NETGEAR®
ENGAGE

User Manual

Engage Controller

October 2022
202-12623-01

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/.

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.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12623-01	October 2022	First publication.

Contents

Chapter 6 Manage Network Profiles

Chapter 7 Manage Sites

Chapter 8 Configure an Individual Switch: Audio-Video Profile Templates and Network Profiles

Chapter 9 Configure an individual switch: Link Aggregation

Chapter 15 Configure an individual switch: Diagnostics and Troubleshooting

1

Introduction

The NETGEAR Engage™ Controller provides central management and configuration of M4250 and M4300 switches through a free, audio-video (AV)-friendly, portable app for Windows and MacOS. Automatic switch detection, centralized profile repository, firmware upgrades, and more can now be realized across all NETGEAR switches on your AV network.

In this manual, we refer to the NETGEAR Engage™ Controller as the *controller*.

This user manual is intended for AV network administrators and describes how to install the software and get started quickly.

For a list of NETGEAR M4250 and M4300 switch models with which the controller is compatible, visit kb.netgear.com/000065072.

This chapter includes the following sections:

Note: For more information about the topics that are covered in this manual, visit the support website at netgear.com/support, enter your model number in the search box, and then select your product.

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. Some products can regularly check the site and download new firmware, or 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.

Features

These are some of the main features of the controller:

- Automatically detects all NETGEAR M4250 series and M4300 series switches in the network to which you connect it.
- Lets you centrally trigger a firmware upgrade for all NETGEAR M4250 series and M4300 series switches on the network.
- Lets you use the AV user interface (UI) with port-based profiles to configure each NETGEAR M4250 series and M4300 series switch on your network.
- Collects the AV profiles of all onboarded switches and lets you select which profiles to share among the switches on your AV network.
- Lets you display your AV network layout (topology) for easier configuration across switches.
- Lets you leverage the unique IGMP, Auto-LAG, and Auto-Trunk features for automated interconnection between the NETGEAR M4250 series and M4300 series switches on your network.
- Centrally stores all your sites, credentials, and configurations.
- The controller is a portable application that can reside on a USB thumb drive, so it can be easily moved to any network location. For Windows-based computers, launch the app directly from the USB thumb drive, and save all configuration data to the same USB thumb drive. For MacOS computers, install the controller app on the computer, and then copy the locally saved configuration data back to the USB thumb drive for convenience.

What you can do with the controller

The controller lets you onboard and manage switches. In the first release, we support network profile configuration for the entire site. The controller can display the following components of one or more AV networks:

- **Site**: A network location to which you can onboard and manage switches. When onboarding switches to a site, you can update firmware on all newly added switches at the same time, and automatically collect AV profile templates from onboarded switches that can later be used to set up network profiles on ports and VLANs at the site.
  You can set up sites for different AV networks and manage them all through the controller. For example, if a venue has one large and one small auditorium with different AV requirements, you can set up two sites, one for each auditorium.

- **Site settings**: The AV network profiles that you can use for a site.
  You can set up new network profiles or import existing profiles to assign to switch ports on the switches at your site.
  For example, you might assign the Default network profile on selected switch ports of several switches and a unique network profile that is based on the Dante AV profile template for other switch ports of the same switches.
- **Devices**: NETGEAR M4250 series and M4300 series switches that can be detected, onboarded and assigned to a site, and managed by the controller.
  From the pool of all detected M4250 series and M4300 series switches, you can add switches to sites. For example, if the controller detects eight switches in the entire network that it can reach, you can assign six of them to one site (such as the large auditorium) and keep the other two switches available for another site (such as the small auditorium).
- **Topology**: The network layout of a site.
  For each site, you can display the network layout of the switches, switch ports, and connected devices.

The first time that you log in to the controller, you must go through the Engage Onboarding process, a one-time process that lets you set an admin password for the controller and define a default site with switches and network profiles. For more information, see Set Up the Controller on page 14. Alternately, if you previously saved site settings, you can import existing site settings.

2

Install the Engage Controller Software Application

The controller is a software application for Windows, offered free of charge.

You can install the controller software application on your computer hard drive. For Windows OS, you can also install and run the application from an external drive or USB stick for portability.

This chapter serves as an introduction to the controller and includes the following sections:

- Download and install the controller software application on a Windows-based computer
- Download and install the controller software application on a Mac
- Remove the controller software application

Download and install the controller software application on a Windows-based computer

To download and install the controller software application on a Windows-based computer:

1. Visit https://www.netgear.com/support/product/engage-controller.aspx
   The NETGEAR Engage Controller Support page displays.
2. Download the installation file to a location on your computer.
   An example of the name of the installation file is `Netgear-Engage-x.x.x.x.exe`.

   Note: Before you proceed, you might need to temporarily disable your firewall and anti-virus program, or both. Or you might need to set up an exception in your firewall so that the installer program is not blocked by your firewall. Make sure the application has read, write, and modify permissions at the installation location.

3. Go to the location where you downloaded the installation file and do one of the following:
   - **Standard installation**: Double-click the `.exe` file and follow the prompts of the installer program to install the controller software.
     The default installation location is `C:\Users\`*`your-username`*`\Netgear`. However, you can select another location.
     After installation, the executable file that opens the controller is `Engage.exe`, and an executable icon is placed on your desktop
   - **Custom installation**: Right-click the `.exe` file and select how you want to install the controller.

At the installation location, the data, logs, and site folders contain site-specific and user account information. However, if you later want to export a site configuration directly from the controller, you can select the location where you want to save the site configuration file.

Download and install the controller software application on a Mac

To download and install the controller software application on a Mac:

1. Visit https://www.netgear.com/support/product/engage-controller.aspx
   The NETGEAR Engage Controller Support page displays.
2. Download the installation file to a location on your computer.
   An example of the name of the installation file is `Netgear-Engage-x.x.x.x.dmg`.
3. Double click the **`.dmg`** file.
   The Engage application opens in a new window.
4. Drag and drop the Engage application into the Applications folder.

   Note: After installation, you no longer need the `.dmg` file, and you can delete it.

The Engage application user data is saved at the following path:
`/Users/<login_user_id>/Documents/Engage/`

The user data includes logs and site folders that contain site-specific and user account information.

Remove the controller software application

If you no longer need to the controller software application, you can remove it

Remove the controller software application from a Windows-based computer

To remove the controller software application from a Windows-based computer:

1. Go to the location where you installed the application.
   The default installation location is `C:\Users\`*`your-username`*`\Netgear`.
2. Delete the content of the Netgear folder.
3. Manually delete the desktop icon.
4. If you exported and saved a site configuration file (that is, a file with a `.template` extension), go to the location where you saved the file and manually delete it.

Remove the controller software application from a Mac

To remove the controller software application from a Mac:

1. Locate the application in the Finder by clicking **Applications** in the sidebar of a Finder window.
2. Select the application and then select **File > Move to Trash**.
   You can also drag the application to the Trash.
3. If your Mac requests a user name and password, enter the name and password of an administrator account on your Mac.
   Most likely, this is the user name and password with which you log in to your Mac.
4. To remove the application data, do the following
   a. Select **Users > login_user_id > Documents > Engage**.
   b. Select the **data** folder and then select **File > Move to Trash**.
5. If you exported and saved a site configuration file (that is, a file with a `.template` extension), do the following:
   a. Go to the location where you saved the file.
   b. Select the file, and then select **File > Move to Trash**.
6. Select **Finder > Empty Trash**.

3

Set Up the Controller

Setting up the controller for the first time is a process that includes the following steps:

1. Set a new admin password for the controller.
2. Configure the default site settings, including a site password, name, and description.
3. Select the network interface that the controller must use to discover the switches.
4. Select which discovered switches the controller must onboard to the site.
5. Display or add network profiles that the controller can push to all onboarded switches at the site.

This chapter includes the following sections:

Prepare your AV network for discovery

Before you start the controller onboarding process, consider the following:

- What is the default site name and site password that you want to use?
  The site that you set up during the controller onboarding process is referred to as the default site. Later, you can add more sites and change the default site.
- For each site, how can the computer on which the controller is installed reach the switches? Does the computer receive an IP address from a DHCP server in your network or does the computer require a static IP address?
- The controller can function as a DHCP server for the switches in the network. Is a DHCP server present in the network or does the controller need to function as a DHCP server?
- What is the local device password for each switch that you want to add to the default site? This information is required for each switch so that the controller can onboard and manage the switch.
- Which network profiles do you need for the default site?

Access the controller for the first time and set up the default site

When you access the controller for the first time to set up a site, you must specify the following settings:

- **Password**: The password for future access to the controller.
- **Default site**: A name, description, and password for the default site. (The site that you set up during the controller onboarding process is referred to as the default site.)
- **Network interface**: The interface that lets the controller connect to the default site.
- **Switches**: The switches that the controller discovers at the default site and that you can manage by letting the controller onboard the switches.
- **Network profiles**: The network profiles that are available for the default site. (The network profiles are pulled from the onboarded switches but you can also add a network profile).

Note: For each switch that you want to onboard, you must know the local device password. After the controller onboards the switch, the controller replaces the local device password with the default site password.

CAUTION: The current switch firmware does not support the controller functions. When you let the controller onboard a switch, the controller pushes the latest firmware *with* controller functions to the switch. This firmware update is required: The controller cannot manage the switch without the firmware update.

To access the controller for the first time and set up the default site:

1. On your computer, in the folder in which you installed the controller application, click the **Engage.exe** application icon, or if you created a shortcut, click the **Engage** shortcut.

   The initial login page displays.

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

2. In the **Login Name** field, enter **admin**, and click the **Login** button.

   The Engage Password page displays.

3. In the **New Password** field, set an admin password, repeat the password in the **Confirm Password** field, and click the **Next** button.

   The password must be a minimum of 8 and a maximum of 64 alphanumeric characters and can also contain special characters, except for the quotation mark (“ and ”) and question mark (?) characters. To make the password visible, click the eye icon.

4. Click the **Next** button.

   The Site Setup page display.

5. Keep the **Default Site Configuration** radio button selected (it is selected by default) and set the following information for the default site:

   a. **Site Name**: A name for identification purposes.

   b. **Site Description**: A description for identification purposes.

   c. **New Site Password**: The password must be a minimum of 8 and a maximum of 64 alphanumeric characters and can also contain special characters, except for the quotation mark (“ and ”) and question mark (?) characters. To make the password visible, click the eye icon.
   The controller pushes this password to each switch that it onboards and replaces the switch local device password with the site password.

   d. **Confirm Site Password**: Repeat the password.

6. Click the **Next** button.

   The Network Setup page display.

7. Specify how the computer on which the controller is installed can connect to the AV network at the site by selecting a radio button:

   - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the device (usually a router or WiFi router) that functions as the DHCP server on the network to assign IP addresses to all devices at the site.
   - **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller.
        The Network Setup page shows how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.
   - **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.
        The Network Setup page shows both how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.
     c. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.
     d. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

     Note: We recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

8. Click the **Next** button.
   The Device Setup page displays.
   The Discovered Devices table displays the switches that the controller detects in the network.

9. To let the controller onboard a switch so that it can take control of the switch, click the **Onboard** button for the switch.
   The Add Device window displays for the switch. Specify the following information:
   a. **Device Admin User**: Enter **admin** as the user name for the switch.
   b. **Device Password**: Enter the local device password for the switch.

Note: You are granted five attempts to enter the correct password. After a fifth failed attempt, you are locked out of the switch for five minutes.

The controller also provides the option to enter the switch default password or controller site password:

- **To enter the switch default password**: Turn on the **Use device default password** toggle so that it displays blue and is positioned to the right. For a new switch or a switch that was reset to factory default settings, the switch default password is **password**.
- **To enter the** controller **site password**: Turn on the **Use controller site password** toggle so that it displays blue and is positioned to the right. You defined the controller site password in Step 5.

c. Click the **Apply** button.

Your settings are saved. The switch is moved to the Managed Devices table, and the onboarding process is now in the Pending state.

Note: At the end of this procedure, the controller pushes the site password to the switch (which replaces the switch local device password or switch default password). If any switches do not yet support the controller, the controller pushes a firmware update *with* controller functions to the switch, after which the switch restarts. This process might take up to 10 minutes. The firmware update is required: The controller cannot manage the switches without the firmware update. Only *after* these processes are complete does the switch become a managed device and moves out of the Pending state to the Online state.

CAUTION: During the onboarding process, do not restart the switch or change any cables. Wait until the onboarding process is finished.

10. Repeat the previous step for each switch that you want to let the controller onboard.
11. Click the **Next** button.

    The Profile Setup page displays.

    During the device onboarding process (see Step 9 and Step 10), the controller does the following:

    - Pulls all network profiles that are configured on the switches at the site.
    - Pushes these profiles to all onboarded switches.

12. Review the network profiles that are available for the site, and as an option, set up a new profile.

The page shows the following network profiles:

- The Default network profile, which uses the Data profile template and VLAN 1.
- The network profiles that were pulled from onboarded switches.

To set up a new profile, do the following:

a. Click the **Create Network Profile** link.

b. Set up the network profile. For more information, see Manage Network Profiles on page 35.

13. Click the **Finish** button.

    Your settings are saved. The switches are being onboarded. Because of the firmware update, this process might take up to 10 minutes, after which the page displays Onboarding Finished.

    CAUTION: During the onboarding process, do not restart the switches or change any cables. Wait until the onboarding process is finished.

    Note: If switch settings are incompatible with the network settings, for example, onboarding might fail. If this situation occurs, you can onboard the switch by adding it to the site through the Devices page.

14. Click the **Go to Devices** button.

    The Devices page displays. The page shows the following tables:

    - **Managed Devices**: The table lists all onboarded switches that you can configure using the controller.
    - **Discovered Devices**: The table lists all NETGEAR M4250 series and M4300 series switches that the controller discovered in the network but that the controller did not onboard and that you therefore cannot yet configure using the controller.

Access the controller for the first time and import an existing site

You can use this procedure only if you have used the controller before and exported a site configuration file. Otherwise, see Access the controller for the first time and set up the default site on page 15.

To import a site, you need the site configuration file and password.

To access the controller for the first time and import information for an existing site:

1. On your computer, in the folder in which you installed the controller application, click the **Engage.exe** application icon.
   The initial login page displays.

   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.

2. In the **Login Name** field, enter **admin**, and click the **Login** button.
   The Engage Password page displays.

3. In the **New Password** field, set an admin password, repeat the password in the **Confirm Password** field, and click the **Next** button.
   The password must be a minimum of 8 and a maximum of 64 alphanumeric characters and can also contain special characters, except for the quotation mark (“ and ”) and question mark (?) characters. To make the password visible, click the eye icon.

4. Click the **Next** button.
   The Site Setup page display.

5. Click the **Import Site Configuration** radio button.
   The page adjusts.

6. Click the **Browse** button and navigate to and select the site configuration file that you want to import.

7. In the **Site Configuration Password** field, enter the password for the site configuration file.

8. Click the **Finish** button.
   Your settings are saved. The switches are being onboarded.

   If any switches do not yet support the controller, the controller pushes firmware *with* controller functions to the switches. This firmware update is required: The controller cannot manage the switches without the firmware update. Because of the firmware update, this process might take up to 10 minutes, after which the page displays Onboarding Finished.

   CAUTION: During the onboarding process, do not restart the switches or change any cables. Wait until the onboarding process is finished.

9. Click the **Go to Devices** button.

The Devices page displays. The page shows the following tables:

- **Managed Devices**: The table lists all onboarded switches that you can configure using the controller.
- **Discovered Devices**: The table lists all NETGEAR M4250 series and M4300 series switches that the controller discovered in the network but that the controller did not onboard and that you therefore cannot yet configure using the controller.

4

Manage Devices

The controller lets you centrally configure managed devices or onboard devices from the pool of discovered devices so that you *can* manage and configure them

Note: This chapter describes management options through the controller. For information about configuring *individual* devices, which you can also access through the controller, see Configure an individual device from the controller on page 25.

This chapter includes the following sections:

Add a device to a site

If a device (a switch) does not display in the list of discovered devices at a site, you can manually add the switch as a managed device to the site by specifying the switch IP address and access credentials.

To add a switch to a site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Click the **Add Device** link.
   The Add Device pop-up window displays.
5. To let the controller onboard a switch so that it can take control of the switch, click the **Onboard** button for the switch.
   The Add Device window displays for the switch. Specify the following information:
   a. **Device Admin User**: Enter **admin** as the user name for the switch.
   b. **Device Password**: Enter the local device password for the switch.

      Note: You are granted five attempts to enter the correct password. After a fifth failed attempt, you are locked out of the switch for five minutes.

      The controller also provides the option to enter the switch default password or controller site password:

      - **To enter the switch default password**: Turn on the **Use device default password** toggle so that it displays blue and is positioned to the right.
      - **To enter the** controller **site password**: Turn on the **Use controller site password** toggle so that it displays blue and is positioned to the right. You defined the controller site password in Step 5.

   c. **Device IP Address**: Enter the IP address for the switch.
   d. Click the **Apply** button.

Your settings are saved. The switch is moved to the Managed Devices table, and the onboarding process is now in the Pending state.

Note: At the end of this procedure, the controller pushes the site password to the switch (which replaces the switch local device password or switch default password). If the firmware version on the switch does not support the controller, the controller automatically updates firmware, after which the switch restarts. When these processes are complete, the switch becomes a managed device and moves out of the Pending state to the Online state. This process might take up to 10 minutes.

6. Click the **Add** button.
   Your settings are saved. The switch is added to the Managed Devices table on the Devices page.
7. To save the settings to the running configuration, at the top of the page, click the **Save** button.

Add a system name for a device

After the controller onboards a device, you can use the controller to add a stem name for the device. A system name allows you and others to identify the switch in the network. By default, no system name is configured.

To use the controller to add a system name for a device:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **pencil** icon.
   The **System Name** field becomes accessible.
5. Specify a system name.
6. Click the green check mark.

Your settings are saved.

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

Configure an individual device from the controller

After the controller onboards a device, you can configure the device from the audio-video (AV) user interface (UI).

To configure an individual device from the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Configure the switch.
   The AV UI offers multiple configuration options. For detailed information, see the information in the following chapters:
   - Configure an Individual Switch: Audio-Video Profile Templates and Network Profiles on page 53
   - Configure an individual switch: Link Aggregation on page 73
   - Configure an individual switch: Multicast on page 81
   - Configure an individual switch: Power over Ethernet on page 86
   - Configure an individual switch: Port Configuration on page 98
   - Configure an individual switch: Security on page 105

- Configure an individual switch: Manage and monitor the switch on page 113
- Configure an individual switch: Diagnostics and Troubleshooting on page 138

6. To save the settings to the running configuration, at the top of the page, click the **Save** button.
7. To return to the Devices page of the controller, select **Devices Management**.

Launch the main user interface for a device

After the controller onboards a device, you can launch the device's main user interface (UI) from the controller.

To launch the main UI for an individual device from the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. To save the settings to the running configuration, at the top of the page, click the **Save** button.
5. In the table, for the switch that you want to manage, click the **3 dots** icon and select **Lauch Switch UI**.
   Depending on your browser configuration, the controller launches a web page and display the Login page of the main UI.
   For more information, see the main user manual, which you can download by visiting netgear.com/support/download/.

Launch the command-line interface for a device

After the controller onboards a device, you can launch the device's command-line interface (CLI) from the controller.

This feature is supported for the M4200 series switches. For an M4300 series switch, you can open the CLI by logging in to the switch.

To launch the CLI for an individual device from the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Devices page adjusts.

4. To save the settings to the running configuration, at the top of the page, click the **Save** button.
5. In the table, for the switch that you want to manage, click the **3 dots** icon and select **Launch Terminal**.

   Depending on your browser configuration, the controller launches a web page and display the login page of the CLI.

   For more information, see the CLI command reference manual, which you can download by visiting netgear.com/support/download/.

Manually update the firmware for a device

After the controller onboards a device, you can use the controller to manually update firmware for device.

You can update the firmware from a file that you downloaded and that is, for example, located on the same computer as the controller.

To use the controller to manually update firmware for an individual device:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to manage, click the **3 dots** icon and select **Update Firmware**.
   The Update Firmware pop-up window displays.
5. Select the **Manual** radio button, and click the **Continue** button.
   The pop-up window adjusts and display the current and previous firmware version.
6. Do one of the following:
   - **Load the previous firmware version**: Select the radio button for the previous firmware version.
   - **Select a firmware file that you downloaded:** Click in the **Browse File** field, navigate to the firmware file, and select it.
7. Click the **Upload** button.
   A pop-up window displays the progress of the firmware file upload.
   During the firmware upload, do not power down the device.
8. After the upload completes, in the pop-up window, click the **Restart Now** button.
   The device restarts. During the restart process, do not power down the device.

Restart a device

After the controller onboards a device, you can restart the device from the controller.

To restart an individual device from the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to manage, click the **3 dots** icon and select **Reboot Now**.
   A pop-up window displays a warning.
5. Do one of the following:
   - To save the settings to the running configuration, click the **Yes** button.
   - To restart without saving, click the **No** button.

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

Remove a device from the Managed Devices table

You can remove a device from the controller, which means that the device is removed from the Managed Devices table. The controller might redetect the device and displays it in the Discovered Devices table.

To remove an individual device from the Managed Devices table:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to manage, click the **3 dots** icon and select **Remove**.
   The Delete Devices pop-up window displays.
5. Click the **Delete** button.
   The device is removed from the Managed Devices table.

5

Site Topologies

The controller let you display the topology for a site and manage individual devices from the topology page.

This chapter includes the following sections:

Display the site topology

You can display the topology for a site.

To display the site topology:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Select **Configure > Topology**.
   The Topology page displays.
5. To view detailed information about a device, point to the device.
   A pop-up window displays details:
   - **Managed devices**: The information includes the status, serial number, MAC address, IP address, firmware version, model, and the number of clients.
   - **Clients**: Depending on the information that the controller detects, the information can include the MAC address, IP address, and port number.
6. To view the topology legend, do the following:
   a. At the right of the page, click the blue left arrow icon.
      A pop-up menu displays.
   b. Click the **exclamation mark** icon.
      The Legend pop-up window displays. The legend displays the device types, device status types, and the connection types.
   c. To close the Legend window, at the top of the window, click the **x**.
7. To change the topology view, do the following:
   a. If the pop-up menu does not display, at the right of the page, click the blue left arrow icon.
      A pop-up menu displays.
   b. Click the **topology** icon.

The Topology Views pop-up window displays. By default, the Tree View radio button is selected, and the topology displays as a tree.

c. To display the topology as star, select the **Abstract View** radio button, and click the **Apply** button.
The topology adjusts.

d. To hide clients in the topology, turn off the **Show Clients** toggle so that it displays gray and is positioned at the left, and click the **Apply** button.
The clients are hidden in the topology.
By default, the clients are displayed, and the Show Clients toggle displays blue and is positioned at the right.

e. To close the Topology Views window, at the top of the window, click the **x**.

8. To find a specific device, do the following:
   a. If the pop-up menu does not display, at the right of the page, click the blue left arrow icon.
   A pop-up menu displays.
   b. Click the **hourglass** icon.
   The Search pop-up window displays.
   c. Enter a search term.
   Devices with names that do not match the search are grayed out.
   d. To close the Search window, at the top of the window, click the **x**.

Configure an individual device from the site topology

From the site topology, you can you open the audio-video (AV) user interface (UI) for a managed device. This method lets you make changes across your AV network while an overview of the devices and connections is displayed.

To open the AV UI for a managed device from the site topology:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Select **Configure > Topology**.
   The Topology page displays.
5. Point to the managed device that you want to configure.
   A pop-up window displays details.
6. Click the **Configure** button.
   The Overview page displays.
7. Configure the switch.
   The AV UI offers multiple configuration options. For detailed information, see the information in the following chapters:
   - Configure an Individual Switch: Audio-Video Profile Templates and Network Profiles on page 53
   - Configure an individual switch: Link Aggregation on page 73
   - Configure an individual switch: Multicast on page 81
   - Configure an individual switch: Power over Ethernet on page 86
   - Configure an individual switch: Port Configuration on page 98
   - Configure an individual switch: Security on page 105
   - Configure an individual switch: Manage and monitor the switch on page 113
   - Configure an individual switch: Diagnostics and Troubleshooting on page 138
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Topology page of the controller, select **Topology**.

6

Manage Network Profiles

The controller and onboarded switches provide preconfigured audio-video (AV) profile templates that you can configure and assign to switch ports and VLANs at a site, thereby creating network profiles. As an advanced option, 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.

During the device onboarding process (see Set Up the Controller on page 14), the controller does the following:

- Pulls all network profiles that are configured on the switches at a site.
- Pushes these profiles to all onboarded switches at the site.

This chapter includes the following sections:

Note: For more information about creating and assigning network profiles, see the NETGEAR Engage™ Controller User Manual, which you can download by visiting netgear.com/support/download/.

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 controller provides the following preconfigured AV profile templates:

- **Audio AES67**: Use this template to connect the switch to AES67 audio IP devices and their controller.
- **Audio Video AVB**: Use this template to connect an M4250 series switch to IP audio devices that support Audio Video Bridging (AVB).
  AVB is not supported on M4300 series switches.
- **Audio Dante**: Use this template to connect the switch to Dante audio devices and their controller.
- **Audio Q-SYS**: Use this template to connect the switch to IP audio Q-SYS 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.
- **Lighting**: Use this template to connect the switch to streaming ACN (sACN), Art-Net, and MANET lighting devices.
- **Shure Converged Audio and Control Network**: Use this template to connect the switch to Shure devices requiring audio and control traffic on a single VLAN. Compatible with Dante, AES67, QSYS, and Biamp Dante devices.
- **Shure Split Audio and Control Network**: Use this template to connect the switch to Shure devices requiring separation of audio and control traffic into different VLANs. Compatible with Dante, AES67, QSYS, and Biamp Dante devices.
- **Video**: Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.

- **Video NDI4**: Use this template to connect the switch to video devices and cameras that support Network Device Interface (NDI) version 4 with multi-TCP (mTCP) transport.
- **Video NDI5 with Dante, Q-Sys or AES67 audio**: Use this template to connect the switch to video devices and cameras that support NDI version 5 with Reliable User Datagram Protocol (RUDP). Audio Dante, Q-SYS, or AES67 is supported at the same time in the same VLAN.
- **Video with AES67 audio**: Use this template to connect the switch to IP video devices and their controllers when AES67 audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with Dante audio**: Use this template to connect the switch to IP video devices and their controllers when Dante audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with Q-SYS audio**: Use this template to connect the switch to IP video devices and their controllers when Q-SYS audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.

Add a network profile by using an AV profile template

When you configure a network profile, you must select an AV profile template (see Overview of preconfigured AV profile templates on page 36) that you base the network profile on, give the profile a name, and assign it to a VLAN. You can also assign a color for visual representation.

After you add the network profile to a site, the profile is available for all switches that are onboarded for that site.

To add a network profile by using an AV profile template :

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Select **Configure > Site Settings**.
   The Network Profiles page displays.
5. Click the **Create New Profile** link.
   The Configure New Profile pop-up window displays.
6. From the **Profile Templates** menu, select an AV profile template.
7. To use the network profile as the default VLAN profile for the site, turn on the **Use As Default VLAN Profile** toggle so that it displays green and is positioned to the right.
8. Click the Next button.
   The pop-up window adjusts.
9. In the **Profile Name** field, enter a name for identification purposes.

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

10. In the **VLAN ID** field, enter the VLAN ID to which the template must apply.
11. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
12. Click the **Apply** button.
    Your settings are saved. The profile is added to the table on the Network Profiles page.
13. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Edit the default network profile

You can change the AV profile template and color for the *default* network profile. The following rules apply:

- The default VLAN profile (VLAN 1) cannot be changed during device onboarding.
- If the controller detects multiple default profiles during onboarding, it assigns a Hybrid profile template.
- If you edit the default network profile using the following procedure, all onboarded devices are updated with the new default profile settings.

For information about editing a profile that is not the default profile, see Edit a non-default network profile on page 40.

To edit the default network profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Select **Configure > Site Settings**.
   The Network Profiles page displays.
5. In the table, for the default profile, click the **3 dots** icon and select **Edit**.
   The Edit Network Profile pop-up window displays.
6. Change the following information as needed:
   a. **Profile Template**: From the **Profile Templates** menu, select another AV profile template.
   b. **Color**: Click the box in the **Color** field, and select a color.

   Note: You cannot change the name (which is Default) and you cannot change the VLAN ID (which is 1).
7. Click the **Apply** button.

Your settings are saved. The altered profile displays in the table on the Network Profile page.

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

Edit a non-default network profile

You can change the profile name and color for a network profile that is *not* the default profile. For information about editing the default profile, see Edit the default network profile on page 39.

To edit a network profile that is not the default profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Select **Configure > Site Settings**.
   The Network Profiles page displays.
5. In the table, for the profile that you want to edit, click the **3 dots** icon and select **Edit**.
   The Edit Network Profile pop-up window displays.
6. Change the following information as needed:
   a. **Profile Name**: A name for identification purposes.
   b. **Color**: Click the box in the **Color** field, and select a color.

   Note: You cannot change the selection from the **Profile Template** menu, and you cannot change the VLAN ID.

7. Click the **Apply** button.
   Your settings are saved. The altered profile displays in the table on the Network Profile page.

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

Delete a network profile

You can delete a network profile to remove it from all switches on the site. You cannot delete the default network profile.

To delete a network profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. Select **Configure > Site Settings**.
   The Network Profiles page displays.
5. In the table, for the network profile that you want to delete, click the **3 dots** icon and select **Delete**.
   The Delete Configured Profile pop-up window displays.
6. Click the **Delete** button.
   The profile is deleted and no longer displays in the table on the Network Profiles page.
7. To save the settings to the running configuration, at the top of the page, click the **Save** button.

7

Manage Sites

The controller lets you create, import, change, and remove sites.

This chapter includes the following sections:

Add a site

A site represents a physical location and is defined by a name, description, password, and network IP address. After you add a site, you can associate multiple devices and network profiles with the site.

You can add multiple sites to the controller.

To add a site to the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.
4. Click the **Create New Site** link.
   The Create New Site pop-up window displays.
5. Set the following information for the site:
   a. **Site Name**: A name for identification purposes.
   b. **Site Description**: A description for identification purposes.
   c. **New Site Password**: The password must be eight characters or more.
      The password must be a minimum of 8 and a maximum of 16 alphanumeric characters and *cannot* contain any special characters. To make the password visible, click the eye icon.
      The controller pushes this password to each switch that it onboards at the site and replaces the switch local device password with the site password.
   d. **Confirm Site Password**: Repeat the password.
6. Click the **Next** button.
   The windows adjusts and the Network Setup settings display.

7. Specify how the computer on which the controller is installed can connect to the AV network at the site by selecting a radio button:

   - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the device (usually a router or WiFi router) that functions as the DHCP server on the network to assign IP addresses to all devices at the site.
   - **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller. The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.
   - **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.
     The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.
     c. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.
     d. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

     Note: We recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

8. Click the **Apply** button.
   Your settings are saved. The site is added to the table on the Manage Site Configurations page.

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

Import an existing site

You can use this procedure only if you have exported a site configuration file. Otherwise, see Add a site on page 43.

To import a site, you need the site configuration file and must know the site password.

To import information fort an existing site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.
4. Click the **Import Site** link.
   The Import Site pop-up window displays.
5. Click the **Browse** button and navigate to and select the site configuration file that you want to import.
6. In the **Site Configuration Password** field, enter the password that you defined when you exported the site, and confirm the password in the **Confirm Site Configuration Password** field.
   The site configuration password is not the same as the site password (although it *could* be). When you exported the site (see Export the site configuration on page 50), you defined the site configuration password.
7. Click the **Upload** button.
   Your settings are saved. The site is added to the table on the Manage Site Configurations page.
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.

Change the password for a site

You can change the password for a site. The controller pushes this password to each switch at the site and replaces the old site password with the new site password.

To change the password for a site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.
4. In the table, for the site for which you want to change the password, click the **3 dots** icon and select **Change Password**.
   The Change Site Password pop-up window displays.
5. Change the password information for the site:
   a. **Old Site Password**: Enter the existing site password.
   b. **New Site Password**: Enter the new password, which must be eight characters or more.
      The password must be a minimum of 8 and a maximum of 64 alphanumeric characters and can also contain special characters, except for the quotation mark (“ and ”) and question mark (?) characters. To make the password visible, click the eye icon.
      The controller pushes this password to each switch that it onboards at the site and replaces the switch local device password with the site password.
   c. **Confirm Site Password**: Repeat the password.
6. Click the **Apply** button.
   Your settings are saved. The controller pushes the password to each switch at the site.
7. To save the settings to the running configuration, at the top of the page, click the **Save** button.

Edit a site

You can change the name, description, or network setup of a site:

To edit a site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.
4. In the table, for the site that you want to edit, click the **3 dots** icon and select **Edit**.
   The Edit Site pop-up window displays.
5. Change the following information as needed:
   a. **Site Name**: A name for identification purposes.
   b. **Site Description**: A description for identification purposes.
6. Click the **Next** button.
   The windows adjusts and the Network Setup settings display.
7. Change how the computer on which the controller is installed can connect to the AV network at the site by selecting a radio button:
   - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the device (usually a router or WiFi router) that functions as the DHCP server on the network to assign IP addresses to all devices at the site.
   - **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller. The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.

- **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:
  a. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.
  The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.
  b. From the **Engage Network Interface** menu, select the static IP address.
  c. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.
  d. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

  Note: We recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

8. Click the **Apply** button.
   Your settings are saved. The altered site displays in the table on the Manage Site Configurations page.
9. To save the settings to the running configuration, at the top of the page, click the **Save** button.

Edit the network setup of a site

You can change the network setup of a site:

To edit the network setup of a site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.

4. In the table, for the site that you want to edit, click the **3 dots** icon and select **Network Setup**.

   The Edit Site pop-up window displays. The window displays the Network Setup settings.

5. Change how the computer on which the controller is installed can connect to the AV network at the site by selecting a radio button:

   - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the device (usually a router or WiFi router) that functions as the DHCP server on the network to assign IP addresses to all devices at the site.
   - **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller. The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.
   - **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.
     The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.
     b. From the **Engage Network Interface** menu, select the static IP address.
     c. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.
     d. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

     Note: We recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

6. Click the **Apply** button.

   Your settings are saved. The altered site displays in the table on the Manage Site Configurations page.

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

Export the site configuration

You can change export the site configuration. This allows you to later import the site configuration.

To export the site configuration:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.

3. Select **Controller Management**.
   The Manage Site Configurations page displays.

4. In the table, for the site for which you want to export the site configuration, click the **3 dots** icon and select **Export**.
   The Export Site Configuration pop-up window displays.

5. Enter a site configuration password and repeat the site configuration password.
   The site configuration password is not the same as the site password, although you could use the same password. For the site configuration password, you can set a unique password that protects the security of the switches, configurations and site (and switches) password.

   Note: If you later want to import this site into the controller (see Import an existing site on page 45), you must enter the site configuration password that you define in this step.

6. Click the **Apply** button.
   Your settings are saved. The altered site displays in the table on the Manage Site Configurations page.

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

Change the default site

You change the default site and make another site the default site. Any devices that the controller discovers but that you do not assign to a specific site remain in the pool of discovered devices at the default site.

To change the default site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.
4. In the table, for the site that you want to make the default site, click the **3 dots** icon and select **Set as Default Site**.
   The site that you select is now the default site.
5. To save the settings to the running configuration, at the top of the page, click the **Save** button.

Delete a site

You can delete a site that you no longer need. After you delete a site, any switches that were assigned to the site are returned to the pool of discovered devices. You can then onboard the switches to a new site.

- You cannot delete a site you are currently viewing.
- You cannot delete the default site, but you can make another site the default site (see Change the default site on page 51), and then delete the old default site.

To delete a site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. Select **Controller Management**.
   The Manage Site Configurations page displays.
4. In the table, for the site that you want to delete, click the **3 dots** icon and select **Delete**.
   The Delete Configured Site pop-up window displays.
5. Click the **Delete** button.
   The site is deleted and no longer displays in the table on the Manage Site Configurations page.
6. To save the settings to the running configuration, at the top of the page, click the **Save** button.

8

Configure an Individual Switch: Audio-Video Profile Templates and Network Profiles

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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

You can also set up your own AV profile templates.

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

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

The chapter contains the following sections:

Overview of preconfigured AV profile templates

An AV profile template integrates NETGEAR proprietary settings, allowing you to optimize specific audio and video environments. You can use an AV profile template to create one or multiple network profiles. For example, you 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 controller provides the following preconfigured AV profile templates:

- **Audio AES67**: Use this template to connect the switch to AES67 audio IP devices and their controller.
- **Audio Video AVB**: Use this template to connect an M4250 series switch to IP audio devices that support Audio Video Bridging (AVB).
  AVB is not supported on M4300 series switches.
- **Audio Dante**: Use this template to connect the switch to Dante audio devices and their controller.
- **Audio Q-SYS**: Use this template to connect the switch to IP audio Q-SYS 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.
- **Lighting**: Use this template to connect the switch to streaming ACN (sACN), Art-Net, and MANET lighting devices.
- **Shure Converged Audio and Control Network**: Use this template to connect the switch to Shure devices requiring audio and control traffic on a single VLAN. Compatible with Dante, AES67, QSYS, and Biamp Dante devices.
- **Shure Split Audio and Control Network**: Use this template to connect the switch to Shure devices requiring separation of audio and control traffic into different VLANs. Compatible with Dante, AES67, QSYS, and Biamp Dante devices.
- **Video**: Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.

- **Video NDI4**: Use this template to connect the switch to video devices and cameras that support Network Device Interface (NDI) version 4 with multi-TCP (mTCP) transport.
- **Video NDI5 with Dante, Q-Sys or AES67 audio**: Use this template to connect the switch to video devices and cameras that support NDI version 5 with Reliable User Datagram Protocol (RUDP). Audio Dante, Q-SYS, or AES67 is supported at the same time in the same VLAN.
- **Video with AES67 audio**: Use this template to connect the switch to IP video devices and their controllers when AES67 audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with Dante audio**: Use this template to connect the switch to IP video devices and their controllers when Dante audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with Q-SYS audio**: Use this template to connect the switch to IP video devices and their controllers when Q-SYS audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.

About audio video bridging

802.1AS timing and synchronization is an audio video bridging (AVB) feature. AVB (also referred to as 802.1AS) requires a license. For information about purchasing a license, contact NETGEAR or your local NETGEAR reseller.

AVB is supported on M4250 series switches but not on M4300 series switches.

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

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

Note: Another PTP feature that the switch supports, *PTP residency time stamping*, is incompatible with 802.1AS on the same switch. For more information, see About PTP residency time stamping on page 56. If you must support both AVB and PTP residency time stamping in your network, we recommend that you use two separate switches.

About PTP residency time stamping

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

The switch supports a PTP end-to-end transparent clock that is used in the *PTP residency time stamping* feature, which, by default, is enabled globally on the switch. You can configure PTP residency time stamping globally only (see Configure PTP residency time stamping on page 70).

Note: Another feature that the M4250 series switches support, 802.1AS (audio video bridging, or AVB), is incompatible with PTP residency time stamping on the same switch. AVB is not supported on M4300 series switches. For more information, see About audio video bridging on page 55 and the information below. If you must support both PTP residency time stamping and AVB in your network, we recommend that you use two separate switches.

Note how PTP residency time stamping and AVB function on the switch:

- **Mutual exclusion between PTP residency time stamping and AVB**: If you add a network profile that is incompatible with PTP residency time stamping, such as Audio AVB, PTP residency time stamping is globally disabled.
- **AVB takes precedence over PTP residency time stamping**:
  - If you add a network profile that uses AVB (such as Audio AVB), you cannot manually enable PTP residency time stamping.
  - If PTP residency time stamping is enabled for a network profile (such as the Audio Dante profile) on one port and then you enable a network profile that uses AVB (such as Audio AVB) on another port, PTP residency time stamping is automatically disabled.

- **PTP residency time stamping can be automatically reenabled**: By default, PTP residency time stamping is globally enabled but you can disable it globally. If you disable it and no network profile is using AVB, and then you add a network profile that *can* use PTP residency time stamping (such as Audio Dante), PTP residency time stamping is automatically and globally reenabled.
- **PTP residency time stamping is not a strict requirement**: Whether you need to use PTP residency time stamping depends on your network setup rather than the network profile that you use. Therefore, PTP residency time stamping is not a strict requirement for the network profiles that *can* use it, so you can manually disable PTP residency time stamping (see Configure PTP residency time stamping on page 70). This flexibility lets you, for example, use Audio AVB with Audio Dante on the same switch.

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.

Note: If you add or change a network profile on a switch that is managed by the controller, the new or changed network profile does not synchronize with the controller. The new or changed network profile is specific to the individual switch. However, if you remove the switch from the controller, let the controller rediscover the switch, and then onboard the switch again, all network profiles on the switch are synchronized with the controller, including the new or changed network profile.

Change the Default VLAN profile

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

To change the Default VLAN profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. In the Configured Profiles table, to the right of the Default VLAN, click the **3 dots** icon and select **Edit**.
   The Edit Profile Default window displays.
7. 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.

8. To change the AV profile template, from the **Profile Template** menu, select another template.
   The default AV profile template is the Data template.
9. To change the color for the Default VLAN for visual representation, click the box in the **Color** field, and select a color.
10. Click the **Apply** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.
11. To save the settings to the running configuration, at the top of the page, click the **Save** button.
12. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. 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.
7. 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.

8. In the **Profile Name** field, enter a name for the profile.

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

9. From the **VLAN ID** menu, select the VLAN ID to which the template must apply.
10. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
11. To assign a specific IP address to the network profile, and as an option, use the network profile as a DHCP server, do the following:
    a. Turn on the **Edit VLAN Routing / DHCP Server** toggle so that it displays green and is positioned to the right.
    The IP address menu and fields become available.
    b. From the **VLAN IP Settings** menu, select **Static** or **DHCP client**.
    By default, None is selected. If you select **Static**, you must specify the IP address settings manually and you can also configure the network profile as a DHCP server. (See the following step.)
    If you select **DHCP client**, the network profile functions as a DHCP client and a DHCP server in your network assigns an IP address to the network profile.
    c. If you select **Static** from the **VLAN IP Settings** menu, specify the IP address and subnet mask in the **VLAN IP Address** and **Subnet Mask** fields.
    d. To set up the network profile as a DHCP server, from the **DHCP Server** menu, select **DHCP Server**, and specify the following settings:
       - **Default Router**: The IP address of the router for the DHCP pool. By default, this IP address is the same address as the VLAN IP address, but you can change it.
       - **DHCP Server Pool Start**. The start IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DHCP Server Pool End**. The end IP address of the DHCP server pool. By default, this IP address is derived from the VLAN IP address and subnet mask, but you can change it.
       - **DNS Server 1**: The IP address of the primary DNS server.
       - **DNS Server 2**: As an option, the IP address of the secondary DNS server.
       - **Search Domain**: The domain name for the DHCP server.
       This name is a fully qualified domain name (FQDN).
       - **Lease Time**: The lease time of the IP addresses that the DHCP server assigns. The default is 240 minutes.

12. Click the **Apply** button.

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

13. To save the settings to the running configuration, at the top of the page, click the **Save** button.
14. To return to the Devices page of the controller, select **Devices Management**.

Change a network profile

You can change an existing network profile.

To change a network profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Devices page adjusts.

4. In the table, for the switch that you want to configure, click the **Configure** button.

   The Overview page displays.

5. Select **Network Profiles**.

   The Network Profiles page displays.

6. 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.

7. 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 59.

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

8. Click the **Apply** 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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

Remove a network profile

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

To remove a network profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. 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.
7. Click the **Delete** button.
   The network profile is removed. 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** button.
9. To return to the Devices page of the controller, select **Devices Management**.

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 59).

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.

The Overview page displays.

5. Select **Network Profiles**.
   The Network Profiles page displays.
6. At the top right of the Profile Templates table, click the **Create AV Template** link.
   The Create AV Profiles window displays.
7. In the **Profile Type** field, enter a name for the type of service that the template can provide.
8. In the **Profile Description** field, enter a description for the template.
9. To enable multicast, turn on the **Multicast** toggle so that it displays green and is positioned to the right.
   By default, multicast is disabled and the toggle displays gray and is positioned to the left.
10. To enable PTP, turn the **PTP** toggle so that it displays green and is positioned to the right.
    By default, PTP is disabled and the toggle displays gray and is positioned to the left..
11. 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.

12. To add another QoS configuration to the template, repeat the previous step.
You can add multiple QoS configurations to a single AV profile template.
13. Click the **Save** button.
Your settings are saved. The window closes. The Network Profiles page displays again.
14. To save the settings to the running configuration, at the top of the page, click the **Save** button.
15. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.

The Overview page displays.

5. Select **Network Profiles**.
   The Network Profiles page displays.
6. 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.
7. Change the settings as needed.
   For more information about the settings, Create a custom AV profile template on page 63.
   You cannot change the name of the AV profile template.
8. 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 63.
     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 63.
     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.

9. Click the **Save** button.
   Your settings are saved. The window closes. The Network Profiles page displays again.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. 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.
7. Click the **Delete** button.
   The AV profile template is removed. 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** button.
9. To return to the Devices page of the controller, select **Devices Management**.

Auto-Trunk overview

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

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

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

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

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

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

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

The Auto-Trunk feature functions together with the Auto-LAG feature (see Auto-LAG overview on page 74). 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. Below the graphical display of the switch, do one of the following:
   - **Disable Auto-Trunks**: Do the following:
     a. Turn off the toggle so that it displays gray and is positioned to the left.
        A pop-up window displays a warning.
     b. Click the **Yes** button.
        Your settings are saved.
   - **Enable Auto-Trunks**: Turn on the toggle so that it displays green and is positioned to the right.
     Your settings are saved automatically.
7. To save the settings to the running configuration, at the top of the page, click the **Save** button.
8. To return to the Devices page of the controller, select **Devices Management**.

Configure PTP residency time stamping

Depending on the network profile that is enabled, you can disable or enable the PTP residency time stamping manually, which then applies globally.

If a network profile that uses AVB is enabled (for example, a network profile that is based on Audio AVB), PTP residency time stamping is automatically disabled and you cannot manually enable it. AVB is not supported on M4300 series switches.

Note: PTP residency time stamping is not supported on models M4300-24X24F, M4300-48X, and M4300-48XF, and is not supported in a stacking configuration with any M4300 series models.

To globally enable or disable PTP residency time stamping:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. Below the graphical display of the switch, do one of the following:
   - **Disable PTP residency time stamping**: Turn off the toggle so that it displays gray and is positioned to the left.
   - **Enable PTP residency time stamping**: Turn on the toggle so that it displays green and is positioned to the right.
     By default, PTP residency time stamping is enabled.

   Your settings are saved automatically.

7. To save the settings to the running configuration, at the top of the page, click the **Save** button.
8. To return to the Devices page of the controller, select **Devices Management**.

Configure the IGMP querier for a network profile

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

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

To configure the IGMP querier for a network profile:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Network Profiles**.
   The Network Profiles page displays.
6. In the Configured Profiles table, to the right of the network profile that you want to change, click the **3 dots** icon and select **Querier**.
   The Edit default querier profile window displays.

7. Configure the settings for the querier:

   - **Election Participate**: Select to enable or disable the querier election participate mode for the network profile":

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

     Except for the Default network profile, the election participation is disabled by default, and the toggle displays gray and is positioned to the left

   - **Querier VLAN address**: Specify the IP address to be used as the source IP address in periodic IGMP queries that are sent on the VLAN.

   By default, the operational state is QUERIER, indicating that the network profile can function as a querier.

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** button.

10. To return to the Devices page of the controller, select **Devices Management**.

9

Configure an individual switch: Link Aggregation

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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

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

The chapter contains the following sections:

For more information about the LAG options of the switch, see the main user manual, 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 68.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Link Aggregation**.
   The Link Aggregation Group page displays.
6. Below the graphical display of the switch, the one of the following:
   - **Disable Auto-LAGs**: Do the following:
     a. Turn off the toggle so that it displays gray and is positioned to the left
        A pop-up window displays a warning.
     b. Click the **Yes** button.
        Your settings are saved.
   - **Enable Auto-LAGs**: Turn on the toggle so that it displays green and is positioned to the right.
     Your settings are saved automatically. By default, the Auto-LAG feature is enabled.
7. To save the settings to the running configuration, at the top of the page, click the **Save** button.

8. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Link Aggregation**.
   The Link Aggregation Group page displays.
6. 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.

7. To save the settings to the running configuration, at the top of the page, click the **Save** button.
8. To return to the Devices page of the controller, select **Devices Management**.

Create a LAG

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

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

To create a LAG:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Link Aggregation**.
   The Link Aggregation Group page displays.
6. Below the graphical display of the switch, click the **Create LAG** link.

The Create Link Aggregation Group window displays.

7. Select two or more ports that must become members of the LAG by clicking the individual ports.
8. In the **LAG Name** field, specify a name for the LAG.
9. 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.
10. From the **LAG ID** menu, select an ID from 1 to 8.
11. To create a static LAG instead of a dynamic LAG, turn on the **Static** toggle so that it displays green and is positioned to the right.

    When you create a static LAG, the member ports do not transmit LACPDUs, and the LACPDUs that the member ports receive are dropped.
12. Click the **Apply** button.

    Your settings are saved. The window closes. The Link Aggregation Group page displays again.
13. To save the settings to the running configuration, at the top of the page, click the **Save** button.
14. To return to the Devices page of the controller, select **Devices Management**.

Change a LAG

You can change an existing LAG.

To change a LAG:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Link Aggregation**.
   The Link Aggregation Group page displays.
6. 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.
7. Change the settings as needed.
   For more information about the settings, Create a LAG on page 77.
   You cannot change the LAG ID.
8. Click the **Apply** button.
   Your settings are saved. The window closes. The Link Aggregation Group page displays again.
9. To save the settings to the running configuration, at the top of the page, click the **Save** button.
10. To return to the Devices page of the controller, select **Devices Management**.

Remove a LAG

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

To remove a LAG:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Link Aggregation**.
   The Link Aggregation Group page displays.
6. 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.
7. Click the **Delete** button.
   The LAG is removed. 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** button.
9. To return to the Devices page of the controller, select **Devices Management**.

10

Configure an individual switch: Multicast

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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

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

Multicast is best suited for video and audio traffic requiring multicast packet control for optimal operation. Multicast for IPv4 includes support for IGMPv1, IGMPv2, and IGMPv3.

The chapter contains the following sections:

- Configure the multicast mode for one or more ports
- Add or remove blocked multicast address ranges
- Display the multicast groups in your network

Configure the multicast mode for one or more ports

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

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

To configure the multicast mode for one or more ports:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Multicast**.
   The Multicast page 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 Ports** check box.
7. From the **Multicast Mode** menu, select the multicast mode:
   - **Default**: Multicast traffic is allowed on the selected port or ports based on the protocols that the switch detects.
     This is the default mode.
   - **Force Multicast**: Multicast traffic is forced through the selected port or ports.
   - **Block Multicast**: Multicast traffic from the networks that you select (see the next step) is blocked on the selected port or ports.

8. If you select **Block Multicast** from the **Multicast Mode** menu in the previous step, in this step select one or more multicast address ranges to be blocked from the **Multicast Block Addresses** menu:
   - **Individual multicast address ranges**: Click the **Network Ranges** text (*not* the check box) and select one or more check boxes for individual network ranges.
   - **All multicast network ranges**: Select the **Network Ranges** check box.

   The switch does not let traffic from a blocked address pass through.
9. Click the **Apply** button.
   Your settings are saved.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

Add or remove blocked multicast address ranges

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

Note: If you want remove a blocked multicast range from a port, we recommend that you set the multicast mode for the port to default mode rather than remove the blockage for the multicast range. For more information, see Configure the multicast mode for one or more ports on page 82.

To add or remove blocked multicast address ranges:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Multicast**.
   The Multicast page displays.
6. From the **Multicast Block Addresses** menu, select one or more ranges to block or unblock:
   - **Individual multicast address ranges**: Click the **Network Ranges** text (*not* the check box) and select or clear one or more check boxes for individual network ranges.
   - **All multicast network ranges**: Select or clear the **Network Ranges** check box.
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** button.
9. To return to the Devices page of the controller, select **Devices Management**.

Display the multicast groups in your network

The switch automatically detects the multicast groups in your network.

To display the multicast groups in your network:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.

The Overview page displays.

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

Legend	Description
Forwarding Port	The port on which multicast is enabled and on which multicast traffic is forwarded in the network.
Network Profile (VLAN)	The network profile to which the port is assigned (see Change the Default VLAN profile on page 57 or Use an AV profile template to configure and assign a network profile on page 59). By default, the port is assigned to the Data network profile with VLAN 1.
Subscriber Address	The IP address of the network device that is subscribed to receive multicast traffic.
Subscriber MAC Address	The MAC address of the network device that is subscribed to receive multicast traffic.
Multicast Address	The IP address of the device from which the multicast traffic originates.
Multicast MAC Address	The MAC address of the device from which the multicast traffic originates.
Type	The IGMP version that is being used (IGMPv1, IGMPv2, or IGMPv3).

6. To return to the Devices page of the controller, select **Devices Management**.

11

Configure an individual switch: Power over Ethernet

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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
- Display the total PoE consumption for the switch

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 PoE+ or PoE++ interfaces with the capacities and budgets that are described in the following table. (Depending on the model, the M4300 series switches can support PoE+ but not PoE++).

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)
M4300-16X	16 PoE+ (802.3at)	30W	From 199W to 500W, depending on the PSU configuration
M4300-28G-PoE+	24 PoE+ (802.3at)	30W	From 480W to 720W, depending on the PSU configuration
M4300-52G-PoE+	48 PoE+ (802.3at)	30W	From 480W to 1440W, depending on the PSU configuration

Supplied power is prioritized according to the port order, up to the total power budget of the device. For example, 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
6. 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.
7. 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.
8. 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.

9. 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.
10. 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.
11. 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.

12. 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.

13. If you set up one or more PoE schedules (see PoE schedules on page 92), from the **PoE Schedule** menu, you can select a schedule.

    The default is None, so that no schedule applies.

14. Click the **Apply** button.

    Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.

15. To save the settings to the running configuration, at the top of the page, click the **Save** button.
16. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
6. 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.
7. Select the port or ports to for which PoE must be disabled.
8. Turn off the **Enable PoE** toggle so that it displays gray and is positioned to the left.
9. Click the **Apply** button.
   Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

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 87). 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
6. Below the graphical display of the switch, click the **Create Schedule** link.
   The Create New PoE Schedule window displays.
7. 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.
8. In the **Schedule Name** field, enter a name for the schedule.

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

   - **Daily**: The schedule works with daily recurrence. This is the default setting. You must set the start and end dates and the start and end times that apply during each day.
     The period that the schedule is effective is defined by the start and end dates (see the following steps). During this period, the schedule can be active or inactive.
     Do the following:
     a. To specify the schedule start date, select a date from the **Start Date** calendar.
     b. To specify the schedule end date, select a date from the **End Date** calendar.
     c. To let the schedule be active all day, turn on the **All Day** toggle so that it displays green and is positioned to the right, or specify specific times by continuing with the following steps.
     d. To specify the schedule start time, select a time from the **Start Time** menu.
     e. To specify the schedule end time, select a time from **End Time** menu.

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

   - **Monthly**: The schedule works with monthly recurrence. The fields in the window adjust. You must select the day in a month that the schedule becomes active, set

the start and end dates, and set the start and end times that apply during the days that the schedule is effective.
Do the following:

a. Click the **Select one for the recurring schedule** field and select the day in a month that the schedule must become active every month during the period that the schedule is effective.
The period that the schedule is effective is defined by the start and end dates (see the following steps). During this period, the schedule can be active or inactive.

b. To specify the schedule start date, select a date from the **Start Date** calendar.

c. To specify the schedule end date, select a date from the **End Date** calendar.

d. To let the schedule be active all day, turn on the **All Day** toggle so that it displays green and is positioned to the right, or specify specific times by continuing with the following steps.

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

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

10. Click the **Apply** button.
    Your settings are saved. The window closes. The Power over Ethernet (PoE) page displays again.

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

12. To return to the Devices page of the controller, select **Devices Management**.

Change a PoE schedule

You can change an existing PoE schedule.

To change a PoE schedule:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

The Devices page adjusts.

4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
6. 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.
7. Change the settings as needed.
   For more information about the settings, Create a PoE schedule on page 92.
   You cannot change the name of the PoE schedule.
8. Click the **Apply** 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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

Remove a PoE schedule

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

To remove a PoE schedule:

1. Select **Configure > Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
2. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
4. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.

5. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
6. Select **Power over Ethernet**.
   The Power over Ethernet (PoE) page displays.
7. 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.
8. Click the **Delete** button.
   The PoE schedule is removed. 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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

Display the total PoE consumption for the switch

You can display the total PoE power consumption for the switch. The fixed PoE budget for the switch is also displayed.

To display the total PoE power consumption for the switch:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Power over Ethernet**.

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

6. To return to the Devices page of the controller, select **Devices Management**.

12

Configure an individual switch: Port Configuration

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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

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

The chapter contains the following sections:

Administratively enable or disable one or more interfaces

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

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

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Port configuration**.
   The Port Configuration page displays.
6. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
7. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Configure an individual switch: Link Aggregation on page 73), you can also select one or more LAGs.
8. Do one of the following:
   - **Disable the selected interfaces**: Turn off the **Enable Port** toggle so that it displays gray and is positioned to the left.
   - **Enable the selected interfaces**: Turn on the **Enable Port** toggle so that it displays green and is positioned to the right.

9. Click the **Apply** button.
   Your settings are saved.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

Add a description to one or more interfaces

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

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

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Port configuration**.
   The Port Configuration page displays.
6. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
7. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Configure an individual switch: Link Aggregation on page 73), you can also select one or more LAGs.
8. In the **Port Description** field, type a text.
9. Click the **Apply** button.

Your settings are saved. The description displays in the Port Interface Details table.

10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

Set the frame size for one or more interfaces

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

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

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Port configuration**.
   The Port Configuration page displays.
6. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
7. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Configure an individual switch: Link Aggregation on page 73), you can also select one or more LAGs.
8. In the **Frame Size** field, enter a value from **1500** (the minimum) to **9198** (the maximum).
   The default value is 9198.

9. Click the **Apply** button.
   Your settings are saved.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

Configure flow control for one or more interfaces

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

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

To configure flow control for one or more ports or LAGs:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Port configuration**.

The Port Configuration page displays.

6. Click the **Port Interface Settings** link:
   The Interface Settings page displays.

7. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Configure an individual switch: Link Aggregation on page 73), you can also select one or more LAGs.

8. From the **Flow Control** menu, select a setting to configure what happens if the port buffers become full:
   - **disable**: The switch does not send pause frames, and data loss could occur. This is the default setting.
   - **symmetric**: The switch sends pause frames to stop traffic. The switch also honors incoming pause frames by temporarily halting transmission.
   - **asymmetric**: The switch does not send pause frames, and data loss could occur. However, the switch does honor incoming pause frames by temporarily halting transmission.

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

10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

Display detailed information about the physical ports and LAGs

To display detailed information about the physical ports and LAGs:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Port configuration**.
   The Port Configuration page displays.
   The Port Interface Details table displays detailed information about each port and LAG.

Legend	Description
Port Description	The description that you added (see Add a description to one or more interfaces on page 100). If you did not add a description, this field is blank.
Media Type	The media type that the port supports. The media type can be copper for an Ethernet port or fiber for a port that supports an SFP or SFP+ transceiver for a fiber connection.
Physical Status	The port speed and duplex mode.
Frame Size	The frame size (see Set the frame size for one or more interfaces on page 101). If you did not change the frame size, the default frame size is 9198.
Flow Control	The mode of flow control (see Configure flow control for one or more interfaces on page 102) . If you did not configure flow control, it is disabled.
Network Profile	The network profile to which the port is assigned (see Change the Default VLAN profile on page 57 or Use an AV profile template to configure and assign a network profile on page 59). By default, the port is assigned to the Data network profile.

6. To return to the Devices page of the controller, select **Devices Management**.

13

Configure an individual switch: Security

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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

The chapter contains the following sections:

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 109).

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 107), 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

The Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Security**.
   The Security page displays.
6. Select the ports to which you want to assign a port authentication mode.
   To select all ports, select the **Select All Ports** check box.
7. 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.
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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

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 106) to enable the switch to keep its network connection and, if applicable, Internet connection.

To manage 802.1X access authentication:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Security**.
   The Security page displays.
6. In the RADIUS Server Settings section, do one of the following:
   - **Enable 802.1X access authentication**: Turn on the **802.1x Access Authentication** button so that it displays green and is positioned to the right.

     CAUTION: Before you enable 802.1X access authentication, manually set the port authentication mode of the uplink port or ports to Authorized (see Manage port authentication for individual ports on page 106).

   - **Disable 802.1X access authentication**: Turn off the **802.1x Access Authentication** button so that it displays gray and is positioned to the left. This is the default setting.
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** button.
9. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Security**.
   The Security page displays.
6. Select the ports from which you want to remove port authentication.
   To select all ports, select the **Select All Ports** check box.
7. Click the **Remove Port Authentication** button.
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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

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 107), 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Security**.
   The Security page displays.
6. 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**.
7. 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.

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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

Remove a RADIUS server

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

To remove the settings for a RADIUS server:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Security**.
   The Security page displays.
6. 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 .

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** button.
9. To return to the Devices page of the controller, select **Devices Management**.

14

Configure an individual switch: Manage and monitor the switch

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

You can manage the firmware of the switch and set the switch to factory defaults. You can also display the switch logs. For any M4250 switch model, you can activate a new AVB license.

The chapter contains the following sections:

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

Audio video bridging (AVB) is supported on M4250 series switches but not on M4300 series switches. Therefore, licenses do not apply to M4300 series switches.

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.

Audio video bridging (AVB) is supported on M4250 series switches but not on M4300 series switches. Therefore, licenses do not apply to M4300 series switches.

To add a license online:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **AVB License**.
   The AVB License page displays.
6. Click the **Activate New License** link.
   The Activate New License window displays.
   By default, the **Online License Activation** radio button is selected.

7. In the **License Key** field, enter your license.
8. Click the **Apply** button.
   The switch contacts the NETGEAR license server.
9. To activate the license, restart the switch by doing the following:
   a. Select **Devices Management**.
      The Devices page of the controller displays.
   b. In the table, for the switch, click the **3 dots** icon and select **Reboot Now**.
      A Warning pop-up window displays.
   c. 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.

Audio video bridging (AVB) is supported on M4250 series switches but not on M4300 series switches. Therefore, licenses do not apply to M4300 series switches.

To add a license offline:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **AVB License**.
   The AVB License page displays.
6. Click the **Activate New License** link.
   The Activate New License window displays.

7. Click the **Offline License Activation** radio button.
8. Click in the **Browse** field, navigate to the license, and select it.
9. Click the **Apply** button.
   The license is uploaded to the switch.
10. To activate the license, restart the switch by doing the following:
    a. Select **Devices Management**.
       The Devices page of the controller displays.
    b. In the table, for the switch, click the **3 dots** icon and select **Reboot Now**.
       A Warning pop-up window displays.
    c. 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.

Audio video bridging (AVB) is supported on M4250 series switches but not on M4300 series switches. Therefore, licenses do not apply to M4300 series switches.

To delete a license:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **AVB License**.
   The AVB License page displays.
6. To the right of the license, click the **trashcan** icon.
   A confirmation window displays

7. Click the **Delete** button.
   The license is deleted.
8. To deactivate the license on the switch, restart the switch by doing the following:
   a. Select **Devices Management**.
      The Devices page of the controller displays.
   b. In the table, for the switch, click the **3 dots** icon and select **Reboot Now**.
      A Warning pop-up window displays.
   c. 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Maintenance**.
   The Maintenance page displays.
6. Click in the **Browse Field** field, navigate to the firmware file, and select it.
7. Click the **Upload** button.
   A pop-up window displays the progress of the firmware file upload.
8. After the upload completes, in the pop-up window, click the **Reboot Now** button.

The firmware upgrade process starts. During the firmware upgrade, do not power down the switch. The switch reboots and restart with the new firmware version. When the process is complete, you can log in again to the AV UI.

Startup configuration

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

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

Save the running configuration

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

To save the running configuration to the startup configuration:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. At the top of the page, click the **Save** button.
   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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Maintenance**.
   The Maintenance page displays.
6. In the Configuration Management section, click the **Download Configuration** button.
   A pop-up window displays.
7. Navigate to a location on your computer and save the text file.
   The file is saved with a `.cfg` extension.
8. To return to the Devices page of the controller, select **Devices Management**.

Restore the configuration

If you downloaded the configuration to a computer (see Download the running configuration on page 119), you can restore both the running configuration and startup configuration from your saved configuration file.

To restore the configuration:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Maintenance**.
   The Maintenance page displays.
6. In the Configuration Management section, click in the **Browse File** field.
   A pop-up window displays.
7. Navigate to and select the saved configuration file.
   The file has a `.cfg` extension.
8. Click the **Upload** button.
   A pop-up window displays.
9. 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the Date & Time field, click the **pencil** icon.
   The Time Configuration window displays.
6. Click in the **Date** field, and from the pop-up calendar, select a date.
7. Click in the **Time** field, use the menus to select the hour, minutes, seconds, and meridian setting, and click the **OK** button.
8. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
9. To save the settings to the running configuration, at the top of the page, click the **Save** button.
10. To return to the Devices page of the controller, select **Devices Management**.

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 configure one or more SNTP servers:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the Date & Time field, click the **pencil** icon.
   The Time Configuration window displays.
6. Turn on the **Enable SNTP** toggle so that it displays green and is positioned to the right.
7. From the **Time Zone** menu, select the time zone in which the switch operates.
8. 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.
9. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the System Name field, click the **pencil** icon.
   The Edit System Name window displays.
6. In the **New System Name** field, specify a system name.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.

Management interface IP address

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

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

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

Set a fixed IP address for the management interface

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

To set a fixed IP address for the management interface:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the Management IP Address field, click the **pencil** icon.
   The Edit Management IP Address window displays.
6. From the **Management IP Settings** menu, select **DHCP Static** and specify the following settings:
   - **Management IP Address**: The static IP address for the management interface. The default value is 169.254.100.100.
   - **Subnet Mask**: The IP subnet mask for the management interface. This is also referred to as the subnet/network mask and defines the portion of the interface's IP address that is used to identify the attached network.
     The default value is 255.255.0.0.
   - **Default Gateway**: The gateway through which the management interface can be reached.
     The default value is 0.0.0.0.

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

7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.

Enable the DHCP client for the management interface

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

To enable the DHCP client for the management interface:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the Management IP Address field, click the **pencil** icon.
   The Edit Management IP Address window displays.
6. From the **Management IP Settings** menu, select **DHCP Client**.

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

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

8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.

OOB port IP address

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

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

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

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

Set a fixed IP address for the OOB port

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

To set a fixed IP address for the OOB port:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the OOB IP Address field, click the **pencil** icon.

The Edit OOB IP Address window displays.

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

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

7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.

Enable the DHCP client for the OOB port

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

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

To enable the DHCP client for the OOB port:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

The Devices page adjusts.

4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below the OOB IP Address field, click the **pencil** icon.
   The Edit OOB IP Address window displays.
6. From the **OOB IP Settings** menu, select **DHCP Client**.

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

7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.

Set the STP network redundancy for the switch

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

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

The following table shows how the network redundancy settings in the AV UI align with the bridge priority values in the main UI.

Table 2. STP network redundancy in the AV UI and the main UI

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

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

To set the STP network redundancy for the switch:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. In the Device Details section, below to the STP Network Redundancy field, click the **pencil** icon.
   The Edit STP Network Redundancy window displays.
6. Select the **Primary mode**, **Neutral mode**, or **Backup** radio button.
   By default, the Neutral mode radio button is selected.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Maintenance**.
   The Maintenance page displays.
6. 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.
7. 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 and the switch receives an IP address from the DHCP server in the network, the controller can rediscover the switch. If the switch requires a static IP address, you first must set the IP address of the switch before the controller can rediscover the switch.
8. To return to the Devices page of the controller, select **Devices Management**.

Manually control the fans

Note: Depending on the M4250 series model, you can control the fans of M4250 series switches. You cannot control the fans of the M4300 series switches.

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++ M4250 series 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.

5. In the Fans & Temperature section, select one of the following radio buttons.

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

   The fan setting changes immediately. However, depending on the switch model, if the temperature detected by the temperature sensor exceeds its threshold, a PoE budget is exceeded, or a traffic load condition is exceeded, the switch automatically overrides your manual setting.

6. To save the settings to the running configuration, at the top of the page, click the **Save** button.
7. To return to the Devices page of the controller, select **Devices Management**.

Display the status of the ports and switch

To display the status of the ports and switch:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

The Devices page adjusts.

4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.

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

Legend	Description
Connected	The port is connected to a device that is powered up.
Connected & Powered	The port is connected to a powered device (PD) that is receiving PoE from the switch.
Disabled	The port is disabled.
Error	An error occurred on the port.
Available	The port is not connected to a device but is available.
10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port that can accept an SFP or SFP+ transceiver module.
Blocked	The port is blocked. That is, STP blocked the port to prevent a loop.
Admin Down	The port is administratively down.
1G SFP Fiber Port	The port is a 1G SFP fiber port that can accept an 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++.
PoE Disabled	PoE is disabled on the port (see Disable PoE for one or more interfaces on page 91).
LAG	The port is member of a LAG (see Configure an individual switch: Link Aggregation on page 73).
Authorized	The port authentication mode is Authorized (see Port authentication on page 106).
Unauthorized	The port authentication mode is Unauthorized (see Port authentication on page 106).
VLAN Trunk	The port functions as a VLAN trunk. That is, the port is a tagged port that processes tagged VLAN traffic.
Auto Trunk	The port functions as an Auto-Trunk (see Auto-Trunk overview on page 68).

(Continued)

Legend	Description
Force Multicast	This port is configured for forced multicast (see Configure the multicast mode for one or more ports on page 82).
Warning	The port reached 98 percent of its ingress or egress transmit rate.

For more information about the ports, see Display detailed information about the physical ports and LAGs on page 103.

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	The series number of the switch (M4250 or M4300).
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 120).
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 122).
Firmware Version	The active main firmware version of the switch (see Update the firmware on page 117).
AV UI Version	The active firmware version for the AV UI. This firmware is included in the main firmware.
Boot Version	The active boot version of the switch. This firmware is included in the main firmware.
System Uptime	The period in days, hours, minutes, and seconds since the switch was last started.
OOB IP Address	The IP address for access to the main UI or AV UI over the out-of-band (OOB) port of the switch (see OOB port IP address on page 126). (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 (see Management interface IP address on page 123).
STP Network Redundancy	The configured STP network redundancy mode of the switch (see Set the STP network redundancy for the switch on page 128).
Configured Profiles For more information about network profiles, see Network profiles on page 57.	
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 36) or a custom profile template (see Custom AV profile templates on page 63).
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 M4250 Series Switches	
Fans (numbered)	The number of internal fans depends on the switch model. The state of the fan must be Active. If the state is not Active, there might be a problem with the fan and the cooling.
Sensor (numbered)	The temperature in Celsius that is measured by the sensor. The number of internal sensors depends on the switch model.
Max Temperature	The maximum temperature for normal operation of the switch. **Note**: If the switch exceeds this temperature, the operation of the switch might be limited, for example, PoE might be disabled. The fans are placed in Cool mode. To return the switch to normal operation, you must restart the switch. For more information, see the hardware installation guide.

(Continued)

Field or Graph	Description
Fans & Temperature M4300 Series Switches	
Fan (numbered)	The number of internal fans depends on the switch model. The state of the fan must be Active. If the state is not Active, there might be a problem with the fan and the cooling.
MAC (numbered)	The temperature in Celsius that is measured by the the MAC sensor. The maximum is 90°C. The number of MAC sensors depends on the switch model.
System (unnumbered)	The temperature in Celsius that is measured by the the System sensor. The maximum is 90°C.
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.

6. To return to the Devices page of the controller, select **Devices Management**.

Display the neighboring devices

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

To display the neighboring devices:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.

5. Select **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.
   - **Remote Port ID**: The port number of the device.
6. To return to the Devices page of the controller, select **Devices Management**.

15

Configure an individual switch: Diagnostics and Troubleshooting

Note: This chapter describes configuration options for an individual switch. If you make any configuration changes, the changes apply only to the switch that you are accessing from the controller.

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
- Display or clear the port statistics
- Send a ping, traceroute, or DNS lookup request to an IP address or host name
- Perform a cable test
- Configure port mirroring
- Access the CLI through the terminal in the AV UI
- 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Diagnostics > Logs**.
   The Logs page displays.
6. 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.

7. 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.

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** button.
10. To return to the Devices page of the controller, select **Devices Management**.

Display or download the message log

You can display or download the message log.

To display or download the message log:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Diagnostics > Logs**.
   The Logs page displays. The Logs section shows the recorded log entries.
6. 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.
7. To return to the Devices page of the controller, select **Devices Management**.

Display or clear the port statistics

You can display or clear the port statistics.

To display or clear the port statistics:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

The Devices page adjusts.

4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.

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

Table 3. Inbound traffic

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

Table 4. Outbound traffic

Legend	Description
Port	The port or LAG to which the statistics apply.
OutOctets	The number of outbound octets (bytes).
OutUcastPkts	The number of outbound unicast packets.
OutMcastPkts	The number of outbound multicast packets.
OutBcastPkts	The number of outbound broadcast packets.
OutDropPkts	The number of outbound packets that were dropped.

Table 4. Outbound traffic (Continued)

Legend	Description
OutBitRate	The bit rate for outbound traffic.
txError	The number of transmitted packets with errors.

6. To clear all statistics, click the **Clear all statistics** link above the table.
   A pop-up window displays a warning.
7. Click the **Delete** button.
   The port statistics counters are reset to zero.
8. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

The Devices page adjusts.

4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Diagnostics > Troubleshoot**.
   The Troubleshoot page displays.
6. In the **IP Address/Host Name** field, specify the IP address or host name.
7. Do one or more of the following:
   - **Ping**: To ping the IP address or host name, turn on the **Ping** toggle so that it displays green and is positioned to the right.
   - **Traceroute**: To send a traceroute to the IP address or host name, turn on the **Traceroute** toggle so that it displays green and is positioned to the right.
   - **DNS Lookup**: To send a DNS lookup to a host name, turn on the **DNS Lookup** toggle so that it displays green and is positioned to the right.
8. Click the **Run Tests** button.
   The selected tests run one after the other. The results display in the result panes.
9. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.

The Overview page displays.

5. Select **Diagnostics > Cable Test**.
   The Cable Test page displays.
6. Select the ports for which you want to test the attached cables.
7. 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.

8. To return to the Devices page of the controller, select **Devices Management**.

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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Diagnostics > Port Mirroring**.
   The Port Mirroring page displays.
6. Click the **Port Mirroring** toggle so that it displays green and is positioned to the right.
   The page shows two graphical displays of the switch.
7. In the upper graphical display, select one or more source ports.
8. In the lower graphical display, select a single destination port.
9. Click the **Apply** button.
   Your settings are saved.
10. To save the settings to the running configuration, at the top of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

Access the CLI through the terminal in the AV UI

For an M4250 series switch, you can access the command-line interface (CLI) from the AV UI. While you work in the CLI, the AV UI can remain open.

To access the CLI from the AV UI:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Diagnostics > Terminal**.
   Depending on how you configured your browser, the CLI opens in a new browser tab or browser window.

Download diagnostics files for technical support

NETGEAR technical support might request 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. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.
   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.
   The Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.
   The Devices page adjusts.
4. In the table, for the switch that you want to configure, click the **Configure** button.
   The Overview page displays.
5. Select **Diagnostics > Support Diagnostics**.
   The Support Diagnostics page displays.
6. Click the **Download Files** link.
   A pop-up window displays.
7. Navigate to a location on your computer and save the text file.
8. To return to the Devices page of the controller, select **Devices Management**.