UI to identify the profile assigned to the VLAN.

11. To assign a specific IP address to the network profile, and as an option, use the network profile as a DHCP server, do the following:
    a. Turn on the **Edit VLAN Routing / DHCP Server** toggle so that it displays green and is positioned to the right. The IP address menu and fields become available.
    b. From the **VLAN IP Settings** menu, select **Static** or **DHCP client**.

       By default, None is selected. If you select **Static**, you must specify the IP address settings manually and you can also configure the network profile as a DHCP server. (See the following step.)

       If you select **DHCP client**, the network profile functions as a DHCP client and a DHCP server in your network assigns an IP address to the network profile.
    c. If you select **Static** from the **VLAN IP Settings** menu, specify the IP address and subnet mask in the **VLAN IP Address** and **Subnet Mask** fields.
    d. To set up the network profile as a DHCP server, from the **DHCP Server** menu, select **DHCP Server**, and specify the following settings:
       - **Default Router**: The IP address of the router for the DHCP pool. By default, this IP address is the same address as the VLAN IP address, but you can change it.
       - **DHCP Server Pool Start**. The start IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DHCP Server Pool End**. The end IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DNS Server 1**: The IP address of the primary DNS server.
       - **DNS Server 2**: As an option, the IP address of the secondary DNS server.
       - **Search Domain**: The domain name for the DHCP server. This name is a fully qualified domain name (FQDN).
       - **Lease Time**: The lease time of the IP addresses that the DHCP server assigns. The default is 240 minutes.

12. Click the **Apply** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.

13. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Use the Kramer AV profile template to configure and assign a network profile

When you configure a network profile based on the the Kramer AV profile template, you must enable or disable PTP residency time stamping, and give the profile a name and assign it to a VLAN. As an option, you can assign a specific VLAN IP address to the profile and use the profile as a DHCP server.

You can set up a *single* network profile that is based on the Kramer AV profile template.

For this profile, you can set four different VLANs to separate streaming, control, audio, and auxiliary traffic.

To use the Kramer AV profile template to configure and assign a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Profile Templates table, to the right of the Kramer AV profile template, click the **gear** icon.
   The Profile Configure window displays.

6. Select the ports to add them to or exclude them from the VLAN to which the network profile must apply:
   - **Untagged port**: Click the port once. The port is added as an untagged port and is marked with a green icon. To untag all ports, click the **Untag all** button.
   - **Tagged port**: Click the port twice. The port is added as a tagged port and is marked with a T icon (for tagged). To tag all ports, click the **Tag all** button.
   - **Excluded port**: Do not click the port. The port is excluded and is not marked with a green icon or T icon. To exclude all ports, click the **Remove all** button.
7. Below the graphical display of the switch, enable or disable PTP residency time stamping (TC) for the profile:
   - **Enable PTP residency time stamping**: Turn on the toggle so that it displays green and is positioned to the right.
   - **Disable PTP residency time stamping**: Turn off the toggle so that it displays gray and is positioned to the left. This is the default selection for this profile.
8. In the **Profile Name** field, enter a name for the profile.

   NOTE: You cannot change the selection from the **Profile Template** menu.
9. From the **VLAN ID** menu, select the VLAN ID to which the traffic of the profile must be assigned.

   NOTE: For this profile, you cannot add a unique color.

10. For each of the following VLAN settings, which are specific to the Kramer AV network profile, set the VLAN ID, switch tag (tagged or untagged traffic), and the profile template:
    - **Stream VLAN**: A dedicated VLAN for video stream traffic. The default setting from the Profile Template menu is Video.

      Do the following:

      a. In the **Stream VLAN ID**, set a unique VLAN ID.
      b. From the **Tag Stream** menu, select **Untagged** (the default) or **Tagged**, which applies to streaming traffic only.
    - **Control VLAN**: A dedicated VLAN for data and control traffic. Do the following:
      a. From the **Profile Template** menu, select **Data** or **Disabled**. By default, this profile template is disabled.
      b. If you enable the profile template, in the **Control VLAN ID**, set a unique VLAN ID.
      c. If you enable the profile template, from the **Tag Stream** menu, select **Untagged** or **Tagged** (the default), which applies to data or control traffic only.
    - **Audio VLAN**: A dedicated VLAN for audio traffic. Do the following:
      a. From the **Profile Template** menu, select **Audio Dante**, **Audio AES67**, or **Disabled**. By default, this profile template is disabled.
      b. If you enable the profile template, in the **Audio VLAN ID**, set a unique VLAN ID.
      c. If you enable the profile template, from the **Tag Audio** menu, select **Untagged** or **Tagged** (the default), which applies to audio traffic only.
    - **Aux VLAN**: A dedicated VLAN for auxiliary data traffic. Do the following:
      a. From the **Profile Template** menu, select **Data** or **Disabled**. By default, this profile template is disabled.
      b. If you enable the profile template, in the **Aux VLAN ID**, set a unique VLAN ID.
      c. If you enable the profile template, from the **Tag Stream** menu, select **Untagged** or **Tagged** (the default), which applies to auxiliary data traffic only.

11. To assign a specific IP address to the network profile, and as an option, use the network profile as a DHCP server, do the following:
    a. Turn on the **Edit VLAN Routing / DHCP Server** toggle so that it displays green and is positioned to the right. The IP address menu and fields become available.
    b. From the **VLAN IP Settings** menu, select **Static** or **DHCP client**.

       By default, None is selected. If you select **Static**, you must specify the IP address settings manually and you can also configure the network profile as a DHCP server. (See the following step.)

       If you select **DHCP client**, the network profile functions as a DHCP client and a DHCP server in your network assigns an IP address to the network profile.
    c. If you select **Static** from the **VLAN IP Settings** menu, specify the IP address and subnet mask in the **VLAN IP Address** and **Subnet Mask** fields.
    d. To set up the network profile as a DHCP server, from the **DHCP Server** menu, select **DHCP Server**, and specify the following settings:
       - **Default Router**: The IP address of the router for the DHCP pool. By default, this IP address is the same address as the VLAN IP address, but you can change it.
       - **DHCP Server Pool Start**. The start IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DHCP Server Pool End**. The end IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DNS Server 1**: The IP address of the primary DNS server.
       - **DNS Server 2**: As an option, the IP address of the secondary DNS server.
       - **Search Domain**: The domain name for the DHCP server. This name is a fully qualified domain name (FQDN).
       - **Lease Time**: The lease time of the IP addresses that the DHCP server assigns. The default is 240 minutes.

12. Click the **Apply** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.

13. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Use the Shure Split Audio and Control Network AV profile template to configure and assign a network profile

When you configure a network profile based on the Shure Split Audio and Control Network profile template, you must enable or disable PTP residency time stamping, give the profile a name, and set two different VLANs to separate control and audio traffic. You can specify which port is connected to a Shure device as well as which port is a member of the control VLAN or the audio VLAN. As an option, for each VLAN, you can assign a specific VLAN IP address to the profile and use the profile as a DHCP server.

You can set up a *single* network profile that is based on the Shure Split Audio and Control Network profile template.

To use the Shure Split Audio and Control Network template to configure and assign a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. From the **Profile Templates** menu, select **Shure Split Audio and Control Network**.
   The Profile Configure window displays.

5. Select one or more individual ports and make a selection from the port pop-up menu, make a selection from the **All ports** menu to configure all ports simultaneously, or combine these two configuration methods to configure the following settings:
   - **Shure Device**: The port or ports are configured for connection to a Shure device.
   - **Control**: The port or ports are members of the Control VLAN.
   - **Audio**: The port or ports are members of the Audio VLAN.
   - **Tag Control**: The port or ports are tagged members of the Control VLAN.
   - **Tag Audio**: The port or ports are tagged members of the Audio VLAN.
   - **Tag Both**: The port or ports are tagged members of the both the Control VLAN and the Audio VLAN.
   - **Remove**: The port or ports are excluded from the profile configuration.

   NOTE: You cannot change the selection from the **Profile Template** menu.

6. Below the graphical display of the switch, enable or disable PTP residency time stamping (TC) for the profile:
   - **Enable PTP residency time stamping**: Turn on the toggle so that it displays green and is positioned to the right.
   - **Disable PTP residency time stamping**: Turn off the toggle so that it displays gray and is positioned to the left. This is the default selection for this profile.

   NOTE: You cannot add a new name in the **Profile Name** or change the selection from the **Profile Template** menu.

7. From the **Control VLAN ID** menu, select the VLAN ID to which the control traffic of the profile must be assigned.

8. From the **Audio VLAN ID** menu, select the VLAN ID to which the audio control traffic of the of the profile must be assigned.

   NOTE: For this profile, you cannot add a unique color.

9. To assign a specific IP address to the Control L3 VLAN or Audio L3 VLAN for this network profile, and as an option, use the network profile as a DHCP server, do the following:
   a. Select the **Control L3 VLAN** or **Audio L3 VLAN** tab to specify the VLAN for which the configuration must apply.

      You can configure both VLAN settings, but one after the other.
   b. Turn on the **Edit VLAN Routing / DHCP Server** toggle so that it displays green and is positioned to the right. The IP address menu and fields become available.
   c. From the **VLAN IP Settings** menu, select **Static** or **DHCP client**.

      By default, None is selected. If you select **Static**, you must specify the IP address settings manually and you can also configure the network profile as a DHCP server. (See the following step.)

      If you select **DHCP client**, the network profile functions as a DHCP client and a DHCP server in your network assigns an IP address to the network profile.
   d. If you select **Static** from the **VLAN IP Settings** menu, specify the IP address and subnet mask in the **VLAN IP Address** and **Subnet Mask** fields.
   e. To set up the network profile as a DHCP server, from the **DHCP Server** menu, select **DHCP Server**, and specify the following settings:
      - **Default Router**: The IP address of the router for the DHCP pool. By default, this IP address is the same address as the VLAN IP address, but you can change it.
      - **DHCP Server Pool Start**. The start IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
      - **DHCP Server Pool End**. The end IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
      - **DNS Server 1**: The IP address of the primary DNS server.
      - **DNS Server 2**: As an option, the IP address of the secondary DNS server.
      - **Search Domain**: The domain name for the DHCP server. This name is a fully qualified domain name (FQDN).
      - **Lease Time**: The lease time of the IP addresses that the DHCP server assigns. The default is 240 minutes.

10. Click the **Apply** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.

11. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a network profile

You can change an existing network profile.

To change a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the network profile that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit Profile window displays.
6. Change the settings as needed.
   For more information about the settings, Use an AV profile template to configure and assign a network profile on page 17.
   You cannot change the VLAN ID and AV profile template selection.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Network Profiles page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a network profile

You can remove an existing network profile that you no longer need.

To remove a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   > **NOTE:** The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the network profile that you want to remove, click the **3 dots** icon and select **Delete**.
   A confirmation window displays.
6. Click the **Delete** button.
   The network profile is removed. The window closes. The Network Profiles page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Custom AV profile templates

You can create your own AV profile template. After you do so, you can use the custom AV profile template to set up one or multiple network profiles (see Use an AV profile template to configure and assign a network profile on page 17).

The advantage of a custom AV profile template is that you can decide whether to enable multicast, PTP, or both.

Create a custom AV profile template

Before you create a custom AV profile template, consider the following:

- Does the template require multicast to be enabled?
- Does the template require Precision Time Protocol (PTP) to be enabled?

NOTE: You can enable PTP and multicast for a custom AV profile template but you cannot configure the PTP and multicast settings in the AV UI. To configure PTP and multicast settings, use the main UI or the CLI. For more information, see the main user manual or the CLI command reference manual, both of which you can download by visiting netgear.com/support/download.

To create a custom AV profile template:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. At the top right of the Profile Templates table, click the **Create AV Template** link.
   The Create AV Profiles window displays.
6. In the **Profile Type** field, enter a name for the type of service that the template can provide.
7. In the **Profile Description** field, enter a description for the template.
8. To enable multicast, turn on the **Multicast** toggle so that it displays green and is positioned to the right.
   By default, multicast is disabled and the toggle displays gray and is positioned to the left.

9. To enable PTP, turn the **PTP** toggle so that it displays green and is positioned to the right.
   By default, PTP is disabled and the toggle displays gray and is positioned to the left.
10. Click the **Save** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.
11. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure and assign a custom network profile

When you configure a network profile, you must enable or disable PTP residency time stamping (depending on whether the profile supports this feature), give the profile a name and assign it to a VLAN, and add a unique color for visual representation. As an option, you can assign a specific VLAN IP address to the profile and use the profile as a DHCP server.

NOTE: When you configure a network profile from the AV UI, the VLAN ID, profile name, and profile template automatically display in the CLI as interface descriptions.

To use a custom AV profile template to configure and assign a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. In the Profile Templates table, to the right of the custom AV profile template that you want to use, click the **3 dots** icon and select **Configure**.
   The Profile Configure window displays.

5. Select the ports to add them to or exclude them from the VLAN to which the network profile must apply:
   - **Untagged port**: Click the port once. The port is added as an untagged port and is marked with a green icon. To untag all ports, click the **Untag all** button.
   - **Tagged port**: Click the port twice. The port is added as a tagged port and is marked with a T icon (for tagged). To tag all ports, click the **Tag all** button.
   - **Excluded port**: Do not click the port. The port is excluded and is not marked with a green icon or T icon. To exclude all ports, click the **Remove all** button.
6. Below the graphical display of the switch, you can enable or disable PTP residency time stamping (TC) for the profile (for more information, see About PTP residency time stamping on page 15):
   - **Enable PTP residency time stamping**: Turn on the toggle so that it displays green and is positioned to the right.
   - **Disable PTP residency time stamping**: Turn off the toggle so that it displays gray and is positioned to the left.
7. In the **Profile Name** field, enter a name for the profile.

   NOTE: You cannot change the selection from the **Profile Template** menu.
8. In the **VLAN ID** field, type the VLAN ID to which traffic of the profile must be assigned.
9. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
   The profile color displays in the AV UI to identify the profile assigned to the VLAN.

10. To assign a specific IP address to the network profile, and as an option, use the network profile as a DHCP server, do the following:
    a. Turn on the **Edit VLAN Routing / DHCP Server** toggle so that it displays green and is positioned to the right. The IP address menu and fields become available.
    b. From the **VLAN IP Settings** menu, select **Static** or **DHCP client**.

       By default, None is selected. If you select **Static**, you must specify the IP address settings manually and you can also configure the network profile as a DHCP server. (See the following step.)

       If you select **DHCP client**, the network profile functions as a DHCP client and a DHCP server in your network assigns an IP address to the network profile.
    c. If you select **Static** from the **VLAN IP Settings** menu, specify the IP address and subnet mask in the **VLAN IP Address** and **Subnet Mask** fields.
    d. To set up the network profile as a DHCP server, from the **DHCP Server** menu, select **DHCP Server**, and specify the following settings:
       - **Default Router**: The IP address of the router for the DHCP pool. By default, this IP address is the same address as the VLAN IP address, but you can change it.
       - **DHCP Server Pool Start**. The start IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DHCP Server Pool End**. The end IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DNS Server 1**: The IP address of the primary DNS server.
       - **DNS Server 2**: As an option, the IP address of the secondary DNS server.
       - **Search Domain**: The domain name for the DHCP server. This name is a fully qualified domain name (FQDN).
       - **Lease Time**: The lease time of the IP addresses that the DHCP server assigns. The default is 240 minutes.
11. Click the **Apply** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.
12. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a custom AV profile template

You can change an existing custom AV profile template. You cannot change a preconfigured AV profile template.

To change a custom AV profile template:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.

5. In the Profile Templates table, to the right of the custom AV profile template that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit AV Profiles window displays.

6. Change the settings as needed.
   For more information about the settings, Create a custom AV profile template on page 29.
   You cannot change the name of the AV profile template.

7. Click the **Save** button.
   Your settings are saved. The window closes. The Network Profiles page displays again.

8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a custom AV profile template

You can remove an existing custom AV profile template that you no longer need. You cannot remove a preconfigured AV profile template.

To remove a custom AV profile template:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. In the Profile Templates table, to the right of the custom AV profile template that you want to remove, click the **3 dots** icon and select **Delete**.
   A confirmation window displays.

5. Click the **Delete** button.
   The AV profile template is removed. The window closes. The Network Profiles page displays again.

6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Add one or more ports as untagged ports to a network profile

You can add one or more ports are untagged ports to a network profile. For information about manually setting ports as trunks, see Manually set Trunk mode on one or more ports on page 37.

To add one or more ports as untagged ports to a network profile:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. Alternatively,
6. In the graphical display of the switch, select the ports that you want to add to a network profile.
7. From the **Add-Ports-Untagged-To-Profile** menu, select the network profile.
   Your settings are saved automatically.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Auto-Trunk overview

Auto-trunk is a feature that lets the switch automatically enable Trunk mode on capable physical links and LAG interfaces between partner devices. A trunk can carry all active VLANs. By default, the Auto-Trunk feature is enabled on the switch.

If the switch automatically configures a port as a trunk (that is, an Auto-Trunk), all VLANs on the switch become part of the trunk, allowing automatic configuration of all VLANs on the switch and on the partner device with which the trunk is established.

Before the switch configures an Auto-Trunk, the switch first detects the physical links with the partner device that also supports the Auto-Trunk feature, and then automatically configures the ports that are connected and capable of forming a trunk at both ends.

A trunk carries multiple VLANs and accepts both tagged and untagged packets. Typically, a connection between the switch and a partner device such as a router, access point, or another switch functions as a trunk.

For the switch to form an Auto-Trunk with a partner device, the following are required:

- The Auto-Trunk feature must be supported and globally enabled on the switch and the partner device. (On all M4250 switch models, the Auto-Trunk feature is enabled by default.)

- The interconnected ports on both the switch and the partner device must be enabled. (On all M4250 switch models, all ports are enabled by default.)
- LLDP must be enabled on the interconnected ports on both the switch and the partner device. (On all M4250 switch models, LLDP is enabled by default on all ports.)
- The interconnected ports on the switch and the partner device must be in the default switch port mode, which is the General mode. If the ports are in the Access mode or already in the Trunk mode, an Auto-Trunk cannot be formed on an Auto-LAG.

For an Auto-Trunk, the PVID is automatically set to the default VLAN. If you want to change the PVID for an Auto-Trunk, change the default VLAN.

The Auto-Trunk feature functions together with the Auto-LAG feature (see Auto-LAG overview on page 40). After an Auto-LAG is formed, the switch automatically applies trunk mode (that is, an Auto-Trunk) to the LAG at both ends. In other words, after an Auto-LAG is formed, the mode for the ports that participate in an Auto-LAG is automatically changed from the default switch port mode to the trunk port mode, and the Auto-LAG then becomes an Auto-Trunk.

After a port or an Auto-LAG becomes an Auto-Trunk, all VLANs on the switch become part of the trunk, and all VLANs on the switch and the partner device can be configured automatically.

Enable or disable Auto-Trunks

By default, the Auto-Trunk feature is globally enabled but you can globally disable it.

To enable or disable Auto-Trunks:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. Below the graphical display of the switch, do one of the following:
   - **Disable Auto-Trunks**: Do the following:
     a. Turn off the toggle so that it displays gray and is positioned to the left. A pop-up window displays a warning.
     b. Click the **Yes** button. Your settings are saved.
   - **Enable Auto-Trunks**: Turn on the toggle so that it displays green and is positioned to the right. Your settings are saved automatically.
6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Manually set Trunk mode on one or more ports

You can manually assign the Trunk mode on capable physical links and LAG interfaces between partner devices. A trunk can carry all active VLANs. When you assign Trunk mode to one or more ports, all VLANs are tagged except for the management VLAN (VLAN 1). For information about adding one or more ports are untagged ports to a network profile, see Add one or more ports as untagged ports to a network profile on page 34.

You can set the trunk manually whether or not the Auto-Tunk feature is enabled.

To manually set Trunk mode one or more ports, or to reset one or more ports to the default switch port mode (the General mode):

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the graphical display of the switch, select the ports for which you want to set Trunk mode or General mode.
6. Below the graphical display of the switch, select one of the following settings from the Manual-Trunk menu:
   - **Default**: Sets the selected ports to General mode.
   - **All VLANs tagged except Management VLAN 1**: Sets the selected ports to Trunk mode. The ports in the graphical display show an “M” for manual.

   Your settings are saved automatically.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure the IGMP querier for a network profile

IGMP snooping requires that one central switch or router in a VLAN periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port and network profile basis. If the switch does not receive updated membership information in a timely fashion, it stops forwarding multicasts to the port where the end device is located.

Each network profile can function as a querier in the VLAN in which it operates. The IGMP querier for the Default network profile with VLAN 1 is enabled by default. You can configure an IGMP querier for use with a network profile in another VLAN than VLAN 1.

To configure the IGMP querier for a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.

5. In the Configured Profiles table, to the right of the network profile that you want to change, click the **3 dots** icon and select **Querier**.
   The Edit default querier profile window displays.

6. Configure the settings for the querier:
   - **Election Participate**: Select to enable or disable the querier election participate mode for the network profile:
     - **Enabled**: Turn on the toggle so that it displays green and is positioned to the right. This setting indicates that the querier for the network profile participates in querier election, in which the lowest numbered IP address operates as the querier in the VLAN. Any other querier moves to the non-querier state.
     - **Disabled**: Turn off the toggle so that it displays gray and is positioned to the left. This setting indicates that if the querier for the network profile detects another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.

     Except for the Default network profile, the election participation is disabled by default, and the toggle displays gray and is positioned to the left.
   - **Querier VLAN address**: Specify the IP address to be used as the source IP address in periodic IGMP queries that are sent on the VLAN.

   The Operational State field displays DISABLED or QUERIER, indicating if the network profile is functioning as a querier.

7. Click the **Apply** button.
   Your settings are saved.

8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Link Aggregation

Link aggregation groups (LAGs), which are also known as port-channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing.

You can create a LAG that includes two or more ports as members and apply the LAG to a network profile. A LAG can be static or dynamic, and you can configure the LAG as a trunk. The switch can support multiple LAGs.

The chapter contains the following sections:

For more information about the LAG options of the switch, see the main user manual or CLI reference manual, both of which you can download by visiting netgear.com/support/download.

Auto-LAG overview

An Auto-LAG is a LAG that forms automatically between two devices that support the Auto-LAG feature. An Auto-LAG is a dynamic Layer 2 LAG that is based on the Link Aggregation Control Protocol (LACP).

NOTE: A LAG is also referred to as a port channel or an EtherChannel.

The switch can detect the physical links with a partner device and automatically configure a LAG (that is, an Auto-LAG) on interconnected and capable ports at both ends. The switch can form one Auto-LAG only with each partner device.

The Auto-LAG feature functions together with the Auto-Trunk feature, which must also be supported and enabled on the partner device with which the LAG is formed. After an Auto-LAG is formed, the switch automatically applies trunk mode (that is, an Auto-Trunk) to the LAG at both ends. In other words, after an Auto-LAG is formed, the mode for the ports that participate in an Auto-LAG changes from the default switch port mode to the trunk port mode. For more information about the Auto-Trunk feature, see Auto-Trunk overview on page 35.

For the switch to form an Auto-LAG with a partner switch, the following are required:

- Both the Auto-LAG and Auto-Trunk features must be supported and globally enabled on the switch and the partner device. (By default, the Auto-LAG and Auto-Trunk features are

enabled.)

- At least two links must be established between the switch and the partner device, and these links must support the same speed and duplex mode.
- The links cannot be members of a manually configured static or dynamic LAG.
- LLDP must be enabled on the interconnected ports on the switch and the partner device. (By default, LLDP is enabled on all ports.)
- The interconnected ports on the switch and the partner device must be in the default switch port mode, which is the General mode. If the ports are in the Access mode or already in the Trunk mode, an Auto-Trunk cannot be formed on the Auto-LAG.

An Auto-LAG can form with up to eight interfaces as members. Interfaces are automatically selected for the Auto-LAG based on whether they are up and available and on the following conditions:

- The interface is not already manually configured as a member of a LAG.
- The interface is not manually configured as a trunk port or an access port. That is, the interface must be a general interface.

NOTE: The switch can support multiple static and dynamic LAGs, but with each partner device, the switch can support a single Auto-LAG only.

Enable or disable Auto-LAGs

By default, the Auto-LAG feature is globally enabled but you can globally disable it.

To enable or disable Auto-LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. Below the graphical display of the switch, do one of the following:
   - **Disable Auto-LAGs**: Do the following:
     a. Turn off the toggle so that it displays gray and is positioned to the left A pop-up window displays a warning.
     b. Click the **Yes** button. Your settings are saved.
   - **Enable Auto-LAGs**: Turn on the toggle so that it displays green and is positioned to the right. Your settings are saved automatically. By default, the Auto-LAG feature is enabled.
6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure the hash mode for Auto-LAGs

By default, the Auto-LAG feature is enabled and uses the *Layer 2; Destination* mode, which auto-configures a LAG based on the destination MAC address, VLAN, EtherType, and incoming port in the packet. You can change the hash mode (that is, the load balancing mode) for the Auto-LAG feature.

The switch balances traffic on a LAG by selecting one of the links in the channel over which packets must be transmitted. The switch selects the link by creating a binary pattern from selected fields in a packet and associating that pattern with a particular link. The hash mode determines which fields in a packet the switch selects.

To change the hash mode for the Auto-LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

> **NOTE:** The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. Below the graphical display of the switch, from the **Auto-LAG Hash** menu, select the hash mode for the Auto-LAGs:
   - **Layer 2; Source**: Based on the source MAC address, VLAN, EtherType, and incoming port associated with the packet.
   - **Layer 2; Destination**: Based on the destination MAC address, VLAN, EtherType, and incoming port in the packet. This is the default mode.
   - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses, VLAN, EtherType, and incoming port in the packet.
   - **Layer 3+4; Source**: Based on the source IP address and source TCP or UDP port field in the packet.
   - **Layer 3+4; Destination**: Based on the destination IP address and destination TCP or UDP port field in the packet.
   - **Layer 3+4; Source + Destination**: Based on the source and destination IP addresses and source and destination TCP or UDP port field in the packet.

   Your settings are saved automatically.
6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Create a LAG

Although the maximum number of LAGs that you can create and add is eight, the actual number of LAGs is limited by the number of ports that are available.

When you create a LAG, we recommend that you configure a network profile on the LAG rather than on a physical interface. By default, the network profile for a LAG is the default profile with VLAN 1.

To create a LAG:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.

5. Below the graphical display of the switch, click the **Create LAG** link.
   The Create Link Aggregation Group window displays.

6. Select two or more ports that must become members of the LAG by clicking the individual ports.

7. In the **LAG Name** field, specify a name for the LAG.

8. From the **Hash** menu, select the hash mode for the LAG:
   - **Layer 2; Source**: Based on the source MAC address, VLAN, EtherType, and incoming port associated with the packet.
   - **Layer 2; Destination**: Based on the destination MAC address, VLAN, EtherType, and incoming port in the packet. This is the default mode.
   - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses, VLAN, EtherType, and incoming port in the packet.
   - **Layer 3+4; Source**: Based on the source IP address and source TCP or UDP port field in the packet.
   - **Layer 3+4; Destination**: Based on the destination IP address and destination TCP or UDP port field in the packet.
   - **Layer 3+4; Source + Destination**: Based on the source and destination IP addresses and source and destination TCP or UDP port field in the packet.

   The switch balances traffic on a LAG by selecting one of the links in the channel over which packets must be transmitted. The switch selects the link by creating a binary pattern from selected fields in a packet and associating that pattern with a particular link. The hash mode determines which fields in a packet the switch selects.
9. From the **LAG ID** menu, select an ID.
10. To create a static LAG instead of a dynamic LAG, turn on the **Static** toggle so that it displays green and is positioned to the right.
    When you create a static LAG, the member ports do not transmit LACPDUs, and the LACPDUs that the member ports receive are dropped.
11. Click the **Apply** button.
    Your settings are saved. The window closes. The Link Aggregation Group page displays again.
12. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a LAG

You can change an existing LAG.

To change a LAG:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. In the Link Aggregation Group table, to the right of the LAG that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit Link Aggregation Group window displays.
6. Change the settings as needed.
   For more information about the settings, Create a LAG on page 43.
   You cannot change the LAG ID.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Link Aggregation Group page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a LAG

You can remove an existing LAG that you no longer need.

To remove a LAG:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. In the Link Aggregation Group table, to the right of the LAG that you want to remove, click the **3 dots** icon and select **Delete**.
   A confirmation window displays.
6. Click the **Delete** button.
   The LAG is removed. The window closes. The Link Aggregation Group page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Multicast

Communication from point to multipoint is called multicasting. The source host (point) transmits a message to a group of zero or more hosts (multipoint) that are identified by a single IPv4 destination address. Although the task can be accomplished by sending unicast (point-to-point) messages to each of the destination hosts, multicasting is the preferred method for this type of transmission.

A multicast message is delivered to all members of its destination host group with the same best-efforts reliability as regular unicast IPv4 messages. The message is not guaranteed to arrive intact at all members of the destination group or in the same order relative to other messages.

Multicast is best suited for video and audio traffic requiring multicast packet control for optimal operation. Multicast for IPv4 includes support for IGMPv1, IGMPv2, and IGMPv3. For information about NETGEAR IGMP Plus™ and an example of a multicast spine and leaf topology, visit netgear.com/business/solutions/video-over-ip/.

The chapter contains the following sections:

Configure the multicast mode for one or more ports

By default, if the switch detects multicast traffic on a port, it allows the traffic on the port. You can also force the switch to use one or more specific ports to process multicast traffic. As another option, you can block multicast traffic from selected networks on one or more ports.

Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. If you choose to block multicast traffic on one or more ports, you can select one, several, or all of these multicast address ranges.

To configure the multicast mode for one or more ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

> **NOTE:** The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Multicast**.
   The Multicast page displays.
5. Select the port or ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
6. From the **Multicast Mode** menu, select the multicast mode:
   - **Default**: Multicast traffic is allowed on the selected port or ports based on the protocols that the switch detects. This is the default mode.
   - **Force Multicast**: Multicast traffic is forced through the selected port or ports.
   - **Block Multicast**: Multicast traffic from the networks that you select (see the next step) is blocked on the selected port or ports.
7. If you select **Block Multicast** from the **Multicast Mode** menu in the previous step, in this step select one or more multicast address ranges to be blocked from the **Multicast Block Addresses** menu:
   - **Individual multicast address ranges**: Click the **Network Ranges** text (*not* the check box) and select one or more check boxes for individual network ranges.
   - **All multicast network ranges**: Select the **Network Ranges** check box.

   The switch does not let traffic from a blocked address pass through.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Add or remove blocked multicast address ranges

Multicast host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. You can block one, several, or all of these multicast address ranges, which you then can apply to one or more ports. The switch does not let traffic from a blocked address pass through.

NOTE: If you want remove a blocked multicast range from a port, we recommend that you set the multicast mode for the port to default mode rather than remove the blockage for the multicast range. For more information, see Configure the multicast mode for one or more ports on page 48.

To add or remove blocked multicast address ranges:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. From the **Multicast Block Addresses** menu, select one or more ranges to block or unblock:
   - **Individual multicast address ranges**: Click the **Network Ranges** text (*not* the check box) and select or clear one or more check boxes for individual network ranges.
   - **All multicast network ranges**: Select or clear the **Network Ranges** check box.
5. Click the **Apply** button.
   Your settings are saved.
6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display the multicast groups in your network

The switch automatically detects the multicast groups in your network.

To display the multicast groups in your network:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Multicast**.
   The Multicast page displays.
   The Multicast Groups table displays detailed information about each multicast group in your network.

Legend	Description
Forwarding Port	The port on which multicast is enabled and on which multicast traffic is forwarded in the network.
Network Profile (VLAN)	The network profile to which the port is assigned (see Change the Default VLAN profile on page 15 or Use an AV profile template to configure and assign a network profile on page 17). By default, the port is assigned to the Data network profile with VLAN 1.
Subscriber Address	The IP address of the network device that is subscribed to receive multicast traffic.
Subscriber MAC Address	The MAC address of the network device that is subscribed to receive multicast traffic.
Multicast Address	The IP address of the device from which the multicast traffic originates.
Multicast MAC Address	The MAC address of the device from which the multicast traffic originates.
Type	The IGMP version that is being used (IGMPv1, IGMPv2, or IGMPv3).

Power over Ethernet

You can manage the Power over Ethernet (PoE) options for the interfaces.

The chapter contains the following sections:

- PoE concepts
- Manage PoE port settings
- Disable PoE for one or more interfaces
- PoE schedules
- Display the total PoE consumption for the switch and the PoE information for the ports
- Reset one or more PoE ports

For more information about the PoE management options of the switch, see the main user manual, which you can download by visiting netgear.com/support/download.

PoE concepts

The Power over Ethernet (PoE) models support 8, 24, or 40 PoE+ or PoE++ ports with the capacities and budgets that are described in the following table.

Table 1.PoE port capacities and budgets

Model	PoE Ports	Port Capacity	Switch PoE Budget
M4250-10G2F-PoE+	8 PoE+ (802.3at)	30W	125W
M4250-10G2XF-PoE+	8 PoE+ (802.3at)	30W	240W
M4250-10G2XF-PoE++	8 PoE++ (802.3bt)	90W	720W
M4250-26G4F-PoE+	24 PoE+ (802.3at)	30W	300W
M4250-26G4XF-PoE+	24 PoE+ (802.3at)	30W	480W
M4250-26G4F-PoE++	24 PoE++ (802.3bt)	90W	1440W (with 2 power supplies)
M4250-40G8F-PoE+	40 PoE+ (802.3at)	30W	480W
M4250-40G8XF-PoE+	40 PoE+ (802.3at)	30W	960W
M4250-40G8XF-PoE++	40 PoE++ (802.3bt)	90W	2880W (with 3 power supplies)

Supplied power is prioritized according to the port order, up to the total power budget of the device. For example, on a 24-port model, port 1 receives the highest PoE priority, while port 24 is relegated to the lowest PoE priority.

If the power requirements for attached powered devices (PDs) exceed the total power budget of the switch, the PoE power to the device on the highest-numbered active PoE port is disabled to

make sure that the devices connected to the higher-priority, lower-numbered PoE ports are supported first.

Although a device might be listed as an 802.3bt PoE++-powered or 802.3at PoE+-powered device, it might not require the maximum power limit that is specified by its IEEE standard. Many devices require less power, allowing all PoE ports to be active simultaneously when the devices correctly report their PoE class to the switch.

The following table shows the standard power ranges, calculated with the maximum cable length of 328 feet (100 meters). If a device receives insufficient PoE power from the switch, consider using a shorter cable.

Table 2.PoE classes and PoE power allocations

Device Class	Compatible PoE Standard	Class Description	Maximum Power Reserved for the PD	Power Delivered to the PD
0	PoE, PoE+, and PoE++	Default power (full)	15.4W	0.44W–15.8W
1	PoE, PoE+, and PoE++	Very low power	4.0W	0.44W–3.84W
2	PoE, PoE+, and PoE++	Low power	7.0W	3.84W–7.2W
3	PoE, PoE+, and PoE++	Mid power	15.4W	6.49W–15.9W
4	PoE+ and PoE++	High power	30.0W	12.95W–30.8W
5	PoE++	Ultra high power	45.0W	25.5W–47.0W
6	PoE++	Ultra high power	60.0W	51.0W–64.4W
7	PoE++	Ultra high power	75.0W	62.0W–81.1W
8	PoE++	Ultra high power	90.0W	71.0W–96.5W

Manage PoE port settings

You can manage multiple settings for individual PoE ports.

To manage the PoE port settings:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
5. In the upper right of the page, above the graphical display of the switch, click the **PoE Interface Settings** link.
   The PoE Interface Settings window displays. By default, PoE is enabled for interfaces.
6. Select the port or ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All PoE Ports** check box.

7. Either leave the default PoE mode (802.3at for PoE+ models; 802.3bt for PoE++ models), or, depending on your network devices and requirements, select one of the following modes from the **PoE Standard** menu:
   - **802.3af**: The port is powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if the port functions in IEEE 802.3af mode.
   - **Legacy**: The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
   - **Pre-802.3at**: The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high power IEEE 802.3at mode. Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.
   - **802.3at**: The port is powered in the IEEE 802.3at mode and is backward compatible with IEEE 802.3af. The 802.3at mode is the default mode. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3af but is not an IEEE 802.3at Class 4 device, the PD does not receive power from the switch. For PoE+ models, 802.3at is the default setting.
   - **Pre-802.3bt**: The PoE++ port supports Class 4 devices that use 4-pair PoE (4PPoE) to receive power higher than 30W but that are not compliant with IEEE 802.3bt. The port also supports the IEEE 802.3at and IEEE 802.3af modes.
   - **802.3bt-Type3**: The PoE++ port supports the IEEE 802.3bt Type 3 mode, the IEEE 802.3at mode, and the IEEE 802.3af mode.
   - **802.3bt**: The PoE++ port is powered in the IEEE 802.3bt mode and is backward compatible with IEEE 802.3at and IEEE 802.3af. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3at but is not an IEEE 802.3bt device, the PD does not receive power from the switch. For PoE++ models, 802.3bt is the default setting.
8. Either leave the default detection type (4ptdot3af), or, from the **Detection Type** menu, select how the port detects the attached PD:
   - **4ptdot3af**: The port performs a 4-point resistive detection. This is the default setting.
   - **4ptdot3af+legacy**: The port performs a 4-point resistive detection, and if required, continues with legacy detection.
   - **legacy**: The port performs legacy detection.
9. Either leave the default priority type (Low), or, from the **Priority Type** menu, select the priority for the port in relation to other ports if the total power that the switch is capable of delivering exceeds the total power budget:
   - **Low**: Low priority. This is the default setting.
   - **Medium**: Medium priority.
   - **High**: High priority.
   - **Critical**: Critical priority.

10. Either leave the default power limit type (Class), or, from the **Power Limit Type** menu, select how the port controls the maximum power that it can deliver:
    - **None**: For PoE+ (802.3at) ports, the port draws up to Class 0 maximum power in low power mode. In high power mode, the following applies:
      - **PoE+ (802.3at) ports**: The port draws up to Class 4 maximum power.
      - **PoE++ (802.3bt) ports**: The port draws up to Class 8 maximum power.
    - **Class**: The port power limit is equal to the class of the attached PD. This is the default setting. The upper limit is the power that a port can deliver to a PD. The class is detected based on the PD that is attached to the port, and the following applies:
      - **PoE+ (802.3at) ports**: Possible values are from Class 0 to Class 4.
      - **PoE++ (802.3bt) ports**: Possible values are from Class 0 to Class 8.
    - **User**: The port power limit is equal to the value that you specify in the **Power Limit (Watts)** field.
11. If you select **User** from the **Power Limit Type**, enter the maximum power (in W) that the port can deliver in the **Power Limit (Watts)** field.
    The power value (in W) that you can enter depends on the physical capacity of the port (which depends on the switch model) and the selection from the **PoE Standard** menu:
    - **802.3af**: The value that you can enter ranges from 3.0W to 18.0W.
    - **Legacy**: The value that you can enter ranges from 3.0W to 18.0W.
    - **Pre-802.3at**: The value that you can enter ranges from 3.0W to 32.0W.
    - **802.3at**: The value that you can enter ranges from 3.0W to 32.0W.
    - **Pre-802.3bt**: For PoE++ models, the value that you can enter ranges from 3.0W to 60.0W.
    - **802.3bt-Type3**: For PoE++ models, the value that you can enter ranges from 3.0W to 60.0W.
    - **802.3bt**: For PoE++ models, the value that you can enter ranges from 3.0W to 99.9W.
12. If you set up one or more PoE schedules (see PoE schedules on page 58), from the **PoE Schedule** menu, you can select a schedule.
    The default is None, so that no schedule applies.
13. Click the **Apply** button.
    Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.
14. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Disable PoE for one or more interfaces

By default, PoE is enabled for all interfaces. You can disable PoE for one or more interfaces.

To disable PoE for one or more interfaces:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. In the upper right of the page, above the graphical display of the switch, click the **PoE Interface Settings** link.
   The PoE Interface Settings window displays.
5. Select the port or ports to for which PoE must be disabled.
6. Turn off the **Enable PoE** toggle so that it displays gray and is positioned to the left.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

PoE schedules

You can define multiple PoE schedules (each with a unique name) that you can use for PoE power delivery to attached PDs.

After you create a PoE schedule, you can associate it with one or more PoE ports (see Manage PoE port settings on page 54). You can use a separate timer schedule for each PoE port.

After you associate a PoE schedule with a PoE port, the start date and time force the PoE port to stop delivering power, and the stop date and time enable the PoE port to start delivering power.

Create a PoE schedule

The maximum number of PoE schedules that you can create and add is 100.

To create a PoE schedule:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
5. Below the graphical display of the switch, click the **Create Schedule** link.
   The Create New PoE Schedule window displays.
6. Select the port or ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All PoE Ports** check box .
   You can also set up and save the schedule and add the port or ports later.
7. In the **Schedule Name** field, enter a name for the schedule.

8. From the **Recurrence Type** menu, select the frequency of the recurrence, configure the period during which the schedule is effective (and, for weekly or monthly recurrences, during which the schedule can be either active or inactive), and configure the settings that are associated with your selection from the **Recurrence Type** menu:

- **Daily**: The schedule works with daily recurrence. This is the default setting. You must set the start and end dates and the start and end times that apply during each day. The period that the schedule is effective is defined by the start and end dates (see the following steps). During this period, the schedule can be active or inactive.

  Do the following:

  a. To specify the schedule start date, select a date from the **Start Date** calendar.
  b. To specify the schedule end date, select a date from the **End Date** calendar.
  c. To let the schedule be active all day, turn on the **All Day** toggle so that it displays green and is positioned to the right, or specify specific times by continuing with the following steps.
  d. To specify the schedule start time, select a time from the **Start Time** menu.
  e. To specify the schedule end time, select a time from **End Time** menu.

- **Weekly**: The schedule works with weekly recurrence. The fields in the window adjust. You must select one or more days of the week, set the start and end dates, and set the start and end times that apply during the days that the schedule is effective. Do the following:

  a. Select one or more buttons for the days that the schedule must be active each week during the period that the schedule is effective. The days do not need to be consecutive. The period that the schedule is effective is defined by the start and end dates (see the following steps). During this period, the schedule can be active or inactive.
  b. To specify the schedule start date, select a date from the **Start Date** calendar.
  c. To specify the schedule end date, select a date from the **End Date** calendar.
  d. To let the schedule be active all day, turn on the **All Day** toggle so that it displays green and is positioned to the right, or specify specific times by continuing with the following steps.
  e. To specify the schedule start time, select a time from the **Start Time** menu.
  f. To specify the schedule end time, select a time from **End Time** menu.

- **Monthly**: The schedule works with monthly recurrence. The fields in the window adjust. You must select the day in a month that the schedule becomes active, set the start and end dates, and set the start and end times that apply during the days that the schedule is effective. Do the following:

  a. Click the **Select one for the recurring schedule** field and select the day in a month that the schedule must become active every month during the period that the schedule is effective. The period that the schedule is effective is defined by the start and end dates (see the following steps). During this period, the schedule can be active or inactive.
  b. To specify the schedule start date, select a date from the **Start Date** calendar.
  c. To specify the schedule end date, select a date from the **End Date** calendar.
  d. To let the schedule be active all day, turn on the **All Day** toggle so that it displays

green and is positioned to the right, or specify specific times by continuing with the following steps.

e. To specify the schedule start time, select a time from the **Start Time** menu.
f. To specify the schedule end time, select a time from **End Time** menu.

9. Click the **Apply** button.
   Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.
10. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a PoE schedule

You can change an existing PoE schedule.

To change a PoE schedule:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.
   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).
   To display the password, click the **eye** icon.
   The Overview page displays.
4. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
5. In the PoE Schedule table, to the right of the PoE schedule that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit PoE schedule window displays.
6. Change the settings as needed.
   For more information about the settings, Create a PoE schedule on page 59.
   You cannot change the name of the PoE schedule.

7. Click the **Apply** button.
   Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a PoE schedule

You can remove an existing PoE schedule that you no longer need.

To remove a PoE schedule:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
5. In the PoE Schedule table, to the right of the PoE schedule that you want to remove, click the **3 dots** icon and select **Delete**.
   A confirmation window displays.
6. Click the **Delete** button.
   The PoE schedule is removed. The window closes. The Power over Ethernet (PoE) page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display the total PoE consumption for the switch and the PoE information for the ports

You can display the total PoE power consumption for the switch. The fixed PoE budget for the switch is also displayed. In addition, you can display the PoE details for individual ports, including the port PoE power usage and PoE power type.

To display the total PoE power consumption for the switch and the PoE information for the ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays. The bar below the graphical display shows the total PoE power consumption of the switch, with the maximum PoE budget stated to the right of the bar.

5. The PoE Budget table displays information about the active PoE ports on the switch.

Legend	Description
Port	The port that delivers PoE power to an attached PoE device.
Power Usage	The power in watt (W) that the port provides to the attached device.
PoE Schedule	The PoE schedule, if any, that determines when PoE power is provided to the attached device. For more information about PoE schedules see PoE schedules on page 58.
PoE Type	The PoE class of the attached device. For more information about PoE classes, see PoE concepts on page 53.

Reset one or more PoE ports

You can reset (power-cycle) one or more PoE ports. This might be useful if a PoE port does not function as expected.

To reset one or more PoE ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
5. Select the port or ports to reset.

6. Click the **PoE Reset** button.
   A pop-up window displays a warning. When you reset a PoE port, the connected PoE device reboots.
7. Click the **Yes** button.
   The port or ports are reset.

Port Configuration

For the physical ports and LAGs on the switch, you can display the settings and configure the administrative mode of a port or LAG (both of which are enabled by default), the frame size for a port, and the flow control for a port. You can also add port descriptions.

NOTE: In this chapter, we use the term *interface* to indicate both physical ports and link aggregation interfaces.

The chapter contains the following sections:

Add a description for one or more interfaces

You can add a description for a port or LAG. This description is for informational purposes only.

NOTE: When you configure a network profile to a port from the AV UI, the VLAN ID, profile name, and profile template automatically display in the CLI as interface descriptions.

To add a description for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.
5. (**Single port or LAG**) To add a description for an individual port or LAG, do the following:
   a. Select the check box for the port or LAG.
   b. In the **Port Description** field for the port or LAG, type a text.
6. (**Multiple ports or LAGs**) To add the same description for multiple ports, LAGs, or both, do the following:
   a. Select the check boxes for the ports, LAGs, or both.
   b. In the **Port Description** field in the table header row, type a text.
7. (**All ports and LAGs**) To add the same description for all ports and LAGs, do the following:
   a. Select the check box in the table header row.
   b. In the **Port Description** field in the table header row, type a text.
8. Click the **Apply** button.
   Your settings are saved. The description displays in the Port Interface Details table.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Administratively enable or disable one or more interfaces

By default, all ports and LAGs are administratively enabled. You can manually disable a port or LAG, but this can also occur automatically if a fault or other condition occurs. After a port or LAG is manually or automatically disabled, you can reenable the port or LAG.

To administratively enable or disable one or more ports or LAGs:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.

5. (**Single port or LAG**) To administratively enable or disable an individual port or LAG, do the following:
   a. Select the check box for the port or LAG.
   b. From the **Admin Mode** menu for the port or LAG, select **Enable** (the default setting) or **Disable**.

6. (**Multiple ports or LAGs**) To administratively enable or disable multiple ports, LAGs, or both, do the following:
   a. Select the check boxes for the ports, LAGs, or both.
   b. From the **Admin Mode** menu in the table header row, select **Enable** (the default setting) or **Disable**.

7. (**All ports and LAGs**) To administratively enable or disable all ports and LAGs except for the management port, do the following:
   a. Select the check box in the table header row.
   b. Clear the check box for the management port.
   c. From the **Admin Mode** menu in the table header row, select **Enable** (the default setting) or **Disable**.

8. Click the **Apply** button.
   Your settings are saved.

9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure STP and CST settings for one or more interfaces

You can configure the following interface settings that are related to STP and CST:

- **STP Mode**: Lets you enable or disable the Spanning Tree Protocol administrative mode for the port or LAG. The default setting is enabled.
- **Admin STP Edge Port**: Lets you enable or disable the port or LAG as an edge port in the Common and Internal Spanning Tree (CIST). The default setting is enabled.
- **TCN Guard**: Lets you enable or disable the port or LAG from propagating any topology change information that it receives. The default setting is disabled.
- **BPDU Filter**: Lets you enable or disable the BPDU Filter feature on the port or LAG. A BPDU filter normally applies to an operational edge port. An edge port in an operational state connects to hosts that typically drop BPDUs. If an operational edge port receives a BPDU, it loses its operational status. If a port on which BPDU filtering is enabled receives BPDUs, the port drops the BPDUs and remains operational. The default setting is disabled.

To configure STP and CST settings for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.

5. (**Single port or LAG**) To configure STP and CST settings for an individual port or LAG, do the following:
   a. Select the check box for the port or LAG.
   b. From the **STP Mode** menu, **Admin STP Edge Port** menu, **TCN Guard** menu, and **BPDU Filter** menu for the port or LAG, select **Enable** or **Disable**.

      For more information about these menus, see the introduction to this procedure.
6. (**Multiple ports or LAGs**) To configure STP and CST settings for multiple ports, LAGs, or both, do the following:
   a. Select the check boxes for the ports, LAGs, or both.
   b. From the **STP Mode** menu, **Admin STP Edge Port** menu, **TCN Guard** menu, and **BPDU Filter** menu in the table header row, select **Enable** or **Disable**.

      For more information about these menus, see the introduction to this procedure.
7. (**All ports and LAGs**) To configure STP and CST settings for all ports and LAGs, do the following:
   a. Select the check box in the table header row.
   b. From the **STP Mode** menu, **Admin STP Edge Port** menu, **TCN Guard** menu, and **BPDU Filter** menu in the table header row, select **Enable** or **Disable**.

      For more information about these menus, see the introduction to this procedure.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure autonegotiation or speed and duplex mode for one or more interfaces

NOTE: You can set the speed for Ethernet ports. For SFP ports, the speed is automatically detected and you cannot change it.

For an interface (a physical port), you can either enable speed and duplex mode autonegotiation or disable autonegotiation and manually set the speed and duplex mode:

- **Autonegotiation**: From the Autonegotiation menu, select to enable or disable the speed autonegotiation mode for the port. The default is Enable.
- **Speed**: If you disable autonegotiation, you can change the speed for the port, depending on the type of port:
  - **Gigabit Ethernet port**:
    - Auto: The speed is set by the auto-negotiation process. This is the default setting.
    - 1000: The speed is set to 1 Gbits/second (Gbps)
    - 100: The speed is set to 100 Mbits/second (Mbps)
  - **Multispeed Ethernet port** or 10G port:
    - 10G: The speed is set to 10 Gbps.
    - 5G: The speed is set to 5 Gbps. (This setting does not apply to a 10G port.)
    - 2.5G: The speed is set to 2.5 Gbps. (This setting does not apply to a 10G port.)
    - 1000: The speed is set to 1 Gbps.
    - 100: The speed is set to 100 Mbps.
- **Duplex Mode**: If you disable autonegotiation, you can change the duplex mode to half duplex for a port operating at 100 Mbps speed. For ports operating at speeds of 1 Gbps or higher, the mode can be full duplex or Auto.

NOTE: If you change the autonegotiation, speed, or duplex mode for a physical port, the switch might be inaccessible for a number of seconds while the new settings take effect.

To configure either autonegotiation or speed and duplex mode for one or more ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.

5. (**Single port**) To configure either autonegotiation or speed and duplex mode for an individual port, do the following:
   a. Select the check box for the port.
   b. From the **Autonegotiation** menu for the port, select **Enable** (the default setting) or **Disable**.
   c. If you select **Disable** from the **Autonegotiation** menu for the port, do the following:
      - From the **Speed** menu for the port, select the speed.
      - From the **Duplex Mode** menu for the port, select the duplex mode.

      For more information about speed and duplex mode, see the introduction to this procedure.

6. (**Multiple ports**) To configure either autonegotiation or speed and duplex mode for multiple ports, do the following:
   a. Select the check boxes for the ports.
   b. From the **Autonegotiation** menu in the table header row, select **Enable** (the default setting) or **Disable**.
   c. If you select **Disable** from the **Autonegotiation** menu in the table header row, do the following:
      - From the **Speed** menu in the table header row, select the speed.
      - From the **Duplex Mode** menu in the table header row, select the duplex mode.

      For more information about speed and duplex mode, see the introduction to this procedure.

7. (**All ports**) To configure either autonegotiation or speed and duplex mode for all ports, do the following:
   a. Select the check box in the table header row.
   b. From the **Autonegotiation** menu in the table header row, select **Enable** (the default setting) or **Disable**.
   c. If you select **Disable** from the **Autonegotiation** menu in the table header row, do the following:
      - From the **Speed** menu in the table header row, select the speed.
      - From the **Duplex Mode** menu in the table header row, select the duplex mode.

   For more information about speed and duplex mode, see the introduction to this procedure.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Set the frame size for one or more interfaces

The frame size is the maximum Ethernet frame size that the interface supports or is configured to use, including the Ethernet header, CRC, and payload. The default size is 9198.

To set the frame size for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.
5. (**Single port or LAG**) To set the frame size for an individual port or LAG, do the following:
   a. Select the check box for the port or LAG.
   b. In the **Frame Size** field for the port or LAG, enter a value. The minimum value is 1500 and the maximum value is 9198, which is also the default value.
6. (**Multiple ports or LAGs**) To set the frame size for multiple ports, LAGs, or both, do the following:
   a. Select the check boxes for the ports, LAGs, or both.
   b. In the **Frame Size** field in the table header row, enter a value. The minimum value is 1500 and the maximum value is 9198, which is also the default value.
7. (**All ports and LAGs**) To set the frame size for all ports and LAGs, do the following:
   a. Select the check box in the table header row.
   b. In the **Frame Size** field in the table header row, enter a value. The minimum value is 1500 and the maximum value is 9198, which is also the default value.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure flow control for one or more interfaces

You can configure IEEE 802.3x flow control, which can help to prevent data loss when the port cannot keep up with the number of frames being switched:

- **Symmetric flow control**: With symmetric flow control, the switch can send a pause frame to stop traffic on the port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices. The paused port does not forward packets for the time that is specified in the pause frame. When the pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames.
- **Asymmetric flow control**: With asymmetric flow control, the switch does not send pause frames, but does honor incoming pause frames by temporarily halting transmission.

To configure flow control for one or more ports:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.

5. (**Single port**) To configure flow control for an individual port, do the following:
   a. Select the check box for the port.
   b. From the **Flow Control** menu for the port, select what happens if the port buffers become full:
      - **Disable**: The switch does not send pause frames, and data loss could occur. This is the default setting.
      - **Symmetric**: The switch sends pause frames to stop traffic. The switch also honors incoming pause frames by temporarily halting transmission.
      - **Asymmetric**: The switch does not send pause frames, and data loss could occur. However, the switch does honor incoming pause frames by temporarily halting transmission.

6. (**Multiple ports**) To configure flow control for multiple ports, do the following:
   a. Select the check boxes for the ports.
   b. From the **Flow Control** menu in the table header row, select what happens if the port buffers become full:
      - **Disable**: The switch does not send pause frames, and data loss could occur. This is the default setting.
      - **Symmetric**: The switch sends pause frames to stop traffic. The switch also honors incoming pause frames by temporarily halting transmission.
      - **Asymmetric**: The switch does not send pause frames, and data loss could occur. However, the switch does honor incoming pause frames by temporarily halting transmission.
7. (**All ports**) To configure flow control for all ports, do the following:
   a. Select the check box in the table header row.
   b. From the **Flow Control** menu in the table header row, select what happens if the port buffers become full:
      - **Disable**: The switch does not send pause frames, and data loss could occur. This is the default setting.
      - **Symmetric**: The switch sends pause frames to stop traffic. The switch also honors incoming pause frames by temporarily halting transmission.
      - **Asymmetric**: The switch does not send pause frames, and data loss could occur. However, the switch does honor incoming pause frames by temporarily halting transmission.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure broadband storm control for one or more interfaces

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources, cause the network to time out, or do both. The switch measures the incoming packet rate per port for broadcast, multicast, unknown, and unicast packets and discards packets if the rate exceeds the defined value. (You can define the value in the Main UI.) You can enable or disable storm control per interface.

To configure broadband storm control for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.
5. (**Single port**) To configure broadcast storm control for an individual port, do the following:
   a. Select the check box for the port.
   b. From the **Broadcast Storm Control** menu for the port, select **Enable** (the default setting) or **Disable**.
6. (**Multiple ports**) To configure broadcast storm control for multiple ports, do the following:
   a. Select the check boxes for the ports.
   b. From the **Broadcast Storm Control** menu in the table header row, select **Enable** (the default setting) or **Disable**.
7. (**All ports**) To configure broadcast storm control for all ports, do the following:
   a. Select the check box in the table header row.
   b. From the **Broadcast Storm Control** menu in the table header row, select **Enable** (the default setting) or **Disable**.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display detailed information about the physical ports and LAGs

To display detailed information about the physical ports and LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Port configuration**.
   The Port Interface Details page displays.
   The table displays detailed information about each port and LAG.

Legend	Description
Port Description	The description that you added (see Add a description for one or more interfaces on page 67). If you did not add a description, this field is blank. **NOTE:** When you configure a network profile from the AV UI, the VLAN ID, profile name, and profile template automatically display in the CLI as interface descriptions.
Admin Mode	The administrative mode that you set (see Administratively enable or disable one or more interfaces on page 68). By default, the mode is enabled.
STP Mode	The STP mode that you configured (see Configure STP and CST settings for one or more interfaces on page 70). By default, the mode is enabled.
Admin STP Edge Port	The STP edge port mode that you configured (see Configure STP and CST settings for one or more interfaces on page 70). By default, the mode is disabled.
TCN Guard	The TCN guard mode that you configured (see Configure STP and CST settings for one or more interfaces on page 70). By default, the mode is disabled.
Port Forwarding State	A view-only field that displays the current STP state of the interface (a port or LAG). If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are as follows: ○ **Disabled**: STP is currently disabled on the interface. The interface forwards traffic while learning MAC addresses. ○ **Blocking**: The interface is currently blocked and cannot be used to forward traffic or learn MAC addresses. ○ **Listening**: The interface is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses. ○ **Learning**: The interface is currently in the learning mode. The interface cannot forward traffic. However, it can learn new MAC addresses. ○ **Forwarding**: The interface is currently in the forwarding mode. The interface can forward traffic and learn new MAC addresses. ○ **Manual forwarding**: The interface is currently in the manual forwarding mode. The interface can forward traffic and learn new MAC addresses.
Link Status	A view-only field that displays if the port or LAG is up or down.
Autonegotiation	By default, autonegotiation is enabled, but if you disable it (see Configure autonegotiation or speed and duplex mode for one or more interfaces on page 72), you can manually set the speed and duplex mode for the

Legend	Description
	interface. This setting does not apply to LAGs.
Speed	If autonegotiation is disabled, you can manually select the speed for the interface (see Configure autonegotiation or speed and duplex mode for one or more interfaces on page 72). This setting does not apply to LAGs.
Duplex Mode	If autonegotiation is disabled, you can manually set the duplex mode for the interface (see Configure autonegotiation or speed and duplex mode for one or more interfaces on page 72). This setting does not apply to LAGs.
BPDU Filter	The BPDU filter setting that you configured (see Configure STP and CST settings for one or more interfaces on page 70). By default, the mode is disabled.
Frame Size	The frame size (see Set the frame size for one or more interfaces on page 74). If you did not change the frame size, the default frame size displays. (The size and supported range depends on the switch model.)
Flow Control	The mode of flow control (see Configure flow control for one or more interfaces on page 75) . If you did not configure flow control, it is disabled.
Broadcast Storm Control	The broadcast storm control setting that you configured (see Configure broadband storm control for one or more interfaces on page 77). By default, the mode is enabled.
Profile Name	A view-only field that displays the name of the network profile to which the port or LAG is assigned. By default, the profile name is Default.
Profile Template	A view-only field that displays the profile template on which the network profile is based, that is, the network profile to which the port or LAG is assigned. For more information, see Change the Default VLAN profile on page 15 or Use an AV profile template to configure and assign a network profile on page 17. By default, the profile template is Data.

Security

You can configure 802.1X port authentication and the as sociated RADIUS server settings.

The chapter contains the following sections:

For information about all security options of the switch, see the main user manual or CLI reference manual, both of which you can download by visiting netgear.com/support/download.

Port authentication

With port-based authentication, if 802.1X is enabled both globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. 802.1X is the default authentication mode. 802.1X is also referred to as dot1x.

An 802.1X network includes three components:

- **Authenticator**: The port that is authenticated before access to system services is permitted.
- **Supplicant**: The host that is connected to the authenticated port requesting access to the system services.
- **Authentication server**: The external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

For port authentication to function, you must configure at least one RADIUS server (see RADIUS servers on page 87).

Manage port authentication for individual ports

After you enable 802.1X port authentication globally, the default port authentication mode on the ports is Auto.

However, before you enable 802.1X access authentication globally (see Manage 802.1X authentication on page 85), manually set the port authentication mode of the uplink port or ports to Authorized to enable the switch to keep its network connection and, if applicable, Internet connection.

To assign a port authentication mode to individual ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Security**.
   The Security page displays.
5. Select the ports to which you want to assign a port authentication mode.
   To select all ports, select the **Select All Ports** check box.
6. From the menu below the graphical display, select the authentication mode for the selected ports:
   - **Auto**: The authenticator port access entity (PAE) sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. This is the default setting.
   - **Authorized**: The authenticator PAE unconditionally sets the controlled port to authorized.
   - **Unauthorized**: The authenticator PAE unconditionally sets the controlled port to unauthorized.

7. Click the **Apply** button.
   Your settings are saved.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Manage 802.1X authentication

If you enable 802.1X access authentication, port authentication is performed by a RADIUS server. If you disable 802.1X access authentication, port authentication is globally disabled and the switch allows traffic on any ports without authentication.

NOTE: Before you enable 802.1X access authentication globally, manually set the port authentication mode of the uplink port or ports to Authorized (see Manage port authentication for individual ports on page 84) to enable the switch to keep its network connection and, if applicable, Internet connection.

To manage 802.1X access authentication:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Security**.
   The Security page displays.

5. In the RADIUS Server Settings section, do one of the following:
   - **Enable 802.1X access authentication**: Turn on the **802.1x Access Authentication** button so that it displays green and is positioned to the right.

     CAUTION: Before you enable 802.1X access authentication, manually set the port authentication mode of the uplink port or ports to Force-Authorized (see Manage port authentication for individual ports on page 84).
   - **Disable 802.1X access authentication**: Turn off the **802.1x Access Authentication** button so that it displays gray and is positioned to the left.

     This is the default setting.
6. Click the **Apply** button.
   Your settings are saved.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove port authentication from individual ports

After you remove port authentication form a port, the switch allows traffic on the port without authentication.

To remove port authentication mode from individual ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Security**.
   The Security page displays.

5. Select the ports from which you want to remove port authentication.
   To select all ports, select the **Select All Ports** check box.
6. Click the **Remove Port Authentication** button.
7. Click the **Apply** button.
   Your settings are saved.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

RADIUS servers

RADIUS servers provide additional security for networks. A RADIUS server maintains a user database, which can contain per-user or per-port authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password or port and password before authorizing use of the network.

Configure the basic settings for a RADIUS server

After you enable 802.1X access authentication globally (see Manage 802.1X authentication on page 85), you can configure one or more RADIUS servers.

The main UI and CLI let you manage extensive RADIUS settings.(For the M4500 series switches, use the CLI.) For more information, see the main user manual or CLI reference manual, both of which you can download by visiting netgear.com/support/download.

To configure the basic settings for a RADIUS server:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

> **NOTE:** The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Security**.
   The Security page displays.
5. In the RADIUS Server Settings section, do one of the following:
   - **Add a new RADIUS server**: To add the settings for a new RADIUS server, click the **+ Add Server** link.
   - **Change a RADIUS server**: To change the settings for a RADIUS server that you previously added, click the server link, for example, **Server1** or **Server2**.
6. Configure the settings for the RADIUS server in the following fields:
   - **RADIUS Address**: The IP address of the RADIUS server. The switch must be able to reach this IP address. You cannot change the IP address for a RADIUS server that you previously added.
   - **Port Number**: The UDP port number used to reach the RADIUS server. The default is port 1812. You can specify a custom port in the range from 1 to 65535.
   - **Secret Key**: The secret key is the password for authentication and encryption of all RADIUS communications between the switch and the RADIUS server. This password must match the one that is configured on the RADIUS server. You cannot change the secret key for a RADIUS server that you previously added.
7. Click the **Apply** button.
   Your settings are saved.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a RADIUS server

You can remove a RADIUS server that you no longer need.

To remove the settings for a RADIUS server:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Security**.
   The Security page displays.

5. In the RADIUS Server Settings section, next to the server, click the **x**.
   For example, to remove the second RADIUS server that you added, click the **x** next to Server2 .

6. Click the **Apply** button.
   Your settings are saved.

7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Manage and monitor the switch

You can manage the firmware of the switch, set the switch to factory defaults, and activate a new AVB license. You can also display the switch logs.

The chapter contains the following sections:

For information about all management and monitoring options of the switch, see the main user manual or CLI reference manual, both of which you can download by visiting netgear.com/support/download.

Update the firmware

You can update the firmware through the AV UI.

To update the firmware:

1. Download the firmware file to the computer that you use to access the AV UI.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

4. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

5. Select **Configure > Maintenance**.
   The Maintenance page displays.

   NOTE: The switch can hold two firmware versions. If it does, the page displays the active firmware version. The main UI and CLI let you manage firmware files, and change from one version to another. The AV UI lets you update the firmware but does not let you manage firmware versions. If you update firmware using the AV UI, the new firmware becomes the active firmware.

6. Click in the **Browse Field** field, navigate to the firmware file, and select it.
   The firmware file is in `.stk` format.

7. Click the **Upload** button.
   A pop-up window displays the progress of the firmware file upload.

8. After the upload completes, in the pop-up window, click the **Reboot Now** button.
   The firmware upgrade process starts. During the firmware upgrade, do not power down the switch. The switch reboots and restart with the new firmware version. When the process is complete, you can log in again to the AV UI.

Startup configuration

You can manage the startup configuration, that is, the startup-config file. You can do the following:

- Save the running configuration to the startup configuration.
- Download the running configuration file.
- Restore the running and startup configurations from a previously downloaded configuration file.

Save the running configuration

After you make changes on a page of the AV UI and click the **Apply** button (or, in some windows, the **Save** button), your changes are saved for the current session, but are not retained when you restart the switch. That is, your running configuration is not saved to the startup configuration (the startup-config file).

NOTE: The idle time-out period for an AV UI session is five minutes. However, if you are automatically logged out of the AV UI and then log in again, the running configuration is not lost and you can save it to the startup configuration.

To save the running configuration to the startup configuration:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. At the top of the page, click the **Save** icon or text.
   The running configuration is saved to the startup configuration.

Download the running configuration

You can download the running configuration (that is, the current configuration) to a computer. If you do so, you can restore both the running configuration and startup configuration from your saved configuration file.

To download the running configuration:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Maintenance**.
   The Maintenance page displays.

5. In the Configuration Management section, click the **Download Configuration** button.
   A pop-up window displays.

6. Navigate to a location on your computer and save the text file.
   The file is saved with a `.cfg` extension.

Restore the configuration

If you downloaded the configuration to a computer (see Download the running configuration on page 92), you can restore both the running configuration and startup configuration from your saved configuration file.

To restore the configuration:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Configure > Maintenance**.
   The Maintenance page displays.
5. In the Configuration Management section, click in the **Browse File** field.
   A pop-up window displays.
6. Navigate to and select the saved configuration file.
   The file has a `.cfg` extension.
7. Click the **Upload** button.
   A pop-up window displays.
8. Click the **Restore Now** button.
   The running configuration and startup configuration are restored.

Date and time settings

You can either set the date and time for the switch manually or configure one or more Simple Network Time Protocol (SNTP) servers, allowing the switch to synchronizing its internal clock with an SNTP server clock.

Manually set the date and time

You can manually set the date and time for the switch.

To manually set the date and time:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. In the Device Details section, below the Date & Time field, click the **pencil** icon.
   The Time Configuration window displays.
5. Click in the **Date** field, and from the pop-up calendar, select a date.
6. Click in the **Time** field, use the menus to select the hour, minutes, seconds, and meridian setting, and click the **OK** button.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure one or more SNTP servers

You can configure one or more SNTP servers. You must know the domain names or IP addresses of the servers that you want to use. By default, the switch configuration includes one NETGEAR time server, which is time-a.netgear.com.

To configure one or more SNTP servers:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. In the Device Details section, below the Date & Time field, click the **pencil** icon.
   The Time Configuration window displays.
5. Turn on the **Enable SNTP** toggle so that it displays green and is positioned to the right.
6. From the **Time Zone** menu, select the time zone in which the switch operates.
7. In the **SNTP Server Address 1**, **SNTP Server Address 2**, and **SNTP Server Address 3** fields, enter the domain name or IP address for an SNTP server.
   By default, the SNTP Server Address 1 field contains the NETGEAR SNTP server (time-a.netgear.com), but you can replace that SNTP server with another one. Configuring the additional two SNTP servers is optional.
8. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Add a system name

You can add a system name, which allows you and others to identify the switch in the network. By default, no system name is configured.

To add a system name:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. In the Device Details section, below the System Name field, click the **pencil** icon.
   The Edit System Name window displays.
5. In the **New System Name** field, specify a system name.
6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Management interface IP address

The management interface is the logical interface used for in-band connectivity with the switch over any of the switch's network interfaces.

You can set a fixed IP address for the management interface or enable the DHCP client for the interface so that the interface receives an IP address from a DHCP server in your network.

If the management interface does not receive an IP address from a DHCP server, the default IP address for the interface is set to 169.254.100.100 with 255.255.0.0 as the subnet mask.

Set a fixed IP address or change the management VLAN for the management interface

By default, the IP address of the management interface is 169.254.100.100 and the DHCP client is enabled. You can disable the DHCP client for the management interface and set a fixed (static) IP address. You can also change the management VLAN.

To set a fixed IP address or change the management VLAN for the management interface:

1. Launch a web browser.

2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. In the Device Details section, below the Management IP Address field, click the **pencil** icon.
   The Edit Management IP Address window displays.

5. From the **Management IP Settings** menu, select **Static** and specify the following settings:
   - **Management IP Address**: The static IP address for the management interface. The default value is 169.254.100.100.
   - **Subnet Mask**: The IP subnet mask for the management interface. This is also referred to as the subnet/network mask and defines the portion of the interface's IP address that is used to identify the attached network. The default value is 255.255.0.0.
   - **Default Gateway**: The gateway through which the management interface can be reached. The default value is 0.0.0.0.
   - **Management VLAN**: The VLAN ID through which the management interface can be reached. The default management VLAN ID is 1.

   WARNING: If you are logged in to switch over the management interface, when you click the **Apply** button, you are disconnected and need to log in to the switch at the new IP address.

6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.

7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Enable the DHCP client for the management interface

By default, the DHCP client for the management interface is enabled. If you set a fixed IP address for the management interface, the DHCP client is disabled. You can enable the DHCP client again.

To enable the DHCP client for the management interface:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. In the Device Details section, below the Management IP Address field, click the **pencil** icon.
   The Edit Management IP Address window displays.
5. From the **Management IP Settings** menu, select **DHCP client**.

   WARNING: If you are logged in to switch over the management interface, when you click the **Apply** button, you are disconnected and need to log in to the switch at the new IP address that is assigned by the DHCP server. If you do not know the new IP address, determine it by accessing the DHCP server or by using an IP scanner utility.

6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

OOB port IP address

The OOB port, also referred to as the IPv4 service port, is a dedicated Ethernet port for out-of-band (OOB) management of the switch. Traffic on this port is segregated from operational

network traffic on the switch ports and cannot be switched or routed to the operational network.

By default, no IP address is set for the OOB port, but its DHCP client is enabled so that the port can receive an IP address from a DHCP server in your network.

If the OOB port does not receive an IP address from a DHCP server in your network, the IP address for the port is set to 192.168.0.239 with 255.255.255.0 as the subnet mask. The same occurs if you connect the OOB port directly to a computer and reboot the switch.

You can also set a fixed IP address for the OOB port.

Set a fixed IP address for the OOB port

By default, no IP address is set for the OOB port and the DHCP client is enabled. You can disable the DHCP client for the OOB port and set a fixed (static) IP address.

To set a fixed IP address for the OOB port:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. In the Device Details section, below the OOB IP Address field, click the **pencil** icon.
   The Edit OOB IP Address window displays.

5. From the **OOB IP Settings** menu, select **Static** and specify the following settings:
   - **OOB IP Address**: The static IP address for the OOB port. By default, no IP address is set for the OOB port.
   - **Subnet Mask**: The IP subnet mask for the OOB port. By default, no subnet mask is set for the OOB port.
   - **Default Gateway**: The gateway through which the OOB port can be reached. By default, no IP address is set for the default gateway.

   WARNING: If you are logged in to switch over the OOB port, when you click the **Apply** button, you are disconnected and need to log in to the switch at the new IP address.

6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Enable the DHCP client for the OOB port

By default, the DHCP client for the OOB port is enabled.

If you connect the OOB port to your network but the port does not receive an IP address from a DCHP server, the IP address for the port is set to 192.168.0.239 with 255.255.255.0 as the subnet mask. The same occurs if you connect the OOB port directly to a computer and reboot the switch.

If you set a fixed IP address for the OOB port, the DHCP client is disabled. You can enable the DHCP client again.

To enable the DHCP client for the OOB port:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. In the Device Details section, below the OOB IP Address field, click the **pencil** icon.
   The Edit OOB IP Address window displays.

5. From the **OOB IP Settings** menu, select **DHCP Client**.

   WARNING: If you are logged in to switch over the OOB port, when you click the **Apply** button, you are disconnected and need to log in to the switch at the new IP address that is assigned by the DHCP server. If you do not know the new IP address, determine it by accessing the DHCP server or by using an IP scanner utility.

6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.

7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Set the STP network redundancy for the switch

You can set the Spanning Tree Protocol (STP) network redundancy for the switch. This is also referred to as the bridge priority, which is the priority for a multiple spanning tree (MST) instance on the switch.

When switches or bridges are running STP, each is assigned a priority. After exchanging bridge protocol data units (BPDUs), the switch with the lowest priority value becomes the root bridge and the other devices become backup or redundant bridges. The bridge priority is a multiple of 4096. The range is from 0 to 61440. The default is 32768.

The following table shows how the network redundancy settings in the AV UI align with the bridge priority values in the main UI. (The M4500 series switches do not support a main UI.)

Table 3.STP network redundancy in the AV UI and the main UI

Configurable Setting in the AV UI	Associated Bridge Priority Value in the AV UI	Configurable Bridge Priority Setting in the Main UI
Primary mode	0	0
Neutral mode	32768	Any value from 4096~57344
Backup mode	8192	61440

In the AV UI, you can set the STP network redundancy to Primary mode, Neutral mode, or Backup mode. In the main UI, you must set a specific bridge priority value.

To set the STP network redundancy for the switch:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. In the Device Details section, below to the STP Network Redundancy field, click the **pencil** icon.
   The Edit STP Network Redundancy window displays.
5. Do one of the following:
   - Set a mode with a preconfigured priority by selecting the **Primary mode (0)**, **Neutral mode (32768)**, or **(Backup 8192)** radio button.
     By default, the Neutral mode (32768) radio button is selected.
   - Configure a custom priority by clicking **Custom Priority** and selecting a preconfigured custom value (from 0 to 61440) from the menu that becomes available.
6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Restart the switch from the AV UI

You can restart the switch from the AV UI.

To restart the switch:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.
   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).
   To display the password, click the **eye** icon.
   The Overview page displays.
4. At the top of the page, click the **Reboot** icon or text.
   A pop-up window displays a warning.

5. Click the **Yes** button.
   The switch restarts. During the restart process, do not power down the switch.

Reset the switch to factory default settings

You can reset the switch to factory default settings. This process erases all your custom settings, including your network profile assignments and any custom profile templates.

After the switch restarts, its default IP address is 169.254.100.100, the DHCP client is enabled, and the IP address of the OOB port is 192.168.0.239.

To reset the switch to factory default settings:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Maintenance**.
   The Maintenance page displays.
5. Click the **Factory Default** button.
   A pop-up window displays a warning.

   CAUTION: This process erases all your custom settings, including your network profile assignments and any custom profile templates.

6. In the pop-up window, click the **Confirm** button.
   The factory default reset process starts. During the reset process, do not power down the switch. The switch reboots and restarts with factory default settings. When the process is complete, you can log in again to the AV UI, but you first might need to determine the IP address of the switch.

Manually control the fans

The switch includes internal fans that support intelligent operation, which enables the switch to automatically start the operation of the fans, gradually increase the speed of the fans, and either halt PoE or block traffic if the temperature exceeds a critical level.

You can manually control the fans through either the AV UI (see the following procedure) or the command-line interface (CLI).

For the M4250 series switches, if the fans are functioning in Off mode (which you only can set manually) or in Quiet mode, the switch automatically manages the fans and turns on the fans or gradually increases the speed of the fans under the following conditions:

- **PoE+ and PoE++ models**: *Either* the temperature detected by the temperature sensor exceeds its threshold *or* a PoE budget is exceeded.
- **LED tiles model (M4250-12M2XF)**: *Either* the temperature detected by the temperature sensor exceeds its threshold *or* the switch processes a full traffic load.
- **Aggregation model (M4250-16XF)**: *Either* the temperature detected by the temperature sensor exceeds its threshold *or* the switch processes a full traffic load.

NOTE: For detailed information about temperature thresholds, PoE budgets, and traffic load conditions that affect the fans, see the hardware installation guide, which you can download by visiting netgear.com/support/download.

To manually control the fans:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. In the Fans & Temperature section, select one of the following radio buttons.
   - **Off**: The fans are off and produce no noise. You can only manually set the fans in Off mode. The following M4250 series models do not support Off mode.
     - M4250-26G4F-PoE++
     - M4250-40G8XF-PoE+
     - M4250-40G8XF-PoE++
   - **Quiet**: The fans function from 10, 20, or 25 percent (depends on the model) to 100 percent speed. Quiet mode is the default mode. At 10, 20, or 25 percent speed, the fans produce minimal noise. Fan noise increases at 50 percent speed and even more so at 75 percent speed. At 100 percent speed, the fans produce considerable noise. In Quiet mode, the switch might automatically change back and forth between Cool mode and Quiet mode until a temperature, PoE budget, or traffic load condition returns within thresholds.
   - **Cool**: The fans consistently function at 100 percent speed and produce maximum cooling as well as considerable noise.

   The fan setting changes immediately. However, depending on the switch model, if the temperature detected by the temperature sensor exceeds its threshold, a PoE budget is exceeded, or a traffic load condition is exceeded, the switch automatically overrides your manual setting.
5. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display the status of the ports and switch

To display the status of the ports and switch:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

> **NOTE:** The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. To display detailed information about a port that is connected to a device, point to the port in the graphical display of the switch.
   A pop-up window displays information about multiple properties of the port.

5. If the port legends do not display below the graphical display of the switch, select the **Show Legends** check box.
   The following table describes the ports legend.

Legend	Description
Connected	The port is connected to a device that is powered up.
Connected & Powered	The port is connected to a powered device (PD) that is receiving PoE from the switch.
Error	An error occurred on the port.
Disabled	The port is disabled.
Available	The port is not connected to a device but is available.
Blocked	The port is blocked. That is, STP blocked the port to prevent a loop.
Admin Down	The port is administratively down.
Warning	The port reached 98 percent of its ingress or egress transmit rate.
PoE	Depending on the switch model, the port is a PoE port. Also, depending on the switch model, the port can provide PoE+ or both PoE+ and PoE++.
PoE Disabled	PoE is disabled on the port (see Disable PoE for one or more interfaces on page 58).
Force-Authorized	802.1X access authentication is enabled and the port authentication mode is Force-Authorized (see Port authentication on page 83).
Force-Unauthorized	802.1X access authentication is enabled and the port authentication mode is Force-Unauthorized (see Port authentication on page 83).
Authorized	802.1X access authentication is enabled and the port authentication status is Authorized.
Unauthorized	802.1X access authentication is enabled and the port authentication status is Unauthorized.
LAG	The port is member of a LAG (see Link Aggregation on page 40).
VLAN Trunk	The port functions as a VLAN trunk. That is, the port is a tagged port that processes tagged VLAN traffic.
Auto Trunk	The port functions as an Auto-Trunk (see Auto-Trunk overview on page 35).
Force Multicast	This port is configured for forced multicast (see Configure the multicast mode for one or more ports on page 48).
1G SFP Fiber Port	Depending on the switch model, the port is a 1G SFP fiber port that can accept an SFP transceiver module.
10G SFP+ Fiber Port	Depending on the switch model, the port is a 10G SFP+ fiber port that can accept an SFP or SFP+ transceiver module.

Legend	Description
Creston Device Connected	Depending on the switch model, a Creston device is connected to the port.
Visionary Device Connected	Depending on the switch model, a Visionary device is connected to the port.
NUCLEUS Device Connected	Depending on the switch model, a NUCLEUS device is connected to the port.

For more information about the ports, see Display detailed information about the physical ports and LAGs on page 79.

The following table describes the information that displays in the Device Details section, Configured Profiles section, CPU Utilization graph, Memory Utilization graph, and Fans & Temperature section.

Field or Graph	Description
Device Details	
Product Name	M4250 by default. This field is fixed.
Serial Number	The serial number of the switch. This field is fixed.
Model	The model number of the switch. This field is fixed.
Date & Time	The configured or detected date and time (see Date and time settings on page 94).
Country/Region	This field does not apply to the switch (N/A).
Base MAC Address	The MAC address of the switch. This field is fixed.
System Name	The configured system name, if any (see Add a system name on page 96).
Firmware Version	The active main firmware version of the switch (see Update the firmware on page 90).
AV UI Version	The active firmware version for the AV UI. This firmware is included in the main firmware.
Boot Version	The active boot version of the switch. This firmware is included in the main firmware.
System Uptime	The period in days, hours, minutes, and seconds since the switch was last started.
OOB IP Address	The IP address for access to the main UI or AV UI over the out-of-band (OOB) port of the switch (see OOB port IP address on page 99). (This port is also referred to as the service port.)
Management IP Address	The management IP address for access to the main UI or AV UI over any Ethernet network port of the switch (see Management interface IP address on page 97).
STP Network Redundancy	The configured STP network redundancy mode of the switch (see Set the STP network redundancy for the switch on page 103).
Configured Profiles For more information about network profiles, see Network profiles on page 15.	
Profile Name	The name of the network profile.
Profile Type	The profile template on which the network profile is based. The profile template can be any of the preconfigured profile template (

Field or Graph	Description
	for example, Data or Video, see Overview of preconfigured AV profile templates on page 10) or a custom profile template (see Custom AV profile templates on page 28).
VLAN ID	The VLAN ID that is assigned to the network profile.
IP Address	The IP address that is assigned to the network profile.
# of Assigned Ports	The number of ports that are assigned to the network profile.
CPU Utilization	The CPU utilization as a percentage of the CPU capacity.
Memory Utilization	The memory utilization as a percentage of the total memory.
Fans & Temperature	
Fans (numbered)	The number of internal fans depends on the switch model. The state of the fan must be Active. If the state is not Active, there might be a problem with the fan and the cooling.
Sensor (numbered)	The temperature in Celsius that is measured by the sensor. The number of internal sensors depends on the switch model.
Max Temperature	The maximum temperature for normal operation of the switch. **Note**: If the switch exceeds this temperature, the operation of the switch might be limited, for example, PoE might be disabled. The fans are placed in Cool mode. To return the switch to normal operation, you must restart the switch. For more information, see the hardware installation guide.
Fan Mode	The mode can be Off, Quiet, or Cool. For more information, see Manually control the fans on page 106.

Display the neighboring devices

You can display the devices that are connected to the switch.

To display the neighboring devices:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Configure > Neighbor**.
   The Neighbor page displays.
   For each detected device, the page displays the following:
   - **Port**: The port to which the device is attached.
   - **Host**: The system name of the device, if any.
   - **MAC Address**: The MAC address of the device.
   - **VLAN ID**: The VLAN ID of the port to which the device is attached.
   - **IP Address**: The IP address of the device.
   - **Remote Port ID**: The port number of the device.

Diagnostics and Troubleshooting

You can diagnose and troubleshoot the switch and its network.

The chapter contains the following sections:

Manage the switch log, console log, and command log

The switch generates messages in response to events, faults, and errors as well as changes in the configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long-term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

To configure a syslog server and set up remote logging, use the main UI or the CLI. For more information, see the main user manual or the CLI command reference manual, both of which you can download by visiting netgear.com/support/download.

By default, the switch log is enabled at the Notice logging level but the console log and command log are disabled.

To manage the switch log, console log, and command log that are stored locally:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Diagnostics > Logs**.
   The Logs page displays.

5. In the Log Settings section enable or disable logs by doing the following for each individual log:
   - **Enable one or more logs**: Click the **Switch Logging** button, **Console Logging** button, **Command Logging** button, or a combination of these buttons so that they turn green.
   - **Disable one or more logs**: Click the **Switch Logging** button, **Console Logging** button, **Command Logging** button, or a combination of these buttons so that they turn gray.

   By default, the switch log is enabled but the console log and command log are disabled.

6. For the switch log and the console log individually, in the Log Settings section, select the logging level from the **Switch Logging Level** menu or the **Console Logging Level** menu:
   - **Emergency**: Level 0, the system is unusable.
   - **Alert**: Level 1, action must be taken immediately.
   - **Critical**: Level 2, critical conditions.
   - **Error**: Level 3, error conditions. If you enable console logging, this is the default level.
   - **Warning**: Level 4, warning conditions.
   - **Notice**: Level 5, normal but significant conditions. This is the default level for switch logging.
   - **Informational**: Level 6, informational messages.
   - **Debug**: Level 7, debug-level messages.

   NOTE: A log records messages equal to or above the selected severity level. For example, if you select the **Warning** level from the menu, the switch records messages at the Warning, Error, Critical, Alert, and Emergency levels.

7. Click the **Apply** button.
   Your settings are saved.

8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display or download the message log

You can display or download the message log.

To display or download the message log:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Diagnostics > Logs**.
   The Logs page displays. The Logs section shows the recorded log entries.
5. To download the logs, do the following:
   a. Click the **Download Logs** link. A pop-up window displays.
   b. Navigate to a location on your computer and save the file.

Display or clear the port statistics

You can display or clear the port statistics.

To display or clear the port statistics:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.

4. Select **Diagnostics > Port Statistics**.
   The Port Statistics page displays.
   The Inbound Traffic table displays detailed information about the inbound traffic on each port and LAG. The separate Outbound Traffic table displays detailed information about the outbound traffic on each port and LAG.

Table 4.Inbound traffic

Legend	Description
Port	The port or LAG to which the statistics apply.
InOctets	The number of inbound octets (bytes).
InUcastPkts	The number of inbound unicast packets.
InMcastPkts	The number of inbound multicast packets.
InBcastPkts	The number of inbound broadcast packets.
InDropPkts	The number of inbound packets that were dropped.
InBitRate	The bit rate for inbound traffic.
rxError	The number of received packets with errors.

Table 5.Outbound traffic

Legend	Description
Port	The port or LAG to which the statistics apply.
OutOctets	The number of outbound octets (bytes).
OutUcastPkts	The number of outbound unicast packets.
OutMcastPkts	The number of outbound multicast packets.
OutBcastPkts	The number of outbound broadcast packets.
OutDropPkts	The number of outbound packets that were dropped.
OutBitRate	The bit rate for outbound traffic.
txError	The number of transmitted packets with errors.

5. To clear all statistics, click the **Clear all statistics** link above the table.
   A pop-up window displays a warning.
6. Click the **Delete** button.
   The port statistics counters are reset to zero.

Send a ping, traceroute, or DNS lookup request to an IP address or host name

You can you take the following actions independently of each other or simultaneously (or rather, one after the other):

- **Send a ping**: The switch sends a fixed number of ping requests to a particular IP device to determine if it can communicate with the device.
- **Send a traceroute**: The switch attempts to trace the route to a particular IP device to determine the precise path to the device.
- **Send a DNS lookup request**: The switch contacts DNS servers to determine the IP address that is associated with a host name.

When you run one or more tests, the test results are displayed in the panes onscreen.

To send a ping, traceroute, or DNS lookup request to an IP address or host name:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Diagnostics > Troubleshoot**.
   The Troubleshoot page displays.
5. In the **IP Address/Host Name** field, specify the IP address or host name.

6. Do one or more of the following:
   - **Ping**: To ping the IP address or host name, turn on the **Ping** toggle so that it displays green and is positioned to the right.
   - **Traceroute**: To send a traceroute to the IP address or host name, turn on the **Traceroute** toggle so that it displays green and is positioned to the right.
   - **DNS Lookup**: To send a DNS lookup to a host name, turn on the **DNS Lookup** toggle so that it displays green and is positioned to the right.
7. Click the **Run Tests** button.
   The selected tests run one after the other. The results display in the result panes.

Perform a cable test

You can test and display information about the cables that are connected to switch ports.

To perform a cable test:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Diagnostics > Cable Test**.
   The Cable Test page displays.
5. Select the ports for which you want to test the attached cables.

6. Click the **Test Selected Ports** button.
   A cable test is performed on the selected ports. The cable test might take up to 30 seconds to complete. If the port forms an active link with a device, the cable status is Normal. The following table describes the test results that might display in the Cable Test Results section.

Field	Description
Port	The port on which the test was performed
Test Results	**Normal**: The cable is working correctly. **Open**: The cable is disconnected or has a faulty connector. **Short**: An electrical short occurred in the cable. **Cable Test Failed**: The cable status could not be determined. The cable might in fact be working. **Untested**: The cable is not yet tested. **Invalid cable type**: The cable type is unsupported. **No cable**: No cable is detected.
Fault Distance	The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.

Configure port mirroring

Port mirroring lets you select the network traffic of specific switch ports for analysis by a network analyzer. You can select many switch ports as source ports but only a single switch port as the destination port.

A packet that is copied to the destination port is in the same format as the original packet. That means that if the mirror is copying an incoming packet, the copied packet is VLAN-tagged or untagged as it was received on the source port. If the mirror is copying an outgoing packet, the copied packet is VLAN-tagged or untagged as it is being transmitted on the source port.

To configure port mirroring:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Diagnostics > Port Mirroring**.
   The Port Mirroring page displays.
5. Click the **Port Mirroring** toggle so that it displays green and is positioned to the right.
   The page shows two graphical displays of the switch.
6. In the upper graphical display, select one or more source ports.
7. In the lower graphical display, select a single destination port.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Access the CLI through the terminal in the AV UI

You can access the command-line interface (CLI) from the AV UI. While you work in the CLI, the AV UI can remain open.

To access the CLI from the AV UI:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Diagnostics > Terminal**.
   Depending on how you configured your browser, the CLI opens in a new browser tab or browser window.

Download diagnostics files for technical support

NETGEAR technical support might request diagnostic files from your switch. Such files might help troubleshooting a problem. The combined diagnostic files might include the following information:

- Configuration file
- Buffered log
- Tech support file
- Crash logs
- Full memory dump
- Supported MIBs

Please do not send files unless instructed to do so by NETGEAR technical support.

To download the combined diagnostics files in a text file:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login page displays.

   NOTE: The default web browser protocol is HTTPS. Do not use HTTP to access the AV UI.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

   The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ).

   To display the password, click the **eye** icon.

   The Overview page displays.
4. Select **Diagnostics > Support Diagnostics**.
   The Support Diagnostics page displays.
5. Click the **Download Files** link.
   A pop-up window displays.
6. Navigate to a location on your computer and save the text file.