NETGEAR

Audio Video User Manual

AV Line of Fully Managed Switches M4250 Series

March 2021
202-12148-03

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

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/download/.

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

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.

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

Do not use this device outdoors. The PoE source is intended for intra building connection only.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12148-03	March 2021	We added the following chapters: Security on page 43 Diagnostics and Troubleshooting on page 67 We added the following sections to existing chapters: Auto-Trunk overview on page 23 Enable or disable Auto-Trunks on page 24 Auto-LAG overview on page 27 Enable or disable Auto-LAGs on page 28 Configure the hash mode for Auto-LAGs on page 28 Save the running configuration on page 54 Download the running configuration on page 55 Restore the configuration on page 56. Set the STP bridge priority for the switch on page 59 Display the status of the ports and switch on page 63 Display the neighboring devices on page 66 We changed the following sections: Supported Switches on page 7 Use an AV profile template to configure and assign a network profile on page 15 Create a custom AV profile template on page 19 Manage PoE interface settings on page 34 Save the running configuration on page 54
202-12148-02	November 2020	We added the following chapters: Link Aggregation on page 26 Power over Ethernet on page 33 We added a DHCP server option to Use an AV profile template to configure and assign a network profile on page 15.
202-12148-01	September 2020	First publication.

Contents

Chapter 1 Getting Started with the AV UI

Supported Switches....7
Available publications....8
AV local browser UI overview....8
Use a web browser to log in to the AV UI....9
Log in to the AV UI using the switch default IP address....9
Log in to the AV UI with a known IP address....10
Save the running configuration to the startup configuration....10
Register your switch....11

Chapter 2 Audio-Video Profile Templates and Network Profiles

Overview of preconfigured AV profile templates....13
Network profiles....14
Change the default Management VLAN profile....14
Use an AV profile template to configure and assign a network profile....15
Change a network profile....17
Remove a network profile....18
Custom AV profile templates....19
Create a custom AV profile template....19
Change a custom AV profile template....21
Remove a custom AV profile template....22
Auto-Trunk overview....23
Enable or disable Auto-Trunks....24

Chapter 3 Link Aggregation

Auto-LAG overview....27
Enable or disable Auto-LAGs....28
Configure the hash mode for Auto-LAGs....28
Create a LAG....30
Change a LAG....31
Remove a LAG....32

Chapter 4 Power over Ethernet

Manage PoE interface settings....34
Disable PoE for one or more interfaces....37

PoE schedules....38
Create a PoE schedule....38
Change a PoE schedule....41
Remove a PoE schedule....41

Chapter 5 Security

Port authentication....44
Manage port authentication for individual ports....44
Manage 802.1X authentication....45
Remove port authentication from individual ports....46
RADIUS servers....47
Configure the basic settings for a RADIUS server....47
Remove a RADIUS server....48

Chapter 6 Manage and Monitor the Switch

Licenses....51
Add a license online....51
Add a license offline....52
Delete a license....53
Update the firmware....53
Startup configuration....54
Save the running configuration....54
Download the running configuration....55
Restore the configuration....56
Date and time settings....56
Manually set the date and time....57
Configure one or more SNTP servers....57
Add a system name....58
Set the STP bridge priority for the switch....59
Restart the switch from the AV UI....60
Reset the switch to factory default settings....60
Manually control the fans....61
Display the status of the ports and switch....63
Display the neighboring devices....66

Chapter 7 Diagnostics and Troubleshooting

Manage the switch log, console log, and command log....68
Display or download the message log....69
Send a ping, traceroute, or DNS lookup request to an IP address or host name....70
Perform a cable test....71
Configure port mirroring....72
Download diagnostics files for technical support....73

1

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) local browser user interface (UI), in short AV UI.

The chapter contains the following sections:

- Supported Switches
- Available publications
- AV local browser UI overview
- Use a web browser to log in to the AV UI
- Save the running configuration to the startup configuration
- Register your switch

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 release and this AV user manual are for the following M4250 switch models:

- 8-port PoE+ and PoE++ models:
  - **M4250-10G2F-PoE+**: Eight PoE+ (802.3at) 1GBASE-T RJ-45 ports, two 1GBASE-T RJ-45 ports, and two 1G SFP fiber uplink ports. The total PoE budget for the switch is 125W.
  - **M4250-10G2XF-PoE+**: Eight PoE+ (802.3at) 1GBASE-T RJ-45 ports, two 1GBASE-T RJ-45 ports, and two 10G SFP+ fiber uplink ports. The total PoE budget for the switch is 240W.
  - **M4250-10G2XF-PoE++**: Eight PoE++ (802.3bt) 1GBASE-T RJ-45 ports, two 1GBASE-T RJ-45 ports, and two 10G SFP+ fiber uplink ports. The total PoE budget for the switch is 720W.

- 24-port PoE+ and PoE++ models:
  - **M4250-26G4F-PoE+**: 24 PoE+ (802.3at) 1GBASE-T RJ-45 ports, two 1GBASE-T RJ-45 ports, and four 1G SFP fiber uplink ports. The total PoE budget for the switch is 300W.
  - **M4250-26G4XF-PoE+**: 24 PoE+ (802.3at) 1GBASE-T RJ-45 ports, two 1GBASE-T RJ-45 ports, and four 10G SFP+ fiber uplink ports. The total PoE budget for the switch is 480W.
  - **M4250-26G4F-PoE++**: 24 PoE++ (802.3bt) 1GBASE-T RJ-45 ports, two 1GBASE-T RJ-45 ports, and four 10G SFP+ fiber uplink ports. The total PoE budget for the switch is 1440W with both internal power supply units connected.

- 40-port PoE+ and PoE++ models:
  - **M4250-40G8F-PoE+**: 40 PoE+ (802.3at) 1GBASE-T RJ-45 ports and eight 1G SFP fiber uplink ports. The total PoE budget for the switch is 480W.
  - **M4250-40G8XF-PoE+**: 40 PoE+ (802.3at) 1GBASE-T RJ-45 ports and eight 10G SFP+ fiber uplink ports. The total PoE budget for the switch is 960W.
  - **M4250-40G8XF-PoE++**: 40 PoE++ (802.3bt) 1GBASE-T RJ-45 ports and eight 10G SFP+ fiber uplink ports. The total PoE budget for the switch is 2880W with all three internal power supply units connected.

- Special models:
  - **M4250-12M2XF**: LED tiles model with 2.5 Gbps ports. Twelve 2.5GBASE-T RJ-45 ports and two 10G SFP+ fiber uplink ports.
  - **M4250-16XF**: Aggregation model with multiple 10G SFP+ fiber ports. Sixteen 1G/10G SFP+ fiber ports.

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

AV local browser 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 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 local browser 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 local browser 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 audio-video (AV) local browser user interface (UI) to manage and monitor the switch. We abbreviate the audio-video local browser UI as the AV UI.

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 switch default IP address

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

1. Prepare your computer with a static IP address:
   - **Ethernet network port**: For access over an Ethernet network port, use 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.
   - **OOB port**: For access over the OOB port, use a static IP address in the 192.168.0.0 subnet with subnet mask 255.255.0.0.
     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 either an Ethernet network port on the switch or to the OOB port on the switch.
3. Launch a web browser.

4. Enter the default IP address of the switch in the web browser address field:
   - **Ethernet network port**: For access over an Ethernet network port, enter **http://169.254.100.100**.
   - **OOB port**: For access over the OOB port, enter **http://192.168.0.239**.

   The login page displays.
5. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.

Save the running configuration to the startup configuration

After you make changes on a page of the AV UI and click the **Apply** or **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 54.

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.
3. Enter **admin** as the user name, enter your local device password, and click the **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 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:
   https://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.

2

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
- Network profiles
- Custom AV profile templates
- Auto-Trunk overview
- Enable or disable Auto-Trunks

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 could use the same AV profile template to set up three network profiles based on a location within a building: one network profile for the lobby, one for the theater, and one for the patio.

The switch provides the following preconfigured AV profile templates:

- **Audio Dante**: Use this template to connect the switch to Dante audio devices and their controller.
- **Data**: Use this template to connect the switch to streaming ACN (sACN), Art-Net, mobile ad hoc network (MANET), and other network devices as well as to computers.
- **Audio Q-SYS**: Use this template to connect the switch to Q-SYS audio devices and their controller.
- **Video with Q-SYS audio**: Use this template to connect the switch to IP video encoders for transmitting video, IP video decoders for receiving video, and a controller for these devices when Q-SYS audio is supported in the same VLAN. This template can support devices such as Crestron DM NVX systems, AMX SVSI products, Aurora Multimedia products, Atlona products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with AES67 audio**: Use this template to connect the switch to IP video encoders for transmitting video, IP video decoders for receiving video, and a controller for these devices when AES67 audio is supported in the same VLAN. This template can support devices such as Crestron DM NVX systems, AMX SVSI products, Aurora Multimedia products, Atlona products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Audio-over-IP AVB**: Use this template to connect the switch to Audio Video Bridging (AVB) devices.
- **Video**: Use this template to connect the switch to IP video encoders for transmitting video, IP video decoders for receiving video, and a controller for these devices when audio is sent and received from the video nodes using another VLAN ID. This template can support devices such as Crestron DM NVX systems, AMX SVSI products, Aurora Multimedia products, Atlona products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Audio-over-IP AES67**: Use this template to connect the switch to AES67 audio devices and their controller.

- **Video with Dante audio**: IP video encoders for transmitting video, IP video decoders for receiving video, and a controller for these devices when Dante audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, Aurora Multimedia products, Atlona products, Dante video products, and products that comply with standardization by the SDVoE Alliance.

Network profiles

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

Change the default Management VLAN profile

The default network profile is the Management 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 Management 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the Management VLAN, click the **3 dots** icon and select **Edit**.
   The Edit Profile Management VLAN 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. Click the **Save** button.

   Your settings are saved. The window closes. The Network Profiles page displays again.

9. 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 give the profile a name and assign it to a VLAN. You can also assign a specific IP address to the profile and add a color for visual representation.

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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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. In the **Profile Name** field, enter a name for the profile.

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

8. From the **VLAN ID** menu, select the VLAN ID to which the template must apply.
9. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
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. Click the **Enable VLAN Routing / DHCP server** button so that it turns green. 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 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 **Save** 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 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 15.

You cannot change the VLAN ID and AV profile template selection.

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 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 15).

The advantage of a custom AV profile template is that you can decide whether to enable multicast, PTP, and QoS. If you enable QoS, you can specify either a DSCP or CoS configuration.

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?
- Does the template require QoS to be enabled, and if so, in a DSCP or CoS configuration?
  To add one or more QoS configurations, you need knowledge about configuring QoS in a network.

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. For DSCP and CoS, you can configure limited settings in the AV UI. To configure PTP and multicast settings and all DSCP and CoS settings that are available on the switch, 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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, click the **Multicast** button so that it turns green.
   By default, multicast is disabled and the button is gray.
9. To enable PTP, click the **PTP** button so that it turns green.
   By default, PTP is disabled and the button is gray.
10. To add a QoS configuration to the template, do the following:
    a. To the right of the Quality of Service section, click the **Add QoS** link.
    b. The fixed selection from the **QoS Type** menu is **DSCP**, but this setting also includes CoS.
       - In an incoming IP packet, the switch applies QoS according to the information in the DiffServ Code Point (DSCP) field.
       - In an incoming Ethernet frame, the switch applies QoS according to the information in the Class of Service (CoS) field.

       You must select a value from the **Code Point** menu, a value from the **Priority** menu, and a selection from the **Scheduler Type** menu.
    c. From the **Code Point** menu, select a value from **0** to **63**.
       The DSCP value that you select allows an incoming IP packet to be mapped to the egress queue that you select from the **Priority** menu in the following step.
    d. From the **Priority** menu, select the priority value for the egress queue from **0** to number **7**.
       The priority goes from low (0) to high (7). For example, traffic with a priority value of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority, such as 6 or 7, might be time-sensitive traffic, such as voice or video. The priority value for the egress queue applies to either DSCP or CoS.
    e. From the **Scheduler Type** menu, select one of the following types for traffic to which CoS is applied:
       - **Weighted**: The switch uses the weighted round robin (WRR) algorithm to associate a weight with each queue.
       - **Strict**: The switch services traffic with the highest priority on a queue first.

By default, the queue management type is taildrop, irrespective of your selection from the **Scheduler Type** menu. You can change the queue management type to weighted random early detection (WRED) by accessing the main UI.

f. In the Quality of Service section, click the **Save** button.
The QoS configuration is saved.

11. To add another QoS configuration to the template, repeat the previous step.
You can add multiple QoS configurations to a single AV profile template.

12. Click the **Save** 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.

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 19.
You cannot change the name of the AV profile template.

7. To add, change, or delete a QoS configuration in the AV profile template, do one of the following:

   - **Add a QoS configuration**: Do the following:
     a. To the right of the Quality of Service section, click the **Add QoS** link.
     b. Add the QoS configuration.
     For more information about the settings, Create a custom AV profile template on page 19.
     c. In the Quality of Service section, click the **Save** button.
     The QoS configuration is saved.

   - **Change a QoS configuration**: Do the following:
     a. In the Quality of Service section, next to the QoS configuration that you want to change, click the **3 dots** icon, and select **Edit**.
     b. Change the QoS configuration as needed.
     For more information about the settings, Create a custom AV profile template on page 19.
     c. In the Quality of Service section, click the **Save** button.
     The QoS configuration is saved.

   - **Delete a QoS configuration**: Do the following:
     a. In the Quality of Service section, next to the QoS configuration that you want to delete, click the **3 dots** icon, and select **Delete**.
     The QoS configuration is deleted.
     b. In the Quality of Service section, click the **Save** button.
     The QoS configuration is saved.

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

9. 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 remove, click the **3 dots** icon and select **Delete**.
   A confirmation window displays.
6. Click the **Delete** button.
   The AV profile template 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.

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 management VLAN. If you want to change the PVID for an Auto-Trunk, change the management VLAN.

The Auto-Trunk feature functions together with the Auto-LAG feature (see Auto-LAG overview on page 27). 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Configure > Network Profiles**.

The Network Profiles page displays.

5. Below the graphical display of the switch, the one of the following:

   - **Disable Auto-Trunks**: Do the following:
     a. Click the button so that it turns gray.
        A pop-up window displays a warning.
     b. Click the **Yes** button.
        Your settings are saved.

   - **Enable Auto-Trunks**: Click the button so that it turns green.
     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.

3

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:

- Auto-LAG overview
- Enable or disable Auto-LAGs
- Configure the hash mode for Auto-LAGs
- Create a LAG
- Change a LAG
- Remove a LAG

For more information about the LAG options of the switch, see the main user manual, 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 23.

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. (On all M4250 switch models, the Auto-LAG and Auto-Trunk features are enabled by default.)
- 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. (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 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. Below the graphical display of the switch, the one of the following:
   - **Disable Auto-LAGs**: Do the following:
     a. Click the button so that it turns gray.
        A pop-up window displays a warning.
     b. Click the **Yes** button.
        Your settings are saved.
   - **Enable Auto-LAGs**: Click the button so that it turns green.
     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.

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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, which is the Management VLAN profile.

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 from 1 to 8.
10. To create a static LAG instead of a dynamic LAG, click the **Static** button so that it turns green.

    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 **Save** 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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 30.
   You cannot change the LAG ID.
7. Click the **Save** 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

4

Power over Ethernet

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

The chapter contains the following sections:

- Manage PoE interface settings
- Disable PoE for one or more interfaces
- PoE schedules

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.

Manage PoE interface settings

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

Table 1. PoE interface 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. On an 8-port model, port 1 receives the highest PoE priority, while port 8 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.

To manage the PoE interface 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 38), from the **PoE Schedule** menu, you can select a schedule.
    The default is None, so that no schedule applies.
13. Click the **Save** 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.
3. Enter **admin** as the user name, enter your local device password, and click the **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 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.
6. Select the port or ports to for which PoE must be disabled.
7. Click the **Enable PoE** button so that it turns gray.
8. Click the **Save** button.
   Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.
9. 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 interface settings on page 34). 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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, click the **All Day** button so that it turns green, 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, click the **All Day** button so that it turns green., 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, click the **All Day** button so that it turns green., 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 **Save** 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 38.
   You cannot change the name of the PoE schedule.
7. Click the **Save** 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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

5

Security

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

The chapter contains the following sections:

- Port authentication
- Manage port authentication for individual ports
- Manage 802.1X authentication
- Remove port authentication from individual ports
- RADIUS servers
- Configure the basic settings for a RADIUS server
- Remove a RADIUS server

For information about all security options of the switch, see the main user manual, 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 47).

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 45), 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 44) 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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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**: Click the **802.1x Access Authentication** button so that it turns green.

     CAUTION: Before you enable 802.1X access authentication, manually set the port authentication mode of the uplink port or ports to Authorized (see Manage port authentication for individual ports on page 44).

   - **Disable 802.1X access authentication**: Click the **802.1x Access Authentication** button so that it turns gray. 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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 45), you can configure one or more RADIUS servers.

The main UI lets you manage extensive RADIUS settings. For more information, see the main user manual, 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

6

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:

- Licenses
- Update the firmware
- Startup configuration
- Date and time settings
- Add a system name
- Set the STP bridge priority for the switch
- Restart the switch from the AV UI
- Reset the switch to factory default settings
- Manually control the fans
- Display the status of the ports and switch
- Display the neighboring devices

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

Licenses

Full access to the AV UI requires a license.

You can add a license online or offline.

For information about purchasing a license, contact NETGEAR or your local NETGEAR reseller.

After you purchase a license, you receive an email with a license key.

Add a license online

If you received a license key, you can add a license online. Your switch must be connected to the Internet so that your license can be verified and activated by a NETGEAR license server.

To add a license online:

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Configure > AVB License**.
   The AVB License page displays.
5. Click the **Activate New License** link.
   The Activate New License window displays.
   By default, the **Online License Activation** radio button is selected.
6. In the **License Key** field, enter your license.
7. Click the **Save** button.
   The switch contacts the NETGEAR license server.
8. To activate the license, restart the switch by clicking the **Reboot** link in the upper right of the page.
   A pop-up window displays a warning.
9. Click the **Yes** button.

The switch restarts. During the restart process, do not power down the switch.

Add a license offline

You can add a license offline. The license must already be activated by a NETGEAR license server and must be located on the computer that you use to access the AV UI.

To add a license offline:

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Configure > AVB License**.
   The AVB License page displays.
5. Click the **Activate New License** link.
   The Activate New License window displays.
6. Click the **Offline License Activation** radio button.
7. Click in the **Browse** field, navigate to the license, and select it.
8. Click the **Save** button.
   The license is uploaded to the switch.
9. To activate the license, restart the switch by clicking the **Reboot** link in the upper right of the page.
   A pop-up window displays a warning.
10. Click the **Yes** button.
    The switch restarts. During the restart process, do not power down the switch.

Delete a license

You can delete a license that is no longer valid or that you do not need anymore.

To delete a license:

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Configure > AVB License**.
   The AVB License page displays.
5. To the right of the license, click the **trashcan** icon.
   A confirmation window displays
6. Click the **Delete** button.
   The license is deleted.
7. To deactivate the license on the switch, restart the switch by clicking the **Reboot** link in the upper right of the page.
   A pop-up window displays a warning.
8. Click the **Yes** button.
   The switch restarts. During the restart process, do not power down the switch.

Update the firmware

You can update the firmware from a file that you downloaded and that is located on the computer that you use to access the AV UI.

To update the firmware:

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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.

4. 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 lets 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.

5. Click in the **Browse Field** field, navigate to the firmware file, and select it.
6. Click the **Upload** button.

   A pop-up window displays the progress of the firmware file upload.

7. 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** or **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 5 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 55), 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. In the Device Details section, next to 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 **Save** 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 SNTP servers that you want to use. By default, the switch configuration includes one NETGEAR SNTP server, which is time-a.netgear.com.

To update firmware:

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.

4. In the Device Details section, next to the Date & Time field, click the **pencil** icon.
   The Time Configuration window displays.
5. Click the **Enable SNTP** button so that it turns green.
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 **Save** 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. In the Device Details section, next to 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 **Save** 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 bridge priority for the switch

You can set the STP bridge priority for the switch. This 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 BPDUs, the switch with the lowest priority value becomes the root bridge. 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 priority settings in the AV UI align with the priority values in the main UI.

Table 2. STP bridge priority in the AV UI and the main UI

Configurable Setting in the AV UI	Associated Value in the AV UI	Configurable Setting in the Main UI
High	0	0
Medium	32768	Any value from 4096~57344
Low	61440	61440

In the AV UI, you can set the bridge priority to High, Medium, or Low. In the main UI, you must set a specific bridge priority value.

To set the STP bridge priority 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. In the Device Details section, next to the Bridge Priority field, click the **pencil** icon.
   The Edit Bridge Priority window displays.
5. Select the **High**, **Medium**, or **Low** radio button.

By default, the Low radio button is selected.

6. Click the **Save** 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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).

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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 models do not support Off mode.
     - M4250-26G4F-PoE++
     - M4250-40G8XF-PoE+
     - M4250-40G8XF-PoE++
   - **Quiet**: The fans function from 20 or 25 percent (depends on the model) to 100 percent speed. Quiet mode is the default mode. At 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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. 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.
Available	The port is not connected to a device but is available.
1G SFP Fiber Port	The port is a 1G SFP fiber port that can accept an SFP transceiver module.
Authorized	The port authentication mode is Authorized (see Port authentication on page 44).
Connected & Powered	The port is connected to a powered device (PD) that is receiving PoE from the switch.
10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port that can accept an SFP or SFP+ transceiver module.
PoE	The port is a PoE port. Depending on the switch model, the port can provide PoE+ or both PoE+ and PoE++.
Unauthorized	The port authentication mode is Unauthorized (see Port authentication on page 44).
Disabled	The port is disabled.
Blocked	The port is blocked. That is, STP blocked the port to prevent a loop.
PoE Disabled	PoE is disabled on the port (see Disable PoE for one or more interfaces on page 37).

(Continued)

Legend	Description
VLAN Trunk	The port functions as a VLAN trunk. That is, the port is a tagged port that processes tagged VLAN traffic.
Error	An error occurred on the port.
Admin Down	The port is administratively down.
LAG	The port is member of a LAG (see Link Aggregation on page 26).
Auto Trunk	The port functions as an Auto-Trunk (see Auto-Trunk overview on page 23).

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 56).
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 58).
Firmware Version	The active main firmware version of the switch (see Update the firmware on page 53).
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. (This port is also referred to as the service port.)

(Continued)

Field or Graph	Description
Management IP Address	The management IP address for access to the main UI or AV UI over any Ethernet network port of the switch.
Bridge Priority	The configured STP bridge priority of the switch (see Set the STP bridge priority for the switch on page 59).
Configured Profiles For more information about network profiles, see Network profiles on page 14.	
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 (for example, Data or Video, see Overview of preconfigured AV profile templates on page 13) or a custom profile template (see Custom AV profile templates on page 19).
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	
Fan 1 and Fan 2	The state of each fan, which must be Active. If the state is not Active, a problem might be occurring with the fans and the cooling.
Sensor-1 Temperature	The temperature in Celsius that is measured by the first sensor.
Sensor-2 Temperature	The temperature in Celsius that is measured by the second sensor. (The number of internal sensors depends on the model.)

(Continued)

Field or Graph	Description
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 61.

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.
   - **IP Address**. The IP address of the device.

7

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
- Display or download the message log
- Send a ping, traceroute, or DNS lookup request to an IP address or host name
- Perform a cable test
- Configure port mirroring
- Download diagnostics files for technical support

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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, click the **Ping** button so that it turns green.
   - **Traceroute**: To send a traceroute to the IP address or host name, click the **Traceroute** button so that it turns green.
   - **DNS Lookup**: To send a DNS lookup to a host name, click the **DNS Lookup** button so that it turns green.
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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.
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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 Overview page displays.
4. Select **Diagnostics > Port Mirroring**.
   The Port Mirroring page displays.
5. Click the **Port Mirroring** button so that it turns green.
   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.

Download diagnostics files for technical support

NETGEAR technical support might request combined 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:

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.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **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 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.