NETGEAR ENTERPRISE

User Manual

GB406 NETGEAR Align Controller User Manual

Model: GB406

202-12891-03
November 2026

Support

For product support and to access the latest product firmware, visit netgear.com/support.
You can also visit our NETGEAR Community for helpful advice at community.netgear.com.
For the duration of software and cyber security updates, visit netgear.com/about/eos/.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/enterprise.
(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/enterprise.)
For safety and regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.
See the regulatory compliance document before connecting the power supply.
For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.
Where permitted by law, by using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions and if you do not agree, return the device to your place of purchase within your return period.
This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra-building connection only.

Trademarks

© 2026 NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc.
Any non-NETGEAR trademarks are used for reference purposes only.

Contents

Introduction 1
Features 1
Safety Instructions and Warnings 2

Get Started with the Main UI 5
Available publications and online help 5
Register your product 6
Main UI overview and other management options 6
Access Engage through the controller 7
Main UI buttons and user-defined fields 7
Access the controller for the first time and set up a site 8
Set up the controller with the main UI 8
Set up the management IP address 8
Log in to the controller 9
Change the theme of the user interface 10
Onboard Engage to the controller 10
Set up the Engage site 10
Set up the Engage network connection 11
Set up the global WiFi network 12
Onboard devices during Engage setup 13
Review network profiles and finish onboarding 14

Configure System Information 16
View the controller system information 16
View the device port information 17
View the controller networks 18
View the Engage status of devices on the controller 19
View the status of the controller's services 19
Configure the system administration settings 21
Edit the system name 21
Configure the date and time of the controller 21
Sync the date and time of the controller with your local browser 22
Configure daylight saving time settings 22

Manage Your Apps on the controller 24

Copyright © 2026 NETGEAR

Activate your license 24
Activate the license from Insight Cloud 24
Activate the license from MyNETGEAR 26
Activate the license from the device UI 27
Display the apps on your controller 27
Install a new app on your controller 28
Install an app on your controller offline 28
Uninstall an app from the controller 29
Activate or deactivate an app on your controller 29

Manage Configured Networks 31
Configure networks overview 31
Auto-Trunk overview 32
Auto-LAG overview 33
Edit a network 33

Manage System Settings from the Controller 36
Link aggregation groups 36
Configure a LAG and its membership 37
Port settings 39
Configure and display the port settings 40
Configure port settings for multiple ports 41
Configure port settings for a LAG 42

Manage the Service Settings 44
Manage the DHCP server 44
Enable or disable the DHCP server 44
Display the DHCP server overview 45
Configure the global DHCP settings 46
Manage the DHCP subnets 47
Manage the DHCP templates 50
Manage the DHCP reservations 54
View the DHCP bindings 58
View and manage the DHCP logs 59
Manage the PTP server 59
Enable or disable the PTP server 60
Display the PTP server overview 60
Add a PTP instance 62
Edit a PTP instance 64
Delete a PTP instance 66

Copyright © 2026 NETGEAR

View the PTP status page . . . 67
View the PTP statistics . . . 67
View and manage PTP logs . . . 68
Manage the syslog server . . . 69
Enable or disable the syslog server . . . 69
Display the syslog server overview . . . 69
Configure the syslog server settings . . . 71
View and manage syslog logs . . . 72
Manage the NTP server . . . 73
Enable or disable the NTP server . . . 73
Display the NTP server overview . . . 74
Configure the NTP server settings . . . 75
Manage the DNS server . . . 76
Enable or disable the DNS server . . . 76
Display the DNS server overview . . . 77
Configure the DNS server settings . . . 77
Add a DNS zone . . . 78
Edit a DNS zone . . . 79
Delete a DNS zone . . . 80
Add a resource record . . . 80
Edit a resource record . . . 82
Delete a resource record . . . 83
Manage the HTTPS server . . . 84
Display the HTTPS server overview . . . 84
Configure the HTTPS service settings . . . 84
View and manage HTTPS logs . . . 85
Manage the mDNS server . . . 86
Enable or disable the mDNS server . . . 86
Display the mDNS server overview . . . 87
Configure the mDNS server settings . . . 88
View and manage mDNS logs . . . 89
Manage the LLDP service . . . 90
Enable or disable LLDP server . . . 90
Display the LLDP server overview . . . 90
Configure the LLDP global settings . . . 91
Configure the LLDP port settings . . . 92
View and manage LLDP logs . . . 93

Maintenance . . . 95
LCD display overview . . . 95

Copyright © 2026 NETGEAR

View the LCD display main screen . . . 96
View system information on the LCD display . . . 96
View network usage on the LCD display . . . 97
View notifications on the LCD display . . . 97
Configure the LCD auto-screen display settings . . . 98
Set the date and time on the LCD display . . . 98
Manage certificates on the controller . . . 99
Add a certificate . . . 99
Delete a certificate . . . 100
Download a certificate . . . 100
Re-generate a certificate . . . 101
Manage firmware on the controller . . . 101
Update to an installed firmware version . . . 101
Update the controller firmware from a file . . . 102
Update the controller firmware from an online version . . . 103
Manage the Engage version on your controller . . . 103
Update Engage on your controller . . . 104
Reset Engage to the default state . . . 104
Manage the controller's stored files . . . 104
View the stored file locations on the controller . . . 105
Download stored files . . . 105
Delete stored files . . . 106
Manage the SSD storage . . . 106
View the SSD health and partition information . . . 107
Create a partition on the SSD . . . 107
Format a partition on the SSD . . . 108
Delete a partition from the SSD . . . 108
Manage the configuration file . . . 109
Download the configuration file . . . 109
Restore the configuration file . . . 109
Use the main UI to restart the controller . . . 110
Use the Reset button to restart the controller . . . 110
Return the controller to its factory default settings . . . 110
Use the main UI to reset the controller to the factory default settings . . . 110
Use the Reset button to reset the controller to factory default settings . . . 111

Manage the Controller Security . . . 112
Manage the user accounts . . . 112
Add a user . . . 113
Display and manage the active sessions of all users . . . 114

Copyright © 2026 NETGEAR

Change the password on the controller 114

Diagnostics and Troubleshooting 115
Send a ping, traceroute, or DNS lookup request to an IP address or host name 115
Download diagnostics files for technical support 116
Display the neighboring devices 116
Display the resource manager 118
View the CPU utilization 118
View the memory utilization 118
View the network utilization 119
Manage the controller's notifications 120
Display message notifications 120
Display the notifications 121
Manage the message controller's logs 121

Technical Specifications 125
Access default settings for the controller main UI 125
Network profile features default settings 126
System features default settings 126
Service features default settings 127
General hardware technical specifications 129

Revision History 130

Copyright © 2026 NETGEAR

Introduction

This user manual is for the GB406 NETGEAR Align Controller, referred to as the *controller* throughout this guide. The controller is a half-width network management device designed to simplify the deployment, monitoring, and management of AV-over-IP and enterprise network environments. You can install the controller on a flat surface using rubber footpads or mounted in a rack.

You can access the NETGEAR Engage App and manage the controller entirely through NETGEAR's web browser interface, removing the requirement for a computer. The controller includes an on-device Align AppHub page, which supports the installation of containerized applications.

For more information about installing and using the controller, see the Installation Guide and Hardware Installation Guide, which you can download by visiting netgear.com/support/enterprise.

For a complete description of the features and capabilities of Engage, see the NETGEAR Engage Controller User Manual, which you can download by visiting netgear.com/support/enterprise.

This chapter includes the following sections:

- Features
- Safety Instructions and Warnings

Features

The controller supports the following features:

- Integrated Engage application: The controller runs the NETGEAR Engage network management platform directly on the device, eliminating the need for a dedicated computer or laptop. Any authorized user on the network can access and manage all Engage-manageable devices through a web browser. The Engage app on the controller:
  - Automatically detects all Engage-manageable devices connected to the network.
  - Lets you centrally trigger firmware updates for all managed devices on the network.
  - Lets you configure network profiles and assign them to switch ports and VLANs across all onboarded switches.
- Always-on network management: Using the controller lets Engage run on the controller itself rather than on a computer. Engage is available 24 hours a day, 7 days a week, without requiring any workstation to be switched on.
- Centralized device management: The controller lets you onboard, configure, and manage NETGEAR switches, wireless access points, and routers across your site from a single interface.
- Unified user and password management: The controller and Engage share a common set of user accounts and passwords. Changes made on the controller are automatically

synchronized to Engage.
  - Supports the admin, site-admin, and guest (view-only) roles.
  - A single admin password governs both the controller and the Engage application.
- Built-in network services: The controller runs a suite of background services to support device management and network operation, including DHCP, DNS, NTP, HTTP, Syslog, mDNS, and PTP servers.
- Align AppHub: The controller provides a centralized platform for managing applications installed on the controller.
  - Supports cloud-based installation and manual installation by USB or web upload.
  - Validates all application packages using cryptographic signature verification before installation.
  - Each application runs in an isolated Docker container, preventing interference with other applications or the controller operating system.
- LCD touchscreen display: A 480x128 pixel front-panel touchscreen provides at-a-glance system status, port activity, hardware statistics, and notifications without requiring a browser login.
- Internal SSD: The controller provides local storage for logs accessible through a built-in file manager in the web interface.
- Secure onboarding: A guided first-time setup wizard configures the site name, administrator credentials, IP addressing, DHCP settings, and wireless SSID in a single workflow.
- Support for firmware updates through USB: You can manually apply firmware using a USB drive connected directly to the controller, without requiring internet access.

Safety Instructions and Warnings

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.
To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- This product is not suitable for use in locations where children are likely to be present.
- This product is designed for indoor use only in a temperature-controlled (0–45°C or 32–113°F) and humidity-controlled (90 percent maximum relative humidity, noncondensing) environment. Any device that is located outdoors and connected to this product must be properly grounded and surge protected. To the extent permissible by applicable law, failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty.
- Observe and follow service markings:
  - Do not service any product except as explained in your system documentation.
  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock. We recommend that only a trained technician

services components inside these compartments.

- If any of the following conditions occur, unplug the product from the power outlet and replace the part or contact your trained service provider:
  - The power cable, extension cable, or plug is damaged.
  - An object fell into the product.
  - The product was exposed to water.
  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To avoid damaging your system, be sure that the voltage selection switch (if provided) on the power supply is set to match the power at your location:
  - 115V, 60 Hz in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100V, 50 Hz in eastern Japan and 100V, 60 Hz in western Japan
  - 230V, 50 Hz in most of Europe, the Middle East, and the Far East
- Be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cables. If you were not provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable approved for your country. The power cable must be rated for the product and for the voltage and current marked on the product electrical ratings label. The voltage and current rating of the cable must be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded power outlets.
- The peripheral power cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local and national wiring rules.

Get Started with the Main UI

This chapter provides an overview of how you can access the main user interface (UI), also referred to as the main UI.

NOTE: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/enterprise. 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.

This chapter includes the following sections:

- Available publications and online help
- Register your product
- Main UI overview and other management options
- Main UI buttons and user-defined fields
- Access the controller for the first time and set up a site
- Change the theme of the user interface
- Onboard Engage to the controller

Available publications and online help

You can download the following publications and more for the GB406 Align Controller by visiting netgear.com/support/enterprise.

- Installation Guide
- Hardware Installation Guide
- User Manual (this manual)

When you are logged in to the main UI, you can access documentation online by selecting the **Information** icon at the top of the Dashboard.

- Select **Community** to open the NETGEAR Enterprise Community page.
- Select **Support** to open the NETGEAR Enterprise Support page, where you can access documentation, release notes, and firmware.

In addition, context-sensitive online help is available in the main UI.

Register your product

To qualify for product updates and product warranty, we encourage you to register your product. The first time that you log in to the controller, you can register with NETGEAR by clicking the **REGISTER** button.
Registration confirms that your email alerts work, lowers technical support resolution time, and ensures the accuracy of your shipping address. We would also like to incorporate your feedback into future product development. We never sell or rent your email address and you can opt out of communications.

To register your controller with NETGEAR:

1. Visit the NETGEAR website for registration at https://my.netgear.com/registration/login.aspx.
2. Click the **Login** button, and follow the directions onscreen to register the controller with your NETGEAR email address and password.
   If you did not yet create a NETGEAR account, click the **Create account** link, follow the directions onscreen to create an account, and then register the controller with your NETGEAR email address and password.

Main UI overview and other management options

Your controller contains an embedded web server and management software for managing and monitoring the controller's functions.
The controller software includes a comprehensive set of management functions for configuring and monitoring the system by using one of the following methods:

- **Main user interface (main UI)**: The main UI is a web-based management tool that lets you monitor, configure, and control your controller remotely by using a standard web browser. You can access the main UI over an Ethernet network port connected to a computer or laptop. From your web browser, you can monitor the performance of your controller and optimize its configuration for your network. You can configure all available controller features by using the main UI.
  This manual describes how to use the main UI to manage and monitor the controller.
- **NETGEAR Engage Controller application**: The NETGEAR Engage Controller application lets your controller discover, onboard, manage, and monitor your Engage-compatible devices in an AV network or other type of business network.
  For more information, see the Engage Controller User Manual, which you can download by visiting netgear.com/support/enterprise.

Access Engage through the controller

You can access Engage using the main UI on the GB406 controller.

To access Engage through the main UI of the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Engage**.
   A new browser tab opens connected to Engage.

Main UI buttons and user-defined fields

The following table shows the command buttons that are used on the pages in the main UI:

Table 1.Main UI command buttons

Button	Function
Add	Clicking the **Add** button adds the new item configured in the heading row of a table.
Apply	Clicking the **Apply** button sends the updated configuration to the controller. Configuration changes take effect immediately.
Edit	Clicking the **Edit** button edits an item in the configuration.
Continue	Clicking the **Continue** button sends the updated configuration to the controller. Configuration changes take effect immediately.
Cancel	Clicking the **Cancel** button cancels the configuration on the page and resets the data on the page to the previous values of the controller.
Delete	Clicking the **Delete** button removes the selected item.
Refresh	Clicking the **Refresh** button refreshes the page with the latest information from the device.
Save	Clicking the **Save** button saves your settings. This is located in the upper right corner of the main UI.
Logout	Clicking the **Logout** button ends the session. This is located in the upper right corner of the main UI.

All characters can be used except for the following (unless specifically noted for that feature):

Table 2.Invalid characters for user-defined fields

Invalid characters for user-defined fields						
\	|	/	<	>	*	?

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

Before you log in to the controller, install the controller on either a flat surface or in a rack. For information about setting up the controller, see the Installation Guide and Hardware Installation Guide, which you can download by visiting netgear.com/support/enterprise.

Set up the controller with the main UI

To access the controller main UI, connect the controller to a computer or laptop using an Ethernet cable. Configure the computer with a static IP address of 192.168.1.12 and a subnet mask of 255.255.255.0. Open a web browser on the computer connected to the same network and navigate to **192.168.1.250**. On the very first startup, the Get Started page displays.

To log in to the controller for the first time:

1. Set the following information:
   - **Password**: Enter a password for the admin account. The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @#$%^&*(). To make the password visible, click the eye icon. The controller pushes this password to each device that it onboards and replaces the local device password with the site password.
   - **Confirm Password**: Confirm the password.
   - **Password Hint**: Enter a password hint (optional).
2. Select the checkbox to accept NETGEAR's terms and conditions.
3. Click the **Next** button.
   On the very first startup, the Set Up Management IP page displays, see Set up the management IP address on page 8.

Set up the management IP address

To access the controller on the initial startup, you must set the IP address used by your browser to access the Align Management UI.

1. On the Set Up Management IP page, in the Access IP Address section, select one of the following radio buttons:
   - **Static IP**: Use a static IP address to access the controller. Make sure that this IP subnet does not conflict with your existing network connected to the controller. Enter the following information:
     - **IP Address**: Enter a new IP address. The default address is 192.168.1.250.
     - **Subnet Mask**: Enter a new subnet mask. The default mask is 255.255.255.0.
     - **Gateway**: Optionally, enter a default gateway so that the controller can access the internet.
     - **DNS Server 1**: Optionally, you can enter a DNS server.

     Optionally, you can click the **I would like to set up a DHCP server for this port – the Align Controller will automatically assign an IP address to your PC from the range below** checkbox. Enter the following information:
     - **Start IP Address**: Enter a start IP address. The default address is 192.168.1.100.
     - **End IP Address**: Enter an end IP address. The default address is 192.168.1.200.
     - **Subnet Mask**: The field is automatically set at 255.255.255.0. You cannot change the subnet mask for the IP address range.
     - **Router**: Optionally, you can enter a router.
     - **DNS Server 1**: Optionally, you can enter a DNS server.
   - **DHCP Client**: The IP address, subnet mask, gateway, and DNS server is assigned by the DHCP server after you finish setup. Optionally, you can click the **Use the gateway from the DHCP server as Align Controller's default route** checkbox so that the controller can access the internet.
2. Click the **Finish** button.
   The controller's Dashboard page displays. To complete setting up the controller, see Onboard Engage to the controller on page 10.

Log in to the controller

1. Launch a web browser and enter the controller's IP address into your browser's address bar. The factory default IP address is 192.168.1.250.

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

   The Login page displays.
2. On the Login page, enter the username and password.
3. Click the **Login** button.
   The Dashboard page displays.

Change the theme of the user interface

You can change the theme (style) of the main UI from a light theme with gray toggles to a dark theme with green toggles.

To change the theme of the UI on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. At the top of the page, click the **Theme** icon.
   - **Light theme**: With this theme, which is the default, toggles that are turned on display light gray with a dark gray circle. Toggles that are turned off display light gray with a white toggle circle.
   - **Dark theme**: With this theme, the main UI displays dark and the toggles that are turned on display green with a white toggle circle. Toggles that are turned off display black with a white toggle circle.

   The main UI theme adjusts automatically after you select an option.
   Your settings are saved.

Onboard Engage to the controller

To complete your setup, you must onboard Engage to the controller.

To onboard Engage to your controller:

1. On the Dashboard page, select **Engage**.
   The Engage Onboarding site displays in a new tab.
2. On the Engage Password page, click the **Next** button.
   The Engage admin password is synced with the controller's admin password.
   The Site Setup page displays. Follow the procedure outlined in Set up the Engage site on page 10.

Set up the Engage site

To set up the Engage site on your controller:

1. On the Site Setup page, select one of the following radio buttons:
   - Select **Default Site Configuration** and enter the following details:
     - **Site Name**: A name for identification purposes.
     - **Site Description**: A description for identification purposes.
     - **New Site Admin Password**: The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @#$%^&*(). To make the password visible, click the eye icon. The controller pushes this password to each device that it onboards and replaces the local device password with the site password.
     - **Confirm Site Admin Password**: Confirm the password.
     - **New Site Admin Password Hint**: Enter a password hint (optional). Optionally, select the checkbox to configure a view-only guest user password for the site.
       - **New Site Guest Password**: A password for the guest site.
       - **Confirm Site Guest Password**: Confirm the password.
       - **New Site Guest Password Hint**: Enter a password hint (optional).
   - Select **Import Site Configuration** and do the following:
     a. Click the **Browse** button and import an Engage site configuration in .zip file type format.
     b. Enter a password in the **Site Configuration Password** field.
2. Click the **Next** button.
   The Network Setup page displays. Follow the procedure outlined in Set up the Engage network connection on page 11.

Set up the Engage network connection

To set up your Engage network connection on the Network Setup page:

1. Specify how the computer on which Engage is installed can connect to the AV network at the site by selecting a radio button from the following options:
   - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the computer's network interface so that it can receive a dynamic IP address from a DHCP server (or router that functions as a DHCP server) in the network.
   - **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 Engage. The Network Setup page shows how to assign a static IP address to the computer. You can display these steps for a Windows-based computer and Mac.
     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 Engage 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 a Windows-based computer and Mac.
     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 devices at the site for fastest IP address assignment by the controller's DHCP server.

2. Click the **Next** button.
   The Wireless Setup page displays. Either click the **Skip >>** link to skip this step, or if your network includes access points, follow the procedure outlined in Set up the global WiFi network on page 12.

Set up the global WiFi network

To set up the global WiFi network (SSID) for the default site on the Wireless Setup page:

1. In the **Global SSID** field, enter the name for the WiFi network (SSID).
   Optionally, select the **Use the Controller Site Name** toggle.

2. In the **Password** field, enter the password for access to the WiFi network, which uses WPA-MPSK security.
   Optionally, select the **Use the Controller Site Password** toggle.
3. From the **Region** menu, select the region for the country in which the default site is located. After setup, you cannot change the region.
4. From the **Country** menu, select the country in which the default site is located. After setup, you cannot change the country.
5. Click the **Next** button.
   The Device Setup page displays. Follow the procedure outlined in Onboard devices during Engage setup on page 13.

Onboard devices during Engage setup

The Discovered Devices table displays the devices that the controller detects in the network. You can onboard devices now, or later, after you have set up the controller.

To onboard devices during the Engage setup on the Device Setup page:

1. To let the controller onboard a device so that it can take control of the device, click the **Onboard** button for the device.
   The Add Device window displays for the device.
2. In the **Device Admin User** field, enter **admin** as the user name for the device.
3. In the **Device Password** field, enter the local device password for the device.

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

   The controller also provides the option to enter the device default password or controller site password:
   - **To enter the device default password**: Turn on the **Use device default password** toggle so that it displays blue and is positioned to the right.
     For a new device or a device that was reset to factory default settings, the device default password is **password**.
     Access points must be in factory default state, which means that they are using the device default 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 Set up the Engage site on page 10.

4. Click the **Add** button.
   Your settings are saved. The device is moved to the Managed Devices table, and the onboarding process is now in progress.

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

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

5. Repeat the previous step for each device that you want to let the controller onboard.
6. Click the **Next** button.
   A pop-up Notice page displays.
   During the device onboarding process, the controller does the following:
   - Pulls all network profiles that are configured on the devices at the site.
   - Pushes these profiles to all onboarded devices.
7. Click the **OK** button.
   The Profile Setup page displays. Follow the procedure outlined in Review network profiles and finish onboarding on page 14.

Review network profiles and finish onboarding

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 devices, if any.

To set up a new profile, on the Profile Setup page, do the following:

1. Click the **Add Network Profile** button.
2. Set up the network profile.
   For more information, see Manage Configured Networks on page 31.

3. Click the **Finish** button.

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

Your settings are saved and the devices onboard. Because of the firmware update, this process might take up to 10 minutes, after which the page displays the Onboarding Finished message.

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

Your settings are saved and the controller has successfully onboarded Engage.

4. To continue on the Engage site, click the **Go to Devices** button.
   The Devices page displays. The page shows the following tables:
   - **Managed Devices**: The table lists all onboarded devices that you can configure using the controller.
   - **Discovered Devices**: The table lists all Engage-manageable devices that the controller discovered in the network but that the controller did not onboard and that you therefore cannot yet configure using the controller.

Configure System Information

You can view and configure the controller's system information from the main UI.
This chapter includes the following sections:

- View the controller system information
- View the device port information
- View the controller networks
- View the Engage status of devices on the controller
- View the status of the controller's services
- Configure the system administration settings

View the controller system information

When you log in to the controller, the Dashboard page displays. You can view the general device information on this page.

To view the controller system information:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. On the right side of the Dashboard page, the System Information pane displays the following information:

Table 3.System information

Field	Description
System Name	The name of your controller.
Model	The model of your controller.
Serial Number	The serial number of your specific controller.
MAC Address	The MAC address of your controller.
Firmware Version	The firmware version that your controller is running.
System Uptime	The number of minutes since your controller was last started.

3. The System Information pane also displays the following statistical information:

Table 4.System information statistical information

Field	Description
CPU	The percentage of CPU which the controller is using.
RAM	The percentage of RAM which the controller is using. The maximum amount is 15.43 GB.
Fan	The percentage at which the fan is operating on the controller. The maximum amount is 130000 RPM.
App Storage	The percentage of storage which the controller is using. The storage capacity of the controller is 36.88 GB.
Internal Log Storage	The percentage of internal log storage which the controller is using. The internal log storage capacity of the controller is 9.75 GB.
Thermal	The operating temperature of the controller.

View the device port information

You can view the status of the controller's ports on the Dashboard page.

To view the controller port information:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. On the left side of the Dashboard page, the Device Ports pane displays the status information for each port.
   You can view the port status of the controller on the device image. The following table describes the port status indicators:

Table 5.Port status

Indicator	Status	Description
Green outline	Connected	The port has an active link and is passing traffic.
Blue outline	Connected & Powered	The port is connected and supplying power through PoE.
Red outline	Error	The port has encountered an error condition.
Exclamation	Admin Down	The port has been manually disabled by an administrator.
No indicator	Available	The port is operational but no device is currently connected.
Port grayed out	Disabled	The port is disabled and not available for use.
LAG icon	LAG	The port is a member of a Link Aggregation Group.
A icon	Auto Trunk	The port is configured for automatic trunking.
M icon	Manual Trunk	The port is configured as a manual trunk.
S icon	1G SFP Fiber Port	The port is a 1G SFP fiber port.
S+ icon	10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port.
Green outline power symbol	Powered by PoE	The controller is powered through PoE. No Ethernet link is established.

View the controller networks

You can view the status of the controller's networks on the Dashboard page. For information about editing a network, see Edit a network on page 33.

To view the controller network information:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. The Networks pane displays the following information:

Table 6.Networks

Field	Description
Network	The name of the network.
Ports	The ports that belong to the network.
VLANs	The number of VLANs configured on the network.
IP (Native VLAN)	The IP address assigned to the native VLAN of the network.

View the Engage status of devices on the controller

You can view the status of your devices that are connected to Engage, both online and offline, on the Dashboard page. You can also view available devices which Engage has discovered, but that are not yet connected.

To view Engage status of devices on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. You can view the Engage status on your devices connected to the controller on the Engage Status pane. The pane displays the following information:

Table 7.Engage status

Field	Description
Online Devices	The number of switches, routers, and access points that are online and connected to Engage.
Offline Devices	The number of switches, routers, and access points that were previously connected to Engage but are currently offline.
Discovered Devices	The number of switches, routers, and access points that are online and discovered by Engage but are not currently connected.

View the status of the controller's services

The Service Status pane on the Dashboard page displays the network services running on the controller. Each service displays with either a Running or Stopped status.

To view the service status on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. The Service Status pane on the bottom of the Dashboard page displays the status of the following network services:

Table 8.Service status

Field	Description
DHCP	DHCP assigns IP addresses automatically to devices on the network. When running, the controller acts as a DHCP server for connected devices.
PTP	Precision Time Protocol (PTP) provides precision time synchronization for applications that require highly accurate timekeeping, such as audio or video equipment.
Syslog	The syslog server collects and stores log messages from the controller and connected devices for monitoring and troubleshooting purposes.
NTP	Network Time Protocol (NTP) keeps the device clock synchronized with a time source, ensuring accurate timestamps across logs and events.
DNS	DNS resolves hostnames to IP addresses, allowing devices to communicate using names rather than numerical addresses.
mDNS	Multicast DNS enables local network service discovery, allowing devices to find each other on the network without a dedicated DNS server.
LLDP	Link Layer Discovery Protocol (LLDP) allows the controller to discover and share information about neighboring network devices, such as connected switches.
HTTP	HTTP serves the controller web management interface. This service is always active while a device is accessible through a browser.

Configure the system administration settings

You can configure and manage the system settings on the System Administration page. The System Administration page lets you view and configure basic system settings for your device, including the system name, date, time, and time zone. You can also set the device to adjust for daylight saving time automatically.

To edit the system administration settings on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > System**.
   The System Administration page displays.
3. Select from one of the following options:
   - Edit the system name on page 21.
   - Configure the date and time of the controller on page 21.
   - Configure daylight saving time settings on page 22.

Edit the system name

To edit the system name on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > System**.
   The System Administration page displays.
3. In the **System Name** field, enter a new system name.
4. Click the **Apply** button.
   Your settings are saved.

Configure the date and time of the controller

To manually configure the date and time on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. Select **Settings > Configuration > System**.
   The System Administration page displays.
3. In the **Date** field, select a date.
4. In the **Time** field, select a time.
5. Optionally, you can choose to enable daylight saving time settings. For more information, see Configure daylight saving time settings on page 22.
6. Click the **Apply** button.
   Your settings are saved.

Sync the date and time of the controller with your local browser

To sync the date and time of the controller with your local browser:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > System**.
   The System Administration page displays.
3. Click the **Sync date, time, and time zone with browser** button.
4. Click the **Apply** button.
   Your settings are saved.

Configure daylight saving time settings

You can configure settings for summer time, which is also known as daylight saving time. Used in some countries around the world, summer time is the practice of temporarily advancing clocks during the summer months. Typically clocks are adjusted forward one or more hours near the start of spring and are adjusted backward in autumn.

To configure the daylight saving time settings:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > System**.
   The System Administration page displays.
3. Select the **Adjust for daylight saving time automatically** toggle so that it is positioned on the right.

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

Manage Your Apps on the controller

You can discover, install, and manage applications on the controller on the Apps page.

NOTE: Enable internet access on your controller to view the full list of apps available.

Each app displays the app name, a brief summary of the app, the app category, and the current app version. You need to purchase and activate a license key before installing any apps.
You can access the release notes of each app by clicking the **Expand** icon on the app. You can change between grid view and list view at any time using the icons in the top right corner of the page.
This chapter includes the following sections:

- Activate your license
- Display the apps on your controller
- Install a new app on your controller
- Install an app on your controller offline
- Uninstall an app from the controller
- Activate or deactivate an app on your controller

Activate your license

The controller is designed for use with NETGEAR Engage, but you cannot activate the controller license key in Engage. You must activate your license before you can install and use any apps on your controller. You can activate the key in any of the following ways:

- In the Insight Cloud Portal: Activate the license from Insight Cloud on page 24. If you already manage other NETGEAR devices in the Insight Cloud Portal, adding the controller to it is a convenient way to activate the license. You cannot manage the controller in Insight, but you can use Insight to remotely access the device UI of the controller.
- In the device UI of the Align Controller: Activate the license from the device UI on page 27.
- On the MyNETGEAR website at my.netgear.com: Activate the license from MyNETGEAR on page 26.

Activate the license from Insight Cloud

A controller needs a valid license so that you can use the apps on the controller and access the controller remotely. Each controller comes with a 90-day license, and you can add a purchased license key to keep the controller licensed after the 90 days end.

How the controller licenses work

A controller license works differently from other Insight Cloud Portal subscriptions:

- **One key per controller**: Each license key applies to one controller. The key does not use or

add to the subscription credits of your organizations, and it is not shared across organizations.

- **Tied to the serial number**: After you assign and activate the key, it is tied to the serial number of that controller until the license expires. You cannot move the key to another controller, even if you unmanage, delete, or move the original controller.
- **No scheduled activation**: You cannot schedule activation for a later date. The key is activated when you assign it.
- **90-day license ends**: When you assign a purchased key to the controller, the 90-day license ends.
- **License kept after delete**: If you delete a controller and add it again, Insight automatically applies the license that is already tied to the serial number of the controller. You do not need to enter the key again.

What happens when a controller license expires

If the purchased license and the 90-day license both expire, you cannot use the apps on the controller or access the controller remotely until you assign a new key.
For more information, see Add a license key from Insight on page 25.

Add a license key from Insight

- Make sure that you have the Align Controller license key from your NETGEAR partner or authorized distributor.
- To assign the key in this procedure, make sure that the Align Controller is added to an organization and location in the Insight Cloud Portal. You can also add the key without a controller and assign it later.

The LMS license key is activated when you assign it, and is then tied to that Align Controller. For more information, see Activate the license from Insight Cloud on page 24.

1. Access the Insight Cloud Portal.
   For more information, see the Insight Cloud User Manual which you can download by visiting netgear.com/support/enterprise.
   The Insight dashboard displays.
2. Select **Administration > Manage Subscriptions**.
3. Click the **Choose Plan** link.
   A dialog box displays the subscription options.
4. On the **NETGEAR Partner** tile, click the **Choose Plan** button.
5. In the **Subscription Key** field, enter your Align Controller license key.
   Insight identifies the key as an Align Controller license key.
6. Click the **Assign to a device** radio button.

7. Alternatively, select the **Add to unallocated subscription** radio button to add the key without assigning it to a controller.
8. In the **Assign to Device** section, select the Align Controller that you want to assign the key to:
   a. From the **Select Organization** menu, select the organization.
   b. From the **Select Location** menu, select the location.
   c. From the **Select Device** menu, select the Align Controller.
   The menu lists only Align Controllers that use the 90-day license or whose license expired.
9. Click the **Add** button.
   Insight activates the license for the Align Controller. The device status shows **Align** and the number of days remaining.

To assign an unallocated key later, go to the **Manage Subscriptions** page, click the unallocated count in the **Align** row, and click the **Assign** link next to the key.

Activate the license from MyNETGEAR

To activate your license from my.netgear.com/**:**

1. Launch my.netgear.com/.
2. If you have not yet registered the controller:
   a. Under **YOUR REGISTERED PRODUCTS**, locate the controller on which you want to activate the license.
   b. Click the **VIEW PRODUCT** button.
   c. Click the **ACTIVATE LICENSE** button.
   The Activate License Key pop-up window displays.
   d. Enter the license key and click the **ACTIVATE** button.
3. After the activation is complete, click the **DOWNLOAD EAV** button to download the license file to your local computer.
4. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
5. Select **Settings > Configuration > App Licenses**.
6. Click the **Upload** button.
7. Select the downloaded license file.
8. Click the **Upload License** button to install the license on your controller.
   The license key is activated.

Activate the license from the device UI

Your controller must have internet access for license activation through the device UI.

To activate your license from the device UI:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > App Licenses**.
3. Enter the license key in the **License Key** field.
4. Enter your email address.
5. Click the **Activate** button to activate the license.
   The license key is activated.

Display the apps on your controller

The Align AppHub page displays a list of available apps for your controller. Each app in the displays the app name, description, category, and the current firmware version.

To view the apps on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Apps**.
   The Align AppHub page displays. You can launch, install, update, or uninstall the apps.
3. Use the search bar on the top right-hand corner to search for a specific app.
4. To filter the apps by category, select one of the following tabs:
   - **All**: Displays all available apps. This is the default setting.
   - **AV**: Displays all AV apps.
   - **Generic**: Displays all generic apps.
   - **Networking**: Displays all networking apps.
   - **Security**: Displays all security apps.

Install a new app on your controller

You can install apps from the Align AppHub page. Once an app is installed, the app displays on the Installed App page.

NOTE: You can cancel an install at any time by clicking the **Cancel** button.

To install a new app on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Apps**.
   The Align AppHub page displays showing a list of available apps.
3. Navigate to the app you want to install on the controller.
4. Click the **Install** button.
   The Install App window displays.
5. Click the **Install** button to install the app.
   When the app starts installing, it displays a circular progress bar with a percentage showing progress. The download status also appears on the **Download** icon at the Dashboard's upper right corner.

   NOTE: The controller supports up to two simultaneous app downloads. Additional downloads queue until a slot becomes available.
6. Click the **Launch** button to open the app.
   You can view the installed app on the Installed Apps page. Select **Apps > Installed Apps**.

Install an app on your controller offline

You need a valid App license to install applications. You can install an app offline by downloading an app from the App Catalogue and uploading the app to your controller.

To install an app offline from the App Catalogue:

1. Open a web browser and go to apphub.netgear.com/.
2. Sign in with your NETGEAR account.
3. Find the app that you want to install.
4. Click the **More Details** button to open the app details page.

5. Click the **Export as USB Installed Image** button to download the app installation image to your local computer.
6. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
7. Select **Apps > Offline Install**.
8. Click the **Upload** button.
9. Select the app image that you downloaded from Apps page.
10. After the image is uploaded, click the **Install App** button.

Uninstall an app from the controller

You can uninstall an app from your controller on the Apps page.

NOTE: You cannot uninstall the Engage app from the controller.

To uninstall an app on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Apps > Installed Apps**.
3. On the app which you want to uninstall, click the **Delete** icon.
   The app is uninstalled and your settings are saved.
   You can view the installed app on the Installed Apps page. Select **Apps > Installed Apps**.

Activate or deactivate an app on your controller

After installing an app on your controller, you can activate the app so that it is running on the controller or deactivate the app so that is has stopped running.

To run or stop an app on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Apps > Installed Apps**.

3. To filter the apps by category, select one of the following tabs:
    - **All**: Displays all available apps. This is the default setting.
    - **AV**: Displays all AV apps.
    - **Generic**: Displays all generic apps.
    - **Networking**: Displays all networking apps.
    - **Security**: Displays all security apps.
4. On the app you want to manage, select whether to activate or deactivate the app.
5. If the app is deactivated, to activate the app, select the **Stopped** toggle:
    - The toggle displays **Running** in green and is positioned to the right: The app is activated and running on your controller.
6. If the app is activated, to deactivate the app, select the **Running** toggle:
    - The toggle displays **Stopped** in gray and is positioned to the left: The app is deactivated and has stopped running on your controller.

Manage Configured Networks

You can manage your network topology through the **Networks** page.
A network is an isolated Layer 2 bridge group that owns a set of member ports. You can configure up to six networks on the controller and assign a port to each network. Assigning a port to a network automatically removes it from its previous network. You can assign ports to networks, configure IP settings, and add VLANs to each network from this page.
This chapter includes the following sections:

- Configure networks overview
- Auto-Trunk overview
- Auto-LAG overview
- Edit a network

Configure networks overview

The **Networks** page displays the six fixed networks on the controller and shows how the physical ports are currently assigned. The controller always exposes exactly six networks. You cannot create or delete a network.
You can view the port status of the controller on the device image. The following table describes the port status indicators:

Table 9.Port status

Indicator	Status	Description
Green outline	Connected	The port has an active link and is passing traffic.
Blue outline	Connected & Powered	The port is connected and supplying power through PoE.
Red outline	Error	The port has encountered an error condition.
Exclamation	Admin Down	The port has been manually disabled by an administrator.
No indicator	Available	The port is operational but no device is currently connected.
Port grayed out	Disabled	The port is disabled and not available for use.
LAG icon	LAG	The port is a member of a Link Aggregation Group.
A icon	Auto Trunk	The port is configured for automatic trunking.
M icon	Manual Trunk	The port is configured as a manual trunk.
S icon	1G SFP Fiber Port	The port is a 1G SFP fiber port.

Indicator	Status	Description
S+ icon	10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port.
Green outline power symbol	Powered by PoE	The controller is powered through PoE. No Ethernet link is established.

You can edit a network in the Configured Networks section.
The Configured Networks table displays the following information:

- **Network**: The network name and color indicator.
- **MAC Address**: The MAC address assigned to the network. MAC addresses are sequential from the device base MAC address.
- **Ports**: The ports that belong to the network. The Unassigned row lists any ports not assigned to a network.
- **IP (native VLAN)**: The IP address assigned to the native VLAN of the network.
- **VLANs**: The number of VLANs configured on the network.

Auto-Trunk overview

You can configure trunking on your controller through the Networks page.
Auto-Trunk lets the controller automatically enable trunk mode on capable physical ports and LAG interfaces when it detects a switch with trunk capabilities. A trunk carries multiple VLANs and accepts both tagged and untagged packets. The controller enables Auto-Trunk by default. When the controller automatically configures a port as an Auto-Trunk, all active VLANs become part of the trunk. This lets the controller and the connected partner device automatically configure all VLANs at both ends. The port displays an **A** icon to indicate that the controller configured it as an Auto-Trunk.
Before the controller configures an Auto-Trunk, it detects the physical link with a partner device that also supports Auto-Trunk, then automatically configures the connected ports at both ends. For the controller to form an Auto-Trunk with the partner device, the following are required:

- Both the controller and the partner device must support and have Auto-Trunk enabled.
- The interconnected ports on both devices must be enabled.
- Both devices must have LLDP enabled on the interconnected ports. The controller enables LLDP by default on all ports.
- The interconnected ports must be in the default port mode.

Auto-Trunk works together with the Auto-LAG feature. After the controller and a partner device form an Auto-LAG, the controller automatically applies trunk mode to the LAG at both ends, changing the port mode from the default port mode to trunk mode. The Auto-LAG then becomes an Auto-Trunk, and the controller and the partner device can automatically configure all VLANs.
For more information, see Auto-LAG overview on page 33.

Auto-LAG overview

An Auto-LAG is a LAG that forms automatically between two devices that support the Auto-LAG feature.
Auto-LAG is a dynamic Layer 2 LAG based on the Link Aggregation Control Protocol (LACP). The controller detects physical links with a partner device and automatically configures a LAG on interconnected and capable ports at both ends. The controller can form one Auto-LAG only with each partner device. Auto-LAG works together with the Auto-Trunk feature. After the controller and a partner device form an Auto-LAG, the controller automatically applies trunk mode to the LAG at both ends, changing the port mode from the default port mode to trunk mode. For more information, see Auto-Trunk overview on page 32.
For the controller to form an Auto-LAG with a partner device, your environment must meet the following conditions:

- Both the controller and the partner device must support and have both Auto-LAG and Auto-Trunk enabled.
- At least two links must be established between the controller and the partner device, and these links must support the same speed and duplex mode.
- The links must not be members of a manually configured static LAG.
- Both devices must have LLDP enabled on the interconnected ports. For more information, see Enable or disable LLDP server on page 90.
- The interconnected ports must be in the default port mode.

You can select interfaces for the Auto-LAG provided that the following conditions are met:

- 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.
- The interface must be a general interface.

The controller supports multiple static LAGs, but can form only a single Auto-LAG with each partner device.

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

Edit a network

The controller has six configured networks which you can assign to different ports. You can configure only one network per port, but you can assign multiple ports to a network.
To edit a network on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Networks**.
   The Networks page displays.

3. In the Configured Networks table, select the network you want to edit.
4. Click the **Edit** button.
   The Edit Network page displays.
5. Click the **Ports** tab.
   This is the default tab.
6. In the **Network Name** field, type a name for the network.
7. Click the box in the **Color** field, and select a color.
   This unique color indicates what network a port supports if you tag a port to a network profile in step 8.
8. In the Member Ports section, click the port you want to select as a member of the network.
   The selected port display a green checkmark icon. Selecting a port assigned to another network moves it to this network.
   The port displays the unique color you set in step 7.
9. To configure the trunk settings on the port, select the **Auto Trunk** toggle:
   - **Enable**: The toggle is on and positioned on the right. This is the default setting.
   - **Disable**: The toggle is off and positioned on the left.

   To configure trunking manually, from the Manual Trunk Ports menu, select the port or ports you want to add to the network.
10. To enable automatic link aggregation, turn on the **Auto LAG** toggle.
11. Select an option from the **Auto-LAG Hash** menu:
    - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses in the packet. This is the default option.
    - **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.

    NOTE: Auto Trunk and Auto LAG operate within a single network only. Link aggregation cannot span two different networks. If you want to manually configure a LAG, both ports must belong to the same network. For more information about Auto LAG, see Auto-LAG overview on page 33.
12. Click the **IP & Management** tab.
13. In the **Native / Untagged VLAN ID** field, type the VLAN ID to use as the native VLAN for this network.
    L3 settings on this tab apply to the native VLAN of this network.

14. In the **IP Settings** field, select one of the following options:
    - **Static IP**: Assigns a fixed address manually.
    - **DHCP**: The address is assigned automatically by a DHCP server.

    To set this network as the source of the controller's default route, select the **Use the gateway setting below as Align Controller's default route** checkbox.
15. Click the **VLANs** tab.
    VLANs in a network are available only on that network's trunk ports. All other ports carry only untagged traffic on the native VLAN.
16. To add a new VLAN, click the **Add VLAN** button.
    The Add VLAN page displays.
17. In the **VLAN ID** field, enter the VLAN ID to which the traffic of the profile must be assigned.
    You can configure any value in the range of 1 to 4093.
18. From the **IP Settings** section, select one of the following options:
    - **Static IP**: Assigns a fixed address manually.
    - **DHCP**: The address is assigned automatically by a DHCP server.
    - **None**: No IP address for this VLAN.

    To set this VLAN as the source of the controller's default route, select the **Use the gateway setting below as Align Controller's default route** checkbox.
19. Click the **SAVE** button.
    The VLAN is added to the network and displays in the VLANs table.
20. Click the **APPLY** button.
    Your settings are saved. The updated profile displays in the table on the Network Profile page.

Manage System Settings from the Controller

This chapter includes the following sections:

- Link aggregation groups
- Port settings

Link aggregation groups

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 controller lets you configure the ports and create and manage two LAG options.
You can view which ports are configured as LAGs on the Link Aggregation page.
You can view the port status of the controller on the device image. The following table describes the port status indicators:

Table 10.Port status

Indicator	Status	Description
Green outline	Connected	The port has an active link and is passing traffic.
Blue outline	Connected & Powered	The port is connected and supplying power through PoE.
Red outline	Error	The port has encountered an error condition.
Exclamation	Admin Down	The port has been manually disabled by an administrator.
No indicator	Available	The port is operational but no device is currently connected.
Port grayed out	Disabled	The port is disabled and not available for use.
LAG icon	LAG	The port is a member of a Link Aggregation Group.
A icon	Auto Trunk	The port is configured for automatic trunking.
M icon	Manual Trunk	The port is configured as a manual trunk.
S icon	1G SFP Fiber Port	The port is a 1G SFP fiber port.

Indicator	Status	Description
S+ icon	10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port.
Green outline power symbol	Powered by PoE	The controller is powered through PoE. No Ethernet link is established.

Configure a LAG and its membership

You can configure a single LAG and add physical interfaces as members to the LAG. You can create up to two LAGs on the controller. From the Link Aggregation page, you can create, edit, or delete a LAG.

To display the Link Aggregation page on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Link Aggregation**.
3. In the Link Aggregation Group section, the table displays the following information:
   - **LAG Name**: The name of this LAG entry.
   - **LAG #**: The ID for this LAG.
   - **Hash**: The Hash type of this LAG.
   - **Mode**: The mode of the LAG, which can be Static or Auto.
   - **Members**: The ports assigned to this LAG.
   - **Status**: The status for the LAG.
     - **Up**: The LAG is established and active.
     - **Down**: The LAG is not established.

Create a new LAG

You can create up to two LAGs on the controller.

To create a LAG:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Link Aggregation**.

3. In the Link Aggregation Group section, click the **Add** button.
   The Create Link Aggregation Group page displays.

   NOTE: The **Add** button displays the number of LAGs out of the maximum of two.

4. On the graphical display of the controller, select the port on which to configure the LAG.
5. In the **LAG Name** field, specify a name for the LAG.
6. From the **Hash** menu, select the hash mode for the LAG:
   - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses in the packet. This is the default option.
   - **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.
7. From the **LAG ID** menu, select the LAG ID for the LAG. You can only add up to two LAGs.
8. To create a static LAG, turn on the **Static LAG** toggle so that it is positioned to the right.
9. Click the **SAVE** button.
   Your settings are saved. The new LAG displays in the table.

Edit a LAG on the controller

You can create up to two LAGs on the controller and edit a LAG from the Link Aggregation page.

To edit a LAG:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Link Aggregation**.
3. In the Link Aggregation Group section, select the LAG that you want to edit.
4. Click the **Edit** button.
   The Edit Link Aggregation Group page displays.
5. To edit the port for the LAG, on the graphical display of the controller, select the port on which to configure the LAG.
6. In the **LAG Name** field, specify a name for the LAG.

7. From the **Hash** menu, select the hash mode for the LAG:
   - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses in the packet. This is the default option.
   - **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.
8. From the **LAG ID** menu, select the LAG ID for the LAG. You can only add up to two LAGs.
9. To configure this LAG as a static LAG, turn on the **Static LAG** toggle so that it is positioned to the right.
10. Click the **SAVE** button.
    Your settings are saved. The LAG displays in the table.

Delete a LAG from the controller

To delete a LAG from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Link Aggregation**.
3. In the Link Aggregation Group section, select the LAG that you want to delete.
4. Click the **Delete** button.
   The Confirm Delete page displays.
5. Click the **DELETE** button.
   Your settings are saved.

Port settings

For the physical ports and LAGs on the controller, you can display the settings and configure the administrative mode of a port or LAG (both of which are enabled by default). You can also add port descriptions and adjust the speed of the ports.
You can view the port status of the controller on the device image. The following table describes the port status indicators:

Table 11.Port status

Indicator	Status	Description
Green outline	Connected	The port has an active link and is passing traffic.
Blue outline	Connected & Powered	The port is connected and supplying power through

Indicator	Status	Description
		PoE.
Red outline	Error	The port has encountered an error condition.
Exclamation	Admin Down	The port has been manually disabled by an administrator.
No indicator	Available	The port is operational but no device is currently connected.
Port grayed out	Disabled	The port is disabled and not available for use.
LAG icon	LAG	The port is a member of a Link Aggregation Group.
A icon	Auto Trunk	The port is configured for automatic trunking.
M icon	Manual Trunk	The port is configured as a manual trunk.
S icon	1G SFP Fiber Port	The port is a 1G SFP fiber port.
S+ icon	10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port.
Green outline power symbol	Powered by PoE	The controller is powered through PoE. No Ethernet link is established.

Configure and display the port settings

You can configure and display the information for the physical port on the controller. Some settings that apply to physical ports do not apply to LAGs.

To configure the port settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Port Configuration**.
   The Port Interface Details page displays.
3. Choose the port which you want to configure.
   Ports 1-4 are copper interface ports, port 5 is a 1G SFP fiber port, and port 6 is a 10G SFP+ fiber interface. If you have configured LAGs on your controller, the LAGs also display on the Port Interface Details page.
4. Click the **Port Description** field and enter a description of up to 64 characters.

5. Select the **Admin Mode** toggle to enable or disable admin mode:
   - **Enable**: The toggle so that it is positioned to the right. This is the default setting.
   - **Disable**: The toggle so that it is positioned to the left.
6. You can view the link status of the port from the **Link Status** menu.
   - **Up**: The port has an active physical link.
   - **Down**: The port is inactive or has no physical link.
7. Click the **Speed** menu and select a speed.
   For copper interface ports 1-4:
   - **Auto**: The speed is set by the auto-negotiation process. This is the default setting.
   - **2.5G**: The speed is set to 2.5 Gbps.
   - **1G**: The speed is set to 1 Gbps.
   - **100M**: The speed is set to 100 Mbps.

   For fiber interface ports 5-6:
   - **Auto**: The speed is set by the auto-negotiation process. This is the default setting.
   - **10G**: The speed is set to 10 Gbps.
   - **1G**: The speed is set to 1 Gbps.
8. Click the **Apply** button.
   Your settings are saved.
   The updated values display for each selected port.

NOTE: It might take a number of seconds for your settings to display. You can refresh the page by clicking the **Refresh** button.

Configure port settings for multiple ports

NOTE: The 1G and 2.5G copper ports and fiber 10G ports support auto-negotiation, which is enabled by default. You cannot disable this setting.

To configure port settings for multiple ports at the same time on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Port Configuration**.
   The Port Interface Details page displays.
3. Select the checkbox next to each port or LAG you want to configure.

4. To apply a description to the selected ports, click the **Port Description** field in the top row and enter a description of up to 64 characters.
5. Select the **Admin Mode** toggle in the top row to enable or disable admin mode for the selected ports:
   - To enable the admin mode, select the toggle so that it is positioned to the right. This is the default setting.
   - To disable the admin mode, click the toggle so that it is positioned to the left.
6. To apply a speed setting to the selected ports, click the **Speed** menu in the top row and select a speed.
   For copper interface ports 1-4:
   - **Auto**: The speed is set by the auto-negotiation process. This is the default setting.
   - **2.5G**: The speed is set to 2.5 Gbps.
   - **1G**: The speed is set to 1 Gbps.
   - **100M**: The speed is set to 100 Mbps.

   For fiber interface ports 5-6:
   - **Auto**: The speed is set by the auto-negotiation process. This is the default setting.
   - **10G**: The speed is set to 10 Gbps.
   - **1G**: The speed is set to 1 Gbps.
7. Click the **Apply** button.
   Your settings are saved.
   The updated values display for each selected port.

> **NOTE:** It might take a number of seconds for your settings to display. You can refresh the page by clicking the **Refresh** button.

Configure port settings for a LAG

You can configure and display the information for a LAG that you created controller.

To configure the port settings for a LAG on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Port Configuration**.
   The Port Interface Details page displays.
3. Choose the LAG port which you want to configure.
   The LAGs display as **L1** and **L2** at the bottom of the Port Interface Details page.

4. To edit the LAG name, click the **Port Description** field and enter a description of up to 64 characters.
5. Select the **Admin Mode** toggle to enable or disable admin mode:
   - To enable the admin mode, select the toggle so that it is positioned to the right. This is the default setting.
   - To disable the admin mode, click the toggle so that it is positioned to the left.
6. You can view the link status of the LAG port from the **Link Status** menu.
   - **Up**: The port has an active physical link.
   - **Down**: The port is inactive or has no physical link.
7. Click the **Apply** button.
   Your settings are saved.
   The updated values display for each selected port.

NOTE: It might take a number of seconds for your settings to display. You can refresh the page by clicking the **Refresh** button.

Manage the Service Settings

You can manage the DHCP, PTP, syslog, NTP, DNS, HTTPS, mDNS, and LLDP service settings on the controller.

This chapter includes the following sections:

- Manage the DHCP server
- Manage the PTP server
- Manage the syslog server
- Manage the NTP server
- Manage the DNS server
- Manage the HTTPS server
- Manage the mDNS server
- Manage the LLDP service

Manage the DHCP server

The controller includes a built-in DHCP server that automatically assigns IP addresses and network configuration to devices on your network. The DHCP server is disabled by default. To enable the DHCP server, see Enable or disable the DHCP server on page 44.

You can configure the DHCP server to manage IP address assignment across multiple subnets, each associated with a network profile and VLAN. The controller supports up to 1028 subnets and a total of 65,536 IP addresses across all subnets.

After you enable the DHCP server, you can view the DHCP server overview on the Overview page.

Enable or disable the DHCP server

The DHCP server is disabled by default.

To enable or disable the DHCP server on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Settings**.
   The Settings page displays.
3. Click the **DHCP Service** toggle to enable or disable the DHCP server:
   - **Enable**: The toggle is positioned to the right.
   - **Disable**: The toggle is positioned to the left. This is the default setting.

4. Click the **Apply** button.
   Your settings are saved. After you enable the DHCP server, you can view the DHCP server overview on the Overview page.

Display the DHCP server overview

The Overview page displays the server status, lease statistics, a summary of configured subnets, active bindings, and a chart of DHCP activity over time.

NOTE: You must enable the DHCP server to view the DHCP server overview features. See Enable or disable the DHCP server on page 44.

To view the DHCP settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP**.
   The Overview page displays.
3. The Server section displays the status of the DHCP server. The DHCP server can be Running or Stopped.
4. You can view the following information in the Statistics section:
   - **Total Subnets**: Displays the total number of subnets created by the user.
   - **IPs Available**: Indicates the total number of available IPs (those not yet assigned).
   - **Active Leases**: Displays the total number of leased IPs.
   - **IPs Expired**: Shows the total number of expired IPs.
5. To edit the data in the DHCP Statistics section, click the menu to choose one of the following time periods:
   - **Last Hour**: Displays data for the past hour, with statistics provided every minute.
   - **Last Day**: Displays data for the past 24 hours, with statistics provided every 20 minutes.
   - **Last 7 Days**: Displays data for the past 7 days, with statistics provided on an hourly basis.
6. To edit the chart lines in the DHCP Statistics section, click the **Lines** button:
   - **Active Leases**: Click to enable or disable the toggle to view the active leases.
   - **IPs Available**: Click to enable or disable the toggle to view the available IPs.
   - **IPs Expired**: Click to enable or disable the toggle to view the expired IPs.
   - **Total Requests**: Click to enable or disable the toggle to view the total requests.

7. You can view the following information in the Bindings section:
   - **IP Address**: The IP address assigned.
   - **MAC Address**: The MAC address associated with the IP address.
   - **Hostname**: The hostname designated to the client.
   - **Client ID**: The client ID information provided by the client.
   - **Expire**: The expiration time of this lease.
   - **VLAN ID**: The VLAN ID for this lease.
   - **Subnet**: The subnet name associated with this IP address.
   - **Status**: This lease's status can be either **Active** or **Expired**.
8. You can view the following information in the Subnets section:
   - **Name**: The name of the subnet.
   - **Start IP**: The starting and ending IP addresses of a pool.
   - **End IP**: The starting and ending IP addresses of a pool.
   - **Status**: Indicates the current status of the subnet, which can be **Active** or **Inactive**.
   - **Usage**: Displays the percentage of available IPs relative to the total IP pools.
   - **Template**: Shows the template name associated with this subnet.

Configure the global DHCP settings

The global DHCP server settings apply to all subnets unless a subnet is configured with its own values.

NOTE: The DHCP server is disabled by default. You must enable the DHCP server to view the features, see Enable or disable the DHCP server on page 44.

To configure the global DHCP settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Settings**.
   The Settings page displays.
3. If you have not already enabled the DHCP server, click the **DHCP Service** toggle to enable or disable the DHCP server:
   - **Enable**: The toggle is positioned to the right.
   - **Disable**: The toggle is positioned to the left. This is the default setting.
4. To enable or disable logging, click the **Enable Logging** toggle:
   - To enable logging, click the toggle so that it is positioned to the right.
   - To disable logging, click the toggle so that it is positioned to the left.

5. In the **Option Domain Name** field, enter the domain name for clients.
   If a subnet is configured with its own domain name, the subnet setting takes precedence.
6. In the **Default Lease Time** field, enter the global lease time in minutes.
   The allowed range is 10 to 525,600 minutes. The default value is 1440 minutes.
7. Optionally, in the **DNS Server 1** field, enter the IP addresses of the DNS server.
   If a subnet is configured with its own DNS servers, the subnet settings take precedence.
8. Optionally, in the **DNS Server 2** field, enter the IP addresses of the DNS server.
   If a subnet is configured with its own DNS servers, the subnet settings take precedence.
9. Click the **Apply** button.
   Your settings are saved.

Manage the DHCP subnets

A DHCP subnet defines a pool of IP addresses that the controller assigns to devices on a specific network segment. Each subnet is associated with a VLAN, and can be configured with its own lease time, domain name, DNS servers, and gateway address.
Each subnet can include up to 16 IP address ranges and can be associated with a DHCP template that defines custom options and client classification rules. You can also enable Dynamic DNS updates for a subnet, which lets the controller automatically add and remove hostnames from the DNS server as leases are assigned and released.
The Subnets page lists all configured subnets and displays the subnet name, IP address ranges, the status toggle set to enabled or disabled, the current lease usage, and the DHCP template for each entry.

Add a DHCP subnet

A DHCP subnet defines a pool of IP addresses that the controller assigns to devices on a specific network.

To add a DHCP subnet on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Subnets**.
   The Subnets page displays.
3. Click the **Add** button.
   The Configure DHCP Subnet page displays.
4. In the **Subnet Name** field, enter a name of up to 64 characters.

5. From the **DHCP Template** menu, select a DHCP template to associate with the subnet.
   The default is None.
6. In the **Start IP Address** field, enter the start IP address.
7. In the **End IP Address** field, enter the end IP address.
8. To add an IP address range, click the **Add Range** button and enter a start IP address and end IP address.
   You can add up to 16 IP address ranges. The start and end IP addresses must be within the same subnet range.
9. From the **Option Subnet Mask** menu, select a subnet mask.
   The default value is 255.255.255.0 (/24).
10. Optionally, in the **Option Routers** field, enter the IP address of the option router.
    You can enter up to two IP addresses separated by commas.
11. To enable Dynamic DNS updates for this subnet, click the **DNS Update** toggle so that it is positioned to the right, then select a primary forward zone from the menu that displays.
    When enabled, the controller adds the hostname to the DNS server when a lease is assigned and removes it when the lease expires.

> **NOTE:** DNS Update requires the DNS server to be enabled and a primary forward zone to be configured.

12. To configure additional options, select the **More Options** checkbox and enter values for any of the following fields as needed:
    - **Option Domain Name**: The domain name for this subnet in FQDN format. If left blank, the global domain name setting applies.
    - **DNS Server 1**: Enter the IP addresses of the DNS server.
    - **DNS Server 2**: Enter the IP addresses of the DNS server.
    - **Next Server**: The TFTP server address for this subnet.
    - **Filename**: The DHCP filename option for this subnet.
    - **Option Time Offset**: The time offset in minutes. The allowed range is -720 to +840 minutes.
    - **Default Lease Time**: The lease time for this subnet in minutes. If left blank, the global lease time setting applies.
13. Click the **ADD SUBNET** button.
    The subnet is saved and the Subnets page displays.

Edit a DHCP subnet

To change the settings for a DHCP subnet on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Subnets**.
   The Subnets page displays.
3. Select the checkbox next to the subnet you want to change and click the **Edit** button.
   The Configure DHCP Subnet page displays.
4. In the **Subnet Name** field, enter a name of up to 64 characters.
5. From the **DHCP Template** menu, select a DHCP template to associate with the subnet.
6. To add an IP address range, click the add icon next to **IP Address** and enter a start IP address and end IP address.
   You can add up to 16 IP address ranges. The start and end IP addresses must be within the same subnet range.
7. From the **Option Subnet Mask** menu, select a subnet mask.
   The default value is 255.255.255.0.
8. Optionally, in the **Option Routers** field, enter the IP address of the gateway for this subnet.
   You can enter up to two IP addresses separated by commas.
9. To enable Dynamic DNS updates for this subnet, click the **DNS Update** toggle so that it is positioned to the right, then select a primary forward zone from the menu that displays.
   When enabled, the controller adds the hostname to the DNS server when a lease is assigned and removes it when the lease expires.



NOTE: DNS Update requires the DNS server to be enabled and a primary forward zone to be configured.

10. To configure additional options, select the **More Options** checkbox and enter values for any of the following fields as needed:
    - **Option Domain Name**: The domain name for this subnet in FQDN format. If left blank, the global domain name setting applies.
    - **DNS Server 1**: Enter the IP addresses of the DNS server.
    - **DNS Server 2**: Enter the IP addresses of the DNS server.
    - **Next Server**: The TFTP server address for this subnet.
    - **Filename**: The DHCP filename option for this subnet.
    - **Option Time Offset**: The time offset in minutes. The allowed range is -720 to +840 minutes.
    - **Default Lease Time**: The lease time for this subnet in minutes. If left blank, the global lease time setting applies.
11. Click the **UPDATE SUBNET** button.
    Your settings are saved and the Subnets page displays.

Delete a DHCP subnet

To delete a DHCP subnet from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Subnets**.
   The Subnets page displays.
3. Select the checkbox next to the subnet you want to delete.
4. Click the **Delete** button.
   The Confirm Deletion page displays.
5. Click the **DELETE** button.
   The subnet is removed from the controller.

Manage the DHCP templates

A DHCP template defines a set of custom DHCP options and client classification rules that you can apply to one or more subnets or address reservations. Using templates lets you apply a consistent configuration across multiple subnets without having to configure each subnet individually.
Custom DHCP options let you pass additional configuration information to clients when a lease is assigned. Each template supports up to 16 custom options. You can select from standard DHCPv4 option codes and specify the data type and value for each option.

Client classification rules let you restrict a template to specific clients based on criteria such as vendor class, MAC address prefix, user class, circuit ID, or remote ID. When client classification rules are enabled, only clients that meet the specified condition receive an IP address from subnets associated with that template.
The Templates page lists all configured templates and displays the template name, number of custom options, and whether client classification rules are enabled for each entry.

Add a DHCP template

A DHCP template lets you define a set of custom DHCP options and client classification rules that you can apply to one or more subnets.

To add a DHCP template on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Templates**.
   The Templates page displays.
3. Click the **Add** button.
   The Add DHCP Template page displays.

   NOTE: The **Add** button displays the number of templates out of the maximum of 30.

4. In the **Template Name** field, enter a name of up to 32 characters.

5. To add a custom DHCP option, click the **Add Option** button and configure the following:
   - **Option Name/Code**: Select a standard DHCPv4 option from the menu or enter an option name or code.
   - **Option Type**: Select the data type for the option value from one of the following options:
     - Binary
     - Boolean
     - Int8
     - Int16
     - Int32
     - Uint8
     - Uint16
     - Uint32
     - IPv4 Address
     - IPv6 Address
     - String
     - FQDN.

   You can add up to 16 custom options. To remove an option, click the **Delete** icon next to the entry.
6. In the **Value** field, enter a hex value.
7. To enable client classification rules, select the **Active Client Classification Rules** checkbox and configure the following:
   - **Match Condition**: Select the condition used to classify clients from one of the following options:
     - Vendor Class (Option 60)
     - MAC Prefix
     - User Class (Option 77)
     - Circuit ID
     - Remote ID
   - If you select **Circuit ID**, you can choose to add a remote ID rule by clicking the **Add Remote ID Rule** button.
   - If you select **Remote ID**, you can choose to add a circuit ID rule by clicking the **Add Circuit ID Rule** button.
   - **Match Value**: Enter the value to match against. The allowed format depends on the selected match condition.

   When client classification rules are enabled, only clients that meet the specified condition and value receive an IP address from this template.
8. Click the **ADD TEMPLATE** button.
   Your settings are saved.

Edit a DHCP template

To change the settings for a DHCP template on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Templates**.
   The Templates page displays.
3. Select the checkbox next to the template you want to change and click the **Edit** button.
   The Edit DHCP Template page displays.
4. In the **Template Name** field, enter a name of up to 32 characters.
5. To add a custom DHCP option, click the **Add Option** icon and configure the following:
   - **Option Name/Code**: Select a standard DHCPv4 option from the menu or enter an option name or code.
   - **Option Type**: Select the data type for the option value from one of the following options:
     - Binary
     - Boolean
     - Int8
     - Int16
     - Int32
     - Uint8
     - Uint16
     - Uint32
     - IPv4 Address
     - IPv6 Address
     - String
     - FQDN.

   You can add up to 16 custom options. To remove an option, click the **Delete** icon next to the entry.

6. To enable client classification rules, select the **Active Client Classification Rules** checkbox and configure the following:
   - **Match Condition**: Select the condition used to classify clients from one of the following options:
     - Vendor Class (Option 60)
     - MAC Prefix
     - User Class (Option 77)
     - Circuit ID
     - Remote ID
   - If you select **Circuit ID**, you can choose to add a remote ID rule by clicking the **Add Remote ID Rule** button.
   - If you select **Remote ID**, you can choose to add a circuit ID rule by clicking the **Add Circuit ID Rule** button.
   - **Match Value**: Enter the value to match against. The allowed format depends on the selected match condition.

   When client classification rules are enabled, only clients that meet the specified condition and value receive an IP address from this template.
7. Click the **UPDATE TEMPLATE** button.
   Your settings are saved.

Delete a DHCP template

To delete a DHCP template from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Templates**.
   The Templates page displays.
3. Select the checkbox next to the template you want to delete.
4. Click the **Delete** button.
   The Confirm Deletion page displays.
5. Click the **DELETE** button
   The template is removed from the controller.

Manage the DHCP reservations

An address reservation lets you assign a fixed IP address to a specific device on your network. When a device with a matching identifier requests an IP address from the controller, it always

receives the same reserved address rather than a dynamically assigned one.
The controller identifies devices for address reservation using one of the following methods:

- **Hardware address**: The controller matches the client by its MAC address. This is the default identification method.
- **Client ID**: The controller matches the client by a client identifier string, which can be entered as a hexadecimal or ASCII value.

You can create a reservation manually by entering the identifier and IP address, or you can create one directly from an existing DHCP binding. You can also associate a reservation with a DHCP template to apply custom options to that specific device.
You can import or export reservations from a CSV file, which lets you back up your reservation configuration or transfer it to another controller. The Address Reservations page lists all configured reservations and displays the identifier, IP address, hostname, associated template, and status for each entry.

Add an address reservation

An address reservation lets you assign a fixed IP address to a specific device based on its MAC address or client ID.

To add an address reservation on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Reservation**.
   The Address Reservations page displays.
3. Click the **Add** button.
   The Add Host page displays, showing a table of current bindings including the host, MAC address, and IP address.
4. To create a reservation from an existing binding, select the checkbox next to the binding and click the **SAVE** button.
   The reservation is saved and the Address Reservations page displays.
5. To create a reservation manually, click the **OTHERS** button.
   The Add DHCP Reservation page displays.

6. Configure the following:
   The Add DHCP Reservation page displays.
   - **DHCP Identifier Type**: Select **hw-address** to identify the device by MAC address, or **client-id** to identify it by client ID. The default is hw-address.
   - **Value Type**: Select **hex** or **string**.
   - **Value**: Enter the identifier value. For hex, enter up to 256 hexadecimal characters. For string, enter up to 128 ASCII characters.
   - **IP Address**: Enter the IP address to reserve in IPv4 format.
   - **Template**: Select a template for this reservation. The default is None.
   - **Hostname**: Enter an optional hostname for this reservation. The maximum length is 64 characters.
   - **VLAN ID**: This option is auto-selected from the IP address.
7. Click the **SAVE** button.
   Your settings are saved.

Edit an address reservation

To change an address reservation on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Reservation**.
   The Address Reservations page displays.
3. Select the checkbox next to the reservation you want to change and click the **Edit** button.
   The Edit DHCP Reservation page displays.
4. Configure the following:
   - **IP Address**: Enter the IP address to reserve in IPv4 format.
   - **Template**: Select a DHCP template to associate with this reservation. The default is None.
   - **Hostname**: Enter an optional hostname for this reservation. The maximum length is 64 characters.

   You cannot change the DHCP Identifier Type field, Value Type, Value field, VLAN ID, or Network Profile.
5. Click the **SAVE** button.
   Your settings are saved.

Delete an address reservation

To delete an address reservation from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Reservation**.
   The Address Reservations page displays.
3. Select the checkbox next to the reservation you want to delete.
4. Click the **Delete** button.
   The Confirm Deletion pop-up window displays.
5. Click the **DELETE** button.
   Your settings are saved.

Export address reservations

You can export all address reservations to a CSV file.

To export address reservations from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Reservation**.
   The Address Reservations page displays.
3. Click the **Export** button.
   The reservations are exported to a CSV file and downloaded to your computer.

Import an address reservation

You can import address reservations from a CSV file.

To import address reservations to your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Reservation**.
   The Address Reservations page displays.

3. Click the **Import** button.
   A file browser window displays.
4. Select the CSV file you want to import and click the **OK** button.
   The reservations are imported and display on the Reservation page.

View the DHCP bindings

The Bindings page displays all current and expired DHCP leases on the controller.

To view the DHCP bindings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Bindings**.
   The Bindings page displays a table of all DHCP leases including the IP address, MAC address, hostname, client ID, lease expiry, subnet, VLAN ID, and status for each lease.
3. To search for a specific lease, enter a search term in the **Search** field.
4. To filter the DHCP leases:
   a. Click the **Filter** icon. The Toggle Columns filter page displays.
   b. Select the checkbox for the filters you want to use.
5. To reload the list with the latest lease information, click the **Refresh** button.

Export the DHCP bindings

You can export all DHCP lease information to a CSV file.

To export the DHCP lease data from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Bindings**.
   The Bindings page displays.
3. Select the DHCP lease you want to export.
4. Click the **Export** button.
   The DHCP lease information is exported to a CSV file and downloads to your computer.

View and manage the DHCP logs

The DHCP Logs page displays log messages generated by the DHCP service, including the time, severity, and message for each entry. To view and manage DHCP logs on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DHCP > Logs**.
   The Logs page displays. The log table shows the following information for each entry:
   - **Time**: The date and time the log entry was generated.
   - **Severity**: The severity level of the log entry.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: A description of the event.
3. To search for a specific log entry, enter a search term in the **Search** field.
4. To filter the log entries, click the **Filter** button and select the criteria you want to apply.
5. To download the log entries to your computer, click the **Download** button.
   The log entries download as a file to your computer.
6. To reload the log entries with the latest data, click the **Refresh** button.
7. To clear all log entries, click the **Clear All** button.
   All log entries are permanently removed from the Logs page.

Manage the PTP server

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

clock. By default, PTP is disabled.

Enable or disable the PTP server

The PTP service and PTP logging are disabled by default. PTP logging records PTP-related events and messages to the controller's logs.

To enable or disable the PTP service and PTP logging on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Settings**.
   The Settings page displays.
3. Click the **PTP Service** toggle to enable or disable PTP service:
   - **Enable**: The toggle is positioned to the right.
   - **Disable**: The toggle is positioned to the left. This is the default setting.
4. Click the **Apply** button.
   Your settings are saved. After you enable the PTP service, you can view the PTP service settings on the Overview page.

Display the PTP server overview

See Enable or disable the PTP server on page 60 to enable PTP on your controller.

To view the PTP settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP**.
   The Overview page displays.
3. The Server section displays the status of the PTP service. The PTP server status can be Running or Stopped.
4. You can view the current time on the controller and the controller's timezone setting.

5. The PTP Status section displays the PTP status of all configured PTP instances on the controller. The table displays the following information:
   - **Name**: The name for the PTP instance.
   - **State**: The status of the PTP instance, which can be running or stopped.
   - **PTPv2 / AVB gPTP Profile**: The profile which the PTP instance uses:
     - **Default**: The default PTPv2 settings are used. This is the default setting.
     - **AES67**: A clock profile for connecting audio devices over a common PTP profile.
     - **SMPTE-2059-2**: A clock profile for video traffic.
     - **AES-R16-2016**: A clock profile that interoperates between SMPTE and AES67 clock profiles.
     - **802.1AS AVB**: A clock profile for audio video bridging (AVB).
   - **Role**: The PTP instance has two possible values:
     - **Master**: The clock acts as the grandmaster/master clock, providing time to other devices in the PTP domain.
     - **Slave**: The clock synchronizes its time to a master clock in the PTP domain.
6. The Events section displays the recent events on the controller relating to the PTP service. The table displays the following information:
   - **Time**: The date and time the event was generated
   - **Severity**: The severity level of the event.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: The details of the event notification.

Add a PTP instance

A PTP instance is a specific configuration of the Precision Time Protocol on the controller. Each instance defines how PTP operates on a particular set of ports and network profile, including settings such as the PTPv2 profile, transport method, domain, clock priorities, and timing intervals.
You can add up to six PTP instances on your controller.

To add a PTP instance on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Settings**.
   The Settings page displays.
3. Click the **Add** button.
   The Add PTP Instance page displays.

   NOTE: The **Add** button displays the number of PTP instances out of the maximum of six.

4. In the **Name** field, enter a name of up to 32 characters for this instance.
5. To enable this instance, click the **Admin Mode** toggle so that it is positioned to the right.
   Admin Mode is enabled by default.
6. From the **Network** menu, select the network to associate with this instance.
7. From the **VLAN** menu, select the VLAN to associate with this instance:
   The Ports field automatically populates with the enabled ports from the selected VLAN.
8. To manually select ports, click the **Ports** menu and select one or more ports.
9. From the **PTPv2 / AVB gPTP Profile** menu, select one of the following profiles:
   - **Default**: The default PTPv2 settings are used. This is the default setting.
   - **AES67**: A clock profile for connecting audio devices over a common PTP profile.
   - **SMPTE-2059-2**: A clock profile for video traffic.
   - **AES-R16-2016**: A clock profile that interoperates between SMPTE and AES67 clock profiles.
   - **802.1AS AVB**: A clock profile for audio video bridging (AVB).

   Selecting a profile automatically sets the default values for the timing and transport settings. Some settings are read-only depending on the profile selected.

10. In the **Local Clock Priority 1** field, enter a value between 0 and 255. The default value is 32. The priority 1 determines which switch that is capable of functioning as a grandmaster clock is elected to be the active grandmaster clock in the network.
11. In the **Local Clock Priority 2** field, enter a value between 0 and 255. The default value is 32. The priority 2 also determines which switch that is capable of functioning as a grandmaster clock is elected to be the active grandmaster clock in the network.
12. In the **Announce Interval** field, enter the period between successive Announce messages in logarithm to base 2 format.
    Announce messages help to elect the best grandmaster clock in the network. The following are the supported ranges and default settings for the PTP clock profiles:
    - **Default**: 0 to 4. The default setting is 1.
    - **AES67**: 0 to 4. The default setting is 1.
    - **SMPTE-2059-2**: –3 to 1. The default setting is 0.
    - **AES-R16-2016**: 0 or 1. The default setting is 0.
    - **802.1AS AVB**: –5 to 5. The default setting is 0.
13. In the **Announce Timeout**, enter the number of Announce messages that are not acknowledged before the switch determines that the grandmaster clock is not transmitting. You can enter a number from 2 to 10. The default setting for all PTP clock profiles is 3. For the AES-R16-2016 profile, the only possible value is 3.
14. In the **Sync Interval** field, enter the period between successive Sync messages, in logarithm to base 2 format.
    The following are the supported ranges and default settings for the PTP clock profiles:
    - **Default**: –1 to 1. The default setting is 0.
    - **AES67**: –4 to 1. The default setting is –3.
    - **SMPTE-2059-2**: –7 to –1. The default setting is –3.
    - **AES-R16-2016**: –4 to 1. The default setting is –3.
    - **802.1AS AVB**: –5 to 5. The default setting is –3.
15. In the **Delay-request Interval** or **Initial Pdelay Interval** (802.1AS only) field, enter the period between successive Delay-Request messages from the boundary clock to the grandmaster clock, in logarithm to base 2 format.
    Delay-request messages help to calculate the path delay. The following are the supported ranges and default settings for the PTP clock profiles:
    - **Default**: 0 to 5. The default setting is 0.
    - **AES67**: –3 to 5. The default setting is 0.
    - **SMPTE-2059-2**: –7 to 4. The default setting is –3.
    - **AES-R16-2016**: –4 to 5. The default setting is –3.
    - **802.1AS AVB**: –5 to 5. The default setting is 0.

16. From the **Transport** menu, set the transport protocol for use on the communication path. Select from one of the following options:
    - **IPv4**: The **IPv4** field displays. You can enter an IPv4 address in the **IPv4** field.
    - L2 Transport.

    This setting is read-only for AES67, SMPTE-2059-2, AES-R16-2016, and 802.1AS profiles.
17. In the **PTP Domain** field, enter a PTP domain number. The allowed range is 0 to 127. The default value is 0, except for SMPTE-2059-2 profiles where the default is 127.
18. From the **PTP Version** menu, select **2.0**.
19. Click the **Save** button.
    Your settings are saved. The instance displays on the Instances page.

Edit a PTP instance

To edit a PTP instance on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Settings**.
   The Settings page displays.
3. Select the checkbox next to the instance you want to edit and click the **Edit** button.
   The Edit PTP Instance page displays.
4. In the **Name** field, enter a name of up to 32 characters for this instance.
5. To enable this instance, click the **Admin Mode** toggle so that it is positioned to the right.
   Admin Mode is enabled by default.
6. From the **Network** menu, select the network to associate with this instance.
7. From the **VLAN** menu, select the VLAN to associate with this instance:
   The Ports field automatically populates with the enabled ports from the selected VLAN.
8. To manually select ports, click the **Ports** menu and select one or more ports.

9. From the **PTPv2 / AVB gPTP Profile** menu, select one of the following profiles:
   - **Default**: The default PTPv2 settings are used. This is the default setting.
   - **AES67**: A clock profile for connecting audio devices over a common PTP profile.
   - **SMPTE-2059-2**: A clock profile for video traffic.
   - **AES-R16-2016**: A clock profile that interoperates between SMPTE and AES67 clock profiles.
   - **802.1AS AVB**: A clock profile for audio video bridging (AVB).

   Selecting a profile automatically sets the default values for the timing and transport settings. Some settings are read-only depending on the profile selected.
10. In the **Local Clock Priority 1** field, enter a value between 0 and 255. The default value is 32. The priority 1 determines which switch that is capable of functioning as a grandmaster clock is elected to be the active grandmaster clock in the network.
11. In the **Local Clock Priority 2** field, enter a value between 0 and 255. The default value is 32. The priority 2 also determines which switch that is capable of functioning as a grandmaster clock is elected to be the active grandmaster clock in the network.
12. In the **Announce Interval** field, enter the period between successive Announce messages in logarithm to base 2 format.
    Announce messages help to elect the best grandmaster clock in the network. The following are the supported ranges and default settings for the PTP clock profiles:
    - **Default**: 0 to 4. The default setting is 1.
    - **AES67**: 0 to 4. The default setting is 1.
    - **SMPTE-2059-2**: –3 to 1. The default setting is 0.
    - **AES-R16-2016**: 0 or 1. The default setting is 0.
    - **802.1AS AVB**: –5 to 5. The default setting is 0.
13. In the **Announce Timeout**, enter the number of Announce messages that are not acknowledged before the switch determines that the grandmaster clock is not transmitting. You can enter a number from 2 to 10. The default setting for all PTP clock profiles is 3. For the AES-R16-2016 profile, the only possible value is 3.
14. In the **Sync Interval** field, enter the period between successive Sync messages, in logarithm to base 2 format.
    The following are the supported ranges and default settings for the PTP clock profiles:
    - **Default**: –1 to 1. The default setting is 0.
    - **AES67**: –4 to 1. The default setting is –3.
    - **SMPTE-2059-2**: –7 to –1. The default setting is –3.
    - **AES-R16-2016**: –4 to 1. The default setting is –3.
    - **802.1AS AVB**: –5 to 5. The default setting is –3.

15. In the **Delay-request Interval** or **Initial Pdelay Interval** (802.1AS only) field, enter the period between successive Delay-Request messages from the boundary clock to the grandmaster clock, in logarithm to base 2 format.
    Delay-request messages help to calculate the path delay. The following are the supported ranges and default settings for the PTP clock profiles:
    - **Default**: 0 to 5. The default setting is 0.
    - **AES67**: –3 to 5. The default setting is 0.
    - **SMPTE-2059-2**: –7 to 4. The default setting is –3.
    - **AES-R16-2016**: –4 to 5. The default setting is –3.
    - **802.1AS AVB**: –5 to 5. The default setting is 0.
16. From the **Transport** menu, set the transport protocol for use on the communication path. Select from one of the following options:
    - **IPv4**: The **IPv4** field displays. You can enter an IPv4 address in the **IPv4** field.
    - L2 Transport.

    This setting is read-only for AES67, SMPTE-2059-2, AES-R16-2016, and 802.1AS profiles.
17. In the **PTP Domain** field, enter a PTP domain number. The allowed range is 0 to 127. The default value is 0, except for SMPTE-2059-2 profiles where the default is 127.
18. From the **PTP Version** menu, select **2.0**.
19. Click the **Save** button.
    Your settings are saved. The instance displays on the Instances page.

Delete a PTP instance

To delete a PTP instance from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Settings**.
   The Settings page displays.
3. Select the checkbox next to the instance you want to delete.
4. Click the **Delete** button.
   The Delete PTP Instance page displays.
5. Click the **DELETE** button.
   The instance is removed from the controller.

View the PTP status page

The Status page displays the status of all configured PTP profiles.

To view the PTP status on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Status**.
   The PTP Status page displays.
3. Select a PTP domain to view the following information:
   - **Clock Identity**: The unique identifier of the clock.
   - **Clock Role Type**: Whether the clock is acting as master or slave.
   - **Clock Class**: The class of the clock (indicates its quality/traceability).
   - **Device Profile**: The PTPv2 profile configured for the instance.
   - **Priority 1/2**: The first and second priority value.
   - **Operation Mode**: The operational mode for the instance.
   - **Domain**: The PTP domain number for the instance.
   - **Accuracy**: The clock accuracy for the instance.
   - **Mean Path Delay**: The measured mean path delay between master and slave.

View the PTP statistics

The Statistics page displays the statistics of all ports, including those for PTP-disabled ports.

To view the PTP port statistics on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Statistics**.
   The Statistics page displays.

3. You can view the following information for each port on the controller:
   - **Port Number**: The port number, ranging from 1 to 6.
   - **ANNOUNCE**: The number of PTP announce messages sent and received on this port. Announce messages advertise the clock properties of a PTP device to other devices on the network.
   - **SYNC**: The number of PTP sync messages sent and received on this port. Sync messages are used to synchronize the local clock with the master clock.
   - **FOLLOW_UP**: The number of PTP follow-up messages sent and received on this port. Follow-up messages carry the precise timestamp of the corresponding sync message.
   - **DELAY_REQ**: The number of PTP delay-request messages sent and received on this port. Delay-request messages are used to measure the propagation delay between the local clock and the master clock.

View and manage PTP logs

The PTP Logs page displays log messages generated by the PTP service, including the time, severity, and message for each entry. To view and manage PTP logs on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > PTP > Logs**.
   The Logs page displays. The log table shows the following information for each entry:
   - **Time**: The date and time the log entry was generated.
   - **Severity**: The severity level of the log entry.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: A description of the event.
3. To search for a specific log entry, enter a search term in the **Search** field.
4. To filter the log entries, click the **Filter** button and select the criteria you want to apply.

5. To download the log entries to your computer, click the **Download** button.
   The log entries download as a file to your computer.
6. To reload the log entries with the latest data, click the **Refresh** button.
7. To clear all log entries, click the **Clear All** button.
   All log entries are permanently removed from the Logs page.

Manage the syslog server

The controller includes a built-in syslog server that collects and stores log messages from devices on your network. The syslog server is disabled by default.
The syslog server supports TCP, UDP, and TCP TLS protocols. You can configure the port number for each protocol and select a TLS certificate for secure connections. Log messages can be stored on the internal storage or on an external SSD.

NOTE: The message summary, top five clients, and message chart data are stored in RAM and reset when the controller restarts.

Enable or disable the syslog server

The syslog server is disabled by default.

To enable or disable the syslog server on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > Syslog > Settings**.
   The Syslog Settings page displays.
3. Click the **Syslog Service** toggle to enable or disable the syslog server:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
4. Click the **Apply** button.
   Your settings are saved.

Display the syslog server overview

See Enable or disable the syslog server on page 69 to enable the syslog on your controller.

To view the syslog settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > Syslog**.
   The Overview page displays.
3. The Server section displays the status of the Syslog server. The Syslog server status can be Running or Stopped.
4. The Log Statistics section displays the following information:
   - **Last Hour**: Total messages received in the last hour.
   - **Last 24 Hours**: Total messages received in the last 24 hours.
   - **Hosts**: Total syslog clients sending logs to this server.
5. The Top 5 Clients By Logs section displays the five clients sending the most logs to the server. You can filter the information by the following:
   - Last Hour.
   - Last 24 hrs.
   - Last 7 days.

   The log includes all warning, critical, and error messages.
6. The Messages section displays statistics for the last 24 hours, collected every 10 minutes, or for the last 7 days, collected hourly.
   The log includes all emergency, alert, critical, error, warning, notice, info, and debug messages.
   You can filter the Message section by priority, by host, or by app.

7. The Events section displays the recent events on the controller relating to the syslog service. The table displays the following information:
   - **Time**: The date and time the event was generated
   - **Severity**: The severity level of the event.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: The details of the event notification.

Configure the syslog server settings

To configure the syslog server settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > Syslog > Settings**.
   The Syslog Settings page displays.
3. To enable or disable TCP protocol, click the **TCP Protocol** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right, then enter a port number in the **TCP Port** field. The default port is 514. The allowed range is 1 to 65535.
   - **Disable**: Click the toggle so that it is positioned to the left.
4. To enable or disable UDP protocol, click the **UDP Protocol** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right, then enter a port number in the **UDP Port** field. The default port is 514. The allowed range is 1 to 65535.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. To enable or disable TCP TLS protocol, click the **TCP TLS Protocol** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right, then enter a port number in the **TCP TLS Port** field. The default port is 6514. The allowed range is 1 to 65535.
   - **Disable**: Click the toggle so that it is positioned to the left.

6. If TCP TLS is enabled, from the **Certificate** menu, select the TLS certificate to use for secure connections.
   You can manage the certificates in **Settings > Configuration > Certificate Management**.
7. To set the file storage location, click the **File Location** field and select a location.
   Select **Internal** to store logs in the internal storage at /syslog-server/, or select **SSD** to store logs on an external SSD and specify a path.
8. Click the **Apply** button.
   Your settings are saved.

View and manage syslog logs

The Logs page displays log messages collected by the syslog server. The page displays the most recent 2,000 messages and supports up to 5,000 pages of log entries.

To view and manage syslog logs on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > Syslog > Logs**.
   The Syslog Logs page displays a chart of message count over time and a table of log entries. By default, the chart shows data for the past 7 days.
3. To search for a specific log entry, enter a search term of up to 64 characters in the **Search** field.
   The search applies only to log entries already loaded in the browser.

4. To filter the log entries, click the **Filter** icon and configure the following as needed:
   - **Severity**: The severity level of the log entry.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **App Name**: Select one or more application names to filter by. Up to 10 selections are allowed.
   - **Hostname**: Select one or more hostnames to filter by. Up to 10 selections are allowed.
   - **Time**: Select a start and end time to filter log entries by time range. Selection is limited to the past 7 days in hourly increments.

   Click **Apply** to apply the selected filters, or click **Clear** to remove all filter selections.
5. To sort the log entries, click a column header.
   Sorting applies only to log entries already loaded in the browser.
6. To reload the log entries with the latest data, click the **Refresh** button.
7. To clear all log entries, click the **Clear All** button.
   All log entries are permanently removed from storage.

Manage the NTP server

The controller includes a built-in NTP server that provides time synchronization to devices on your network. The NTP server is disabled by default.
The controller can also act as an SNTP client, synchronizing its own clock with up to five external NTP sources. When auto sync is enabled, the controller automatically synchronizes with the configured NTP sources.

Enable or disable the NTP server

The NTP server is disabled by default.

To enable or disable the NTP server on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > NTP > Settings**.
   The NTP Settings page displays.
3. Click the **NTP Server** toggle to enable or disable the NTP server:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
4. Click the **Apply** button.
   Your settings are saved.

Display the NTP server overview

See Enable or disable the NTP server on page 73 to enable NTP on your controller.

To view the NTP server overview on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > NTP**.
   The Overview page displays.
3. The Server section displays the status of the controller indicating whether the NTP server is Running or Stopped.
4. The Information section displays the following information:
   - **Current Time**: The current time on the controller.
   - **Time Zone**: The time zone configured on the controller.
5. The Client section displays the following information:
   - **Time Source**: The NTP server that the NTP client is currently synchronized with.
   - **Last Synced**: The date and time when the NTP client last synchronized with the NTP server.
6. The NTP Packets section displays a chart of NTP packets received and dropped per minute over the past 24 hours.

7. The Events section displays recent events relating to the NTP server. The table displays the following information:
   - **Time**: The date and time the event was generated
   - **Severity**: The severity level of the event.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: The details of the event notification.

Configure the NTP server settings

To configure the NTP server settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > NTP > Settings**.
   The NTP Settings page displays.
3. If you have not already enabled the NTP server, click the **NTP Server** toggle to enable or disable the NTP server:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
4. To enable or disable logging, click the **Enable Logging** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. To enable or disable the SNTP client, click the **Enable SNTP Client** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right. The **NTP Sources** options display.
   - **Disable**: Click the toggle so that it is positioned to the left. The NTP Sources option is hidden.

6. If the SNTP client is enabled, to enable or disable auto sync, click the **Enable Auto Sync** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
7. If the SNTP client is enabled, in the **NTP Sources** field, enter the FQDN address of an external NTP server.
   You can configure up to four NTP sources. Each address must be in FQDN format with a maximum length of 255 characters. The default NTP source address is time-a.netgear.com.
8. To enable or disable the local reference clock, click the **Enable LOCAL Reference Clock** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right, then select a stratum level from the **LOCAL Stratum** menu. The allowed range is Stratum 1 to Stratum 15. The default is Stratum 10.
   - **Disable**: Click the toggle so that it is positioned to the left.
9. Click the **Apply** button.
   Your settings are saved.

Manage the DNS server

The controller includes a built-in DNS server that resolves domain names to IP addresses for devices on your network. The DNS server is disabled by default.
The DNS server supports forward and reverse zones, and can act as a primary or secondary DNS server for each zone. You can configure the DNS server to forward queries to external DNS servers and to respond to recursive queries from clients.

Enable or disable the DNS server

The DNS server is disabled by default.

To enable or disable the DNS server on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS**.
   The DNS Overview page displays.
3. Select **Settings**.
   The DNS Settings page displays.

4. Click the **DNS Server** toggle to enable or disable the DNS server:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. Click the **Apply** button.
   Your settings are saved.

Display the DNS server overview

See Enable or disable the DNS server on page 76 to enable the DNS on your controller.

To view the DNS server overview on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS**.
   The Overview page displays.
3. The Server section displays the status of the DNS server. The DNS server status can be Running or Stopped.
4. The Zone Overview section displays the following information:
   - The total number of user-configured zones, including primary and secondary zones.
5. The Zone Management section lists all zones, type, and status of each zone.
6. The Events section displays the five most recent log messages generated by the DNS server.

Configure the DNS server settings

To configure the DNS server settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS**.
   The DNS Overview page displays.
3. Select **Settings**.
   The DNS Settings page displays.

4. To enable or disable logging, click the **Enable Logging** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right. Logging is enabled by default.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. To enable or disable recursive queries, click the **Recursive Queries** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right. Recursive queries are enabled by default.
   - **Disable**: Click the toggle so that it is positioned to the left.
6. In the **Forwarders** field, enter the IP address of an external DNS server to forward queries to. To add another forwarder, click the **Add Forwarder** button.
   You can configure up to four forwarder IP addresses.
7. Click the **Apply** button.
   Your settings are saved.

Add a DNS zone

A DNS zone defines the portion of the DNS namespace that the controller manages. The controller supports up to eight zones.

To add a DNS zone on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS > Zone Management**.
   The Zone Management page displays.
3. Click the **Add** button.
   The Add Zone page displays.

   NOTE: The **Add** button displays the number of zones out of the maximum of eight.
4. In the **Zone Name** field, enter a name for the zone.
5. From the **Domain Type** menu, select one of the following:
   - **Forward**: Resolves domain names to IP addresses. The zone name can be up to 253 characters and can contain letters, digits, and hyphens. Hyphens cannot appear as the first or last character of a label.
   - **Reverse**: Resolves IP addresses to domain names. The zone name can be up to 15 characters and must use the *in-addr.arpa.* suffix format.

6. From the **Zone Type** menu, select one of the following:
   - **Primary**: The controller is the authoritative source for this zone. You can optionally enter an IPv4 address in the **Primary DNS Server** field. You can optionally enter up to three IP addresses in the **Allow Transfer To** field to permit zone transfers to secondary DNS servers.
   - **Secondary**: The controller receives zone data from a primary DNS server. Enter up to three IP addresses in the **Master Server(s)** field.
7. Click the **ADD ZONE** button.
   The zone is saved and the Zone Management page displays.
   When you add a forward primary zone, the controller automatically creates the following resource records in the zone: an SOA record, an A record for the name server, and an NS record.
   When you add a reverse primary zone, the controller automatically creates an SOA record and an NS record in the zone.

Edit a DNS zone

To edit a DNS zone on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS > Zone Management**.
   The Zone Management page displays.
3. Select the checkbox next to the zone you want to edit and click the **Edit** button.
   The Edit Zone page displays.
4. In the **Zone Name** field, enter a name for the zone.
5. From the **Domain Type** menu, select one of the following:
   - **Forward**: Resolves domain names to IP addresses. The zone name can be up to 253 characters and can contain letters, digits, and hyphens. Hyphens cannot appear as the first or last character of a label.
   - **Reverse**: Resolves IP addresses to domain names. The zone name can be up to 15 characters and must use the *in-addr.arpa.* suffix format.

6. From the **Zone Type** menu, select one of the following:
   - **Primary**: The controller is the authoritative source for this zone. You can optionally enter an IPv4 address in the **Primary DNS Server** field. You can optionally enter up to three IP addresses in the **Allow Transfer To** field to permit zone transfers to secondary DNS servers.
   - **Secondary**: The controller receives zone data from a primary DNS server. Enter up to three IP addresses in the **Master Server(s)** field.
7. Click the **SAVE** button.
   Your settings are saved and the Zone Management page displays.

Delete a DNS zone

To delete a DNS zone from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS > Zone Management**.
   The Zone Management page displays.
3. Select the checkbox next to the zone you want to delete.
4. Click the **Delete** button.
   The Confirm Deletion page displays.
5. Click the **DELETE** button.
   The zone and all its resource records are removed from the controller.

Add a resource record

A resource record defines how the DNS server responds to queries for a specific name or address within a zone. Each zone supports up to 2,000 manually added resource records.

To add a resource record on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS > Resource Records**.
   The Resource Records page displays.
3. From the **Zone** list, select the zone to which you want to add a record.
   The resource records for the selected zone display.

4. Click the **Add** button.
   The Add Zone Resource Records page displays.
5. In the **Name** field, enter a name for the zone resource record of up to 63 characters. Use letters, numbers, hyphens, or @ for zone apex.
6. From the **Type** menu, select the type of resource record to add:
   For forward zones, the available record types are as follows:
   - **A**: Maps a name to up to five IPv4 addresses.
   - **CNAME**: Maps a name to an FQDN alias.
   - **NS**: Specifies a name server for a domain.
   - **MX**: Specifies up to three mail exchange servers for a domain.
   - **TXT**: Associates text with a name.
   - **SRV**: Specifies the location of services within a domain.
   - **SOA**: Defines the start of authority for the zone. Only one SOA record is allowed per zone.

   For reverse zones, the available record types are NS, PTR, and SOA.
7. Enter the name and target values for the record type:
   - **A**: Enter a name of up to 32 characters and up to five IPv4 addresses.
   - **CNAME**: Enter a name of up to 32 characters and a target FQDN of up to 64 characters.
   - **NS**: Enter a domain name of up to 32 characters and a target FQDN of up to 64 characters.
   - **MX**: Enter a domain name of up to 32 characters and up to three target FQDNs of up to 64 characters each.
   - **TXT**: Enter a name of up to 32 characters and a text value of up to 64 characters.
   - **PTR**: Enter an IP address of up to 32 characters and a target FQDN of up to 64 characters.
   - **SRV**: Enter a name in the format *_service._protocol* of up to 64 characters, a priority value from 0 to 65535, a weight value from 0 to 65535, a port number from 0 to 65535, and up to three target FQDNs.
8. In the **TTL** field, enter the time-to-live value in seconds.
   The allowed range is 60 to 86,400 seconds. The default value is 3,600 seconds.
9. In the **Target** field, enter an IPv4 address.
   You can add up to five target addresses. To add another target address click the **Add Target Address** button.
10. Click the **ADD RECORD** button.
    The resource record is saved and the Resource Records page displays.

Edit a resource record

To edit a resource record on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS > Resource Records**.
   The Resource Records page displays.
3. From the **Zone** list, select the resource record for which you want to edit a record.
   The resource records for the selected zone display.
4. Click the **Edit** button.
   The Edit Zone Resource Records page displays.
5. In the **Name** field, enter a name for the zone resource record of up to 63 characters. Use letters, numbers, hyphens, or @ for zone apex.
6. From the **Type** menu, select the type of resource record to add:
   For forward zones, the available record types are as follows:
   - **A**: Maps a name to up to five IPv4 addresses.
   - **CNAME**: Maps a name to an FQDN alias.
   - **NS**: Specifies a name server for a domain.
   - **MX**: Specifies up to three mail exchange servers for a domain.
   - **TXT**: Associates text with a name.
   - **SRV**: Specifies the location of services within a domain.
   - **SOA**: Defines the start of authority for the zone. Only one SOA record is allowed per zone.

   For reverse zones, the available record types are NS, PTR, and SOA.

7. Enter the name and target values for the record type:
   - **A**: Enter a name of up to 32 characters and up to five IPv4 addresses.
   - **CNAME**: Enter a name of up to 32 characters and a target FQDN of up to 64 characters.
   - **NS**: Enter a domain name of up to 32 characters and a target FQDN of up to 64 characters.
   - **MX**: Enter a domain name of up to 32 characters and up to three target FQDNs of up to 64 characters each.
   - **TXT**: Enter a name of up to 32 characters and a text value of up to 64 characters.
   - **PTR**: Enter an IP address of up to 32 characters and a target FQDN of up to 64 characters.
   - **SRV**: Enter a name in the format *_service._protocol* of up to 64 characters, a priority value from 0 to 65535, a weight value from 0 to 65535, a port number from 0 to 65535, and up to three target FQDNs.
8. In the **TTL** field, enter the time-to-live value in seconds.
   The allowed range is 60 to 86,400 seconds. The default value is 3,600 seconds.
9. In the **Target** field, enter an IPv4 address.
   You can add up to five target addresses. To add another target address click the **Add Target Address** button.
10. Click the **SAVE** button.
    The resource record is saved and the Resource Records page displays.

Delete a resource record

To delete a resource record from your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > DNS > Resource Records**.
   The Resource Records page displays.
3. From the **Zone** list, select the zone that contains the record you want to delete.
   The resource records for the selected zone display.
4. Select the checkbox next to the record you want to delete.
5. Click the **Delete** button.
   The Confirm Deletion page displays.
6. Click the **DELETE** button.
   The resource record is removed from the zone.

Manage the HTTPS server

The controller uses HTTPS to secure the connection between the device and your web browser. The HTTPS service runs by default and cannot be disabled.
You can configure the TLS certificate used for the HTTPS connection, set the login session timeout, and enable or disable logging. Certificates are managed separately under **Settings > Configuration > Certificate Management**.

Display the HTTPS server overview

To view the HTTPS service overview on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > HTTPS**.
   The HTTPS Overview page displays.
3. The Server section displays the status of the HTTPS service. The HTTPS service status can be Running or Stopped.
4. The Certificate Information section displays the following details about the certificate in use:
   - **Valid To**: The expiration date of the certificate.
   - **Issuer**: The issuer of the certificate. If the certificate is self-signed, this field displays **self-sign**.
5. The Last Login Information table displays the following information:
   - **User name**: The name of the user that logged in.
   - **IP Address**: The IP address used to log in.
   - **Login Time**: The time of the login.
   - **Success Result**: The status can be Success or Failed.

Configure the HTTPS service settings

To configure the HTTPS service settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > HTTPS > Settings**.
   The HTTPS Settings page displays.

3. To enable or disable logging, click the **Enable Logging** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right. Logging is enabled by default.
   - **Disable**: Click the toggle so that it is positioned to the left.
4. In the **Login Session Timeout** field, enter the number of minutes before an inactive login session times out.
   The allowed range is 1 to 1,440 minutes. The default value is 30 minutes.
5. From the **Select Certificate** menu, select the TLS certificate to use for the HTTPS connection.
   Certificates are managed under **Settings > Configuration > Certificate Management**. For more information, see Manage certificates on the controller on page 99.
6. Click the **Apply** button.
   Your settings are saved.

View and manage HTTPS logs

The Logs page displays log messages generated by the HTTPS service, including the time, severity, and message for each entry. To view and manage HTTPS logs on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > HTTPS**.
   The HTTPS Overview page displays.

3. Select **Logs**.
   The Logs page displays. The log table shows the following information for each entry:
   - **Time**: The date and time the log entry was generated.
   - **Severity**: The severity level of the log entry.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: A description of the event.
4. To search for a specific log entry, enter a search term in the **Search** field.
5. To filter the log entries, click the **Filter** button and select the criteria you want to apply.
6. To download the log entries to your computer, click the **Download** button.
   The log entries download as a file to your computer.
7. To reload the log entries with the latest data, click the **Refresh** button.
8. To clear all log entries, click the **Clear All** button.
   All log entries are permanently removed from the Logs page.

Manage the mDNS server

The controller includes a built-in multicast DNS (mDNS) server that allows devices on your network to discover the controller and its services without requiring a dedicated DNS server. The mDNS server is disabled by default.
The controller advertises its HTTPS service on the local network using the mDNS protocol. Devices on the same network can discover the controller by its hostname followed by .local.

Enable or disable the mDNS server

The mDNS server is disabled by default.

To enable or disable the mDNS server on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > mDNS > Settings**.
   The Settings page displays.
3. Click the **mDNS Service** toggle to enable or disable the mDNS server:
   - **Enable**: The toggle is positioned to the right.
   - **Disable**: The toggle is positioned to the left. This is the default setting.
4. Click the **Apply** button.
   Your settings are saved. After you enable the mDNS server, you can view the mDNS server overview on the Overview page.

Display the mDNS server overview

See Enable or disable the mDNS server on page 86 to enable mDNS on your controller.

To view the mDNS server overview on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > mDNS**.
   The mDNS Overview page displays.
3. The Server section displays the status of the mDNS service. The mDNS service status can be Running or Stopped.
4. The Information section displays the following details:
   - **Hostname**: The hostname of the controller on the local network, displayed with the .local suffix.
   - **Registered Service**: The services advertised by the controller on the local network. The controller currently advertises the HTTPS service as _https._tcp.

5. The Events section displays recent events relating to the mDNS service. The table displays the following information:
   - **Time**: The date and time the event was generated
   - **Severity**: The severity level of the event.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: The details of the event notification.

Configure the mDNS server settings

To configure the mDNS server settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > mDNS**.
   The mDNS Overview page displays.
3. Select **Settings**.
   The mDNS Settings page displays.
4. Click the **mDNS Service** toggle to enable or disable the mDNS service:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. In the **mDNS Hostname** field, enter a hostname for the controller.
   The hostname can contain up to 63 alphanumeric characters and hyphens. The mDNS domain name is set to **local** and cannot be changed.
6. To enable or disable logging, click the **Enable Logging** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
7. In the **mDNS Hostname** field, enter a hostname of up to 63 characters.

8. The **mDNS Domain Name** field is read-only.
9. Click the **Apply** button.
   Your settings are saved.

View and manage mDNS logs

The Logs page displays log messages generated by the mDNS service, including the time, severity, and message for each entry. To view and manage mDNS logs on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > mDNS**.
   The mDNS Overview page displays.
3. Select **Logs**.
   The Logs page displays. The log table shows the following information for each entry:
   - **Time**: The date and time the log entry was generated.
   - **Severity**: The severity level of the log entry.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: A description of the event.
4. To search for a specific log entry, enter a search term in the **Search** field.
5. To filter the log entries, click the **Filter** button and select the criteria you want to apply.
6. To download the log entries to your computer, click the **Download** button.
   The log entries download as a file to your computer.
7. To reload the log entries with the latest data, click the **Refresh** button.
8. To clear all log entries, click the **Clear All** button.
   All log entries are permanently removed from the Logs page.

Manage the LLDP service

The controller supports the Link Layer Discovery Protocol (LLDP), which allows network devices to advertise their identity and capabilities to neighboring devices on the same network. The controller uses LLDP to discover connected devices and to support features such as Auto-Trunk and Auto-LAG.
The LLDP service is enabled by default on all ports. You can configure the transmit interval, hold time, and system description, and enable or disable LLDP on individual ports.

Enable or disable LLDP server

By default, the LLDP service setting is enabled.

To enable or disable the LLDP global settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > LLDP**.
   The LLDP Overview page displays.
3. Select **Settings**.
   The LLDP Settings page displays.
4. Click the **LLDP Service** toggle to enable or disable the LLDP service:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. Click the **Apply** button.
   Your settings are saved.

Display the LLDP server overview

To view the LLDP service overview on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > LLDP**.
   The LLDP Overview page displays.
3. The Server section displays the status of the LLDP service. The LLDP service status can be Running or Stopped.

4. The System Information section displays the following details:
   - **Chassis ID**: The chassis ID of the controller, which corresponds to the MAC address of Port 1.
   - **System Name**: The hostname of the controller.
   - **System Description**: The system description as configured by the user.
5. The LLDP Neighbor section displays the neighboring devices connected to each port as discovered by the LLDP protocol. The table can display the following information:
   - **Port**: The port on the controller to which the neighbor is connected.
   - **System Name**: The hostname of the neighboring device.
   - **Chassis ID**: The chassis ID of the neighboring device.
   - **Port ID**: The port ID of the neighboring device.
   - **Port Description**: The port description of the neighboring device.
   - **Management IP**: The management IP address of the neighboring device.

   To select which columns to display, click the column selection icon and select the information you want to show.
6. The Port Status section displays the LLDP status for each port, indicating whether LLDP is enabled or disabled.
7. The Events section displays the six most recent events relating to the LLDP service. The table displays the following information:
   - **Time**: The date and time the event was generated
   - **Severity**: The severity level of the event.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: The details of the event notification.

Configure the LLDP global settings

To configure the LLDP global settings on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > LLDP > Settings**.
   The LLDP Settings page displays.
3. If you disabled the LLDP service, click the **LLDP Service** toggle to enable the LLDP service:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
4. To enable or disable logging, click the **Enable Logging** toggle:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.
5. In the **Transmit Interval** field, enter the interval in seconds at which the controller sends LLDP packets.
   The allowed range is 5 to 32,768 seconds. The default value is 30 seconds.
6. In the **Hold Time Multiplier** field, enter the hold time multiplier value.
   The hold time multiplier determines how long a receiving device retains LLDP information before discarding it. The allowed range is 2 to 10. The default value is 4.
7. In the **System Description** field, enter a description for the controller of up to 255 characters.
   The default value is the product description and firmware version.
8. Click the **Apply** button.
   Your settings are saved.

Configure the LLDP port settings

To configure the LLDP settings for individual ports on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > LLDP > Port Settings**.
   The Port Settings page displays a table listing all six ports on the controller.
3. For each port you want to configure, click the **LLDP Enable** toggle to enable or disable LLDP on that port:
   - **Enable**: Click the toggle so that it is positioned to the right.
   - **Disable**: Click the toggle so that it is positioned to the left.

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

View and manage LLDP logs

The Logs page displays log messages generated by the LLDP service, including the time, severity, and message for each entry.

To view and manage LLDP logs on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Services > LLDP**.
   The LLDP Overview page displays.
3. Select **Logs**.
   The Logs page displays. The log table shows the following information for each entry:
   - **Time**: The date and time the log entry was generated.
   - **Severity**: The severity level of the log entry.
     - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error**: Level 3, a device error occurred, such as a port being offline.
     - **Warning**: Level 4, the lowest level of a device warning.
     - **Notice**: Level 5, provides the network administrators with device information.
     - **Informational**: Level 6, provides device information. This is the default setting.
     - **Debug**: Level 7, provides detailed information about the log.
   - **Message**: A description of the event.
4. To search for a specific log entry, enter a search term in the **Search** field.
5. To filter the log entries, click the **Filter** button and select the criteria you want to apply.
6. To download the log entries to your computer, click the **Download** button.
   The log entries download as a file to your computer.
7. To reload the log entries with the latest data, click the **Refresh** button.

8. To clear all log entries, click the **Clear All** button.
   All log entries are permanently removed from the Logs page.

Maintenance

This chapter includes the following sections:

- LCD display overview
- Manage certificates on the controller
- Manage firmware on the controller
- Manage the Engage version on your controller
- Manage the controller's stored files
- Manage the SSD storage
- Manage the configuration file
- Return the controller to its factory default settings

LCD display overview

The controller includes a front-panel LCD touchscreen that displays the current system status and lets you view information, configure settings, and view notifications directly on the device. The LCD display shows one of the following screens depending on the current state of the controller:

Table 12.LCD display screens

Screen	Description
Main screen	The controller is fully operational. The LCD display shows the port dashboard with link status, link speed, and connection indicators. Use the touch icons to navigate to Information, Settings, and Notifications.
Setup Required	The controller has not been configured yet. Visit 192.168.1.250 to complete the setup.
Booting	The controller is booting up and applying its configuration. User interaction with the LCD display is not possible during this time.
Firmware Upgrade	A firmware update is being installed. Do not power off the controller during this process.
Critical Error	A system error has occurred. Check the LCD display for details. Possible errors include: • Secure Boot is disabled. • The Secure Boot keys are not provisioned with NETGEAR. • An invalid firmware signature was detected.

When the screen turns off, touch anywhere on the screen to reactivate it and return to the main screen.

View the LCD display main screen

The main screen displays the port dashboard and provides access to all other sections of the LCD display. To navigate the LCD display main screen on your controller:

1. If the screen is off, touch anywhere on the screen to wake it.
   The main screen displays.
2. The port area displays the status of each port. The following indicators are shown for each port:
   - A green outline around the port indicates a connected link.
   - A blue outline around the port indicates the connected device is powered by PoE.
   - The port displays the link speed when connected: **1G**, **2.5G**, or **10G**.
   - The port color corresponds to the network profile assigned to that port.
3. To view the IP address and details for a specific port, tap the **port** icon.
   The port details display in the information area.
4. The date and time display in the information area when no port is selected.
5. To navigate to a section of the LCD display, tap one of the following icons in the navigation area:
   - **Home** icon: Returns to the main screen.
   - **Information** icon: Displays system information, hardware metrics, network usage, and a support QR code.
   - **Settings** icon: Displays display and date and time settings.
   - **Notification** icon: Displays unread notifications.

   Swipe the navigation area up or down to scroll through the available icons.
6. To turn off the screen, tap the screen off icon in the upper-right corner of the display.

View system information on the LCD display

The Information section displays system details, hardware metrics, and network usage for the controller. To view system information on the LCD display of your controller:

1. If the screen is off, touch anywhere on the screen to wake it.
   The main screen displays.
2. Tap the **Information** icon in the navigation area.
   The System Information page displays. Swipe left or right to move between the following pages.

3. The System Information page displays the following details. Scroll up or down to view all information:
   - Firmware version
   - Engage version
   - LCD firmware version
   - MAC address
   - Uptime
   - Serial number
   - Model name
4. Swipe left to view the hardware metrics page, which displays the following information, refreshed every two seconds:
   - **CPU**: CPU loading as a percentage.
   - **RAM**: Memory usage as a percentage.
   - **Sensor 1, 2, 3**: Temperature readings from each sensor in degrees Celsius.
   - **Fan**: Fan speed in RPM. If the fan speed is 0 RPM, the display shows IDLE.
5. Swipe left again to view the Network Usage page. For more information, see View network usage on the LCD display on page 97.
6. Swipe left again to view the About page, which displays a QR code. Scan the QR code to access the NETGEAR support site at netgear.com/support/enterprise.

View network usage on the LCD display

The Network Usage page displays real-time traffic statistics for each port on the controller, refreshed every second. To view network usage on the LCD display of your controller:

1. If the screen is off, touch anywhere on the screen to wake it.
   The main screen displays.
2. Tap the **Information** icon in the navigation area.
   The System Information page displays.
3. Swipe left to navigate to the Network Usage page.
   The Network Usage page displays traffic statistics for the selected port.
4. To view the statistics for a different port, tap the port number in the upper-right corner of the page and select the port you want to view.

View notifications on the LCD display

The Notifications section displays unread notifications on the controller, with the most recent notification first. The controller supports up to 2,000 unread notifications. To view notifications on the LCD display of your controller:

1. If the screen is off, touch anywhere on the screen to wake it.
   The main screen displays.
2. Tap the **Notification** icon in the navigation area.
   The Device Notification page displays a list of unread notifications. The total number of unread notifications displays in the upper-right corner of the page.
3. Scroll up or down to browse the notification list.
4. To view the details of a notification, tap the notification.
   The notification details display.
5. Tap **OK** to return to the notification list.
6. To refresh the notification list, tap the **Refresh** icon in the upper-right corner of the page.

Configure the LCD auto-screen display settings

You can configure the auto screen off time for the LCD display. To configure the LCD display settings on your controller:

1. If the screen is off, touch anywhere on the screen to wake it.
   The main screen displays.
2. Tap the **Settings** icon in the navigation area.
   The Display Settings page displays.
3. Tap the auto screen off time and select one of the following options:
   - **5 Mins**
   - **10 Mins**
   - **15 Mins** (default)
   - **30 Mins**
   - **1 Hour**
   - **2 Hours**
   - **4 Hours**

   The auto screen off timer resets each time you touch the screen.

Set the date and time on the LCD display

You can set the system date, time, and time zone directly from the LCD display. To set the date and time on the LCD display of your controller:

1. If the screen is off, touch anywhere on the screen to wake it.
   The main screen displays.
2. Tap the **Settings** icon in the navigation area.
   The Display Settings page displays.

3. Swipe left to navigate to the Date and Time Settings page.
4. To set the date, tap the **Date** field or icon.
   A scroll selector displays. The date format is YYYY-MM-DD.
5. Scroll to select the year, month, and day, then confirm your selection.
6. To set the time, tap the **Time** field or icon.
   A scroll selector displays. The time format is HH:MM AM/PM.
7. Scroll to select the hour, minute, and AM or PM, then confirm your selection.
8. To set the time zone, tap the **Time zone** field or icon and scroll to select the correct UTC offset.

Manage certificates on the controller

The controller uses TLS certificates to secure the HTTPS connection between the controller and your web browser.
By default, the controller uses a self-signed certificate, which causes browsers to display a security warning when you first connect. To remove this warning, you can import a CA-signed certificate from a trusted certificate authority. The Certificate Management page displays a table listing the certificates on the controller, including the default self-signed certificate. You can view the following information on the table:

- **Name**: The name of the certificate.
- **Issuer**: The certificate can be self-signed or imported.
- **Expires**: The expiration period by date and time in hours, minutes, and seconds.
- **Validity Start Time**: The start time of the certificate on the controller by date and time in hours, minutes, and seconds.

The controller supports up to three self-signed or imported certificates. You can download, delete, or re-generate certifications.

NOTE: You cannot delete the default server certificate.

Add a certificate

You can add a certificate by either importing a CA-signed certificate or generating a new self-signed certificate. The controller supports up to three certificates.

To add a certificate on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. Select **Settings > Configuration > Certificate Management**.
   The Certificate Management page displays.
3. Click the **Add** button.
   The Add Certificate page displays.

> **NOTE:** The **Add** button displays the number of certificates out of the maximum of three.

4. In the **Certificate Name** field, enter a name of up to 32 characters.
5. Select a certification type radio button:
   - **Import Certificate**: Click the **Upload Certificate** button to browse for a certificate file, or drag and drop the file into the upload area.
     The file must be in PEM format and must include both the private key and the certificate.
   - **Create Self-Signed Certificate**: The controller generates a new self-signed certificate.
6. Click the **ADD** button.
   The Certificate Management page displays the new certificate.

Delete a certificate

The controller supports up to three certificates. If the controller has three existing certificates, you must delete a certificate before you can add a new one.

To delete a certificate on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Certificate Management**.
   The Certificate Management page displays.
3. Select the certificate you want to delete.
4. Click the **Delete** button.
   The Confirm Delete page displays.
5. Click the **DELETE** button.
   Your settings are saved.

Download a certificate

To download a certificate from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Certificate Management**.
   The Certificate Management page displays.
3. Select the certificate you want to download.
4. Click the **Download** button.
   A pop-up message displays when the certificate downloads.

Re-generate a certificate

To re-generate a certificate on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Configuration > Certificate Management**.
   The Certificate Management page displays.
3. Select the certificate you want to re-generate.
4. Click the **Re-Generate** button.
   If the certificate is in use, a pop-up warning displays. You can re-generate the certificate in use by clicking the **Continue** button. Regenerating a certificate in use causes a brief disconnection.

Manage firmware on the controller

The controller supports dual firmware images, allowing it to store two firmware versions simultaneously. One version is active and runs the current firmware. The other version is inactive. You can change between firmware versions without performing a full reinstall.

Update to an installed firmware version

The controller can store two firmware versions at the same time. You can switch to the inactive firmware version without downloading a new version.

To update to an installed firmware on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. Select **Settings > Maintenance > Firmware Update**.
   The Firmware Update page displays.
   The Installed Firmware Versions section lists both firmware versions installed on the controller. The currently running version is indicated by the **Active** label.
3. Select the radio button for the inactive firmware version.
4. Click the **Apply** button.
   The controller restarts and runs the selected firmware version.

Update the controller firmware from a file

You can update the controller firmware by uploading a firmware image file from your local computer.

> ⚠ **CAUTION:** Updating the firmware this way requires the controller to reset to factory default.

To update the firmware on your controller from a file:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings**.
   The Settings page displays.
3. Select **Maintenance > Firmware Update**.
   The Firmware Update page displays.
4. In the Browse File field, click the **Upload** field and select the firmware image file on your local computer.
   The file name displays in the Browse File field.
5. Click the **Update Firmware** button.
   The Confirm Firmware Update window displays.
6. Click the **UPLOAD & UPDATE** button.
   The controller uploads the firmware file and writes it to the inactive installed firmware version. When the installation is complete, a two-minute countdown displays before the controller restarts.
7. Launch a web browser and enter the controller's default IP address 192.168.1.250 into the browser's address bar.

8. Continue the controller setup. For more information, see Set up the controller with the main UI on page 8.

Update the controller firmware from an online version

You can check for new firmware on the NETGEAR update server and download it directly to the controller.

NOTE: The controller must have internet access before you can update the firmware from an online version.

To update the firmware on your controller from the cloud:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings**.
   The Settings page displays.
3. Select **Maintenance > Firmware Update**.
   The Firmware Update page displays. The Firmware Update section shows the latest firmware information from the cloud.
4. If the page shows that no new firmware is available, click the **Check for Update** button to check the update server immediately.
5. When new firmware is available, click the **Download** button.
   The download progress displays on the page. You can also monitor the download in the Downloads area in the upper-right corner of the dashboard.
   To cancel the download, click the **Cancel** button and then click the **Confirm** button in the confirmation window that displays.
6. When the download is complete, click the **Update** button.
   A confirmation window displays.
7. Click the **Update** button to confirm.
   The controller installs the firmware and displays an updating window. When the installation is complete, a two-minute countdown displays before the controller restarts.

Manage the Engage version on your controller

You can manage the version of Engage from your controller. We recommend using the latest version of Engage on your controller.

Update Engage on your controller

To update Engage on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Maintenance > Engage**.
   The Engage page displays.
   The Installed Firmware Versions section lists the Engage version installed on the controller.
3. In the Engage Update section, if an update is available, click the **Check for Update** button.
4. Download the latest Engage version on your computer.
5. Click the **Upload** button and select the downloaded version of Engage.
6. Click the **Update Engage** button.
   Your Engage version updates.

Reset Engage to the default state

To reset Engage to the default state on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Maintenance > Engage**.
   The Engage page displays.
3. In the Reset Engage section, click the **Reset Engage** button.
   Engage resets to the default state.

Manage the controller's stored files

Use the Files page to browse and manage files stored across the three storage locations on your controller. Each storage location is displayed as a card showing a usage bar and the amount of free space available.
You can change between grid view and list view at any time using the icons in the top right corner of the page.
This chapter includes the following sections:

- View the stored file locations on the controller
- Download stored files
- Delete stored files

View the stored file locations on the controller

To view the stored file locations on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Files**.
   The following storage cards are displayed:
   - **Internal Storage**: The controller's internal storage, used for logs.
   - **SSD**: External SSD storage. This card is only available if an SSD is installed in the controller.
   - **USB**: USB storage. This card is only available if a USB drive is connected to the controller.

Download stored files

You can browse the contents of each storage location and download an individual file or multiple files.

To download a stored file on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Files**.
3. Click the storage card you want to browse. You can choose one of the following options:
   - **Internal Storage**: The device's internal storage, used for logs.
   - **SSD**: External SSD storage. This card is only available if an SSD is installed in the device.
   - **USB**: USB storage. This card is only available if a USB drive is connected to the device.
4. Click a folder to browse its contents.
5. To find a specific file or folder, enter a search term in the **Search Files** bar at the top of the page.
6. Select the file you want to download. You can select multiple files, or select the **Select All** checkbox to download all the files in the folder.
7. Click the **Download** icon.
   The files are downloaded onto your computer or laptop. You can view any downloaded files by clicking the **Downloads** icon on the Dashboard page. The Downloads page displays and you can view all active downloads or your download history.

Delete stored files

You can browse the contents of each storage location and delete an individual file or multiple files.

To delete a stored file on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Files**.
3. Click the storage card you want to browse. You can choose one of the following options:
   - **Internal Storage**: The device's internal storage, used for logs.
   - **SSD**: External SSD storage. This card is only available if an SSD is installed in the device.
   - **USB**: USB storage. This card is only available if a USB drive is connected to the device.
4. Click a folder to browse its contents.
5. To find a specific file or folder, enter a search term in the **Search Files** bar at the top of the page.
6. Select the file you want to delete. You can select multiple files, or select the **Select All** checkbox to delete all the files in the folder.
7. Click the **Delete** icon.
   Your settings are saved.

Manage the SSD storage

The controller supports an external M.2 SATA SSD installed in the M.2 expansion slot. The Storage Manager page displays the health of the SSD and manage its partitions, including creating, formatting, and deleting partitions.
If no SSD is installed, the Storage Manager displays **No SSD is installed**. The M.2 expansion slot does not support hot-plugging. You must power off the controller before installing or removing an SSD.
The SSD health status displays one of the following values:

Table 13.SSD health status

Status	Description
Healthy	The SSD is operating normally.
Degraded	SSD performance is declining. Attention is recommended.
Failing	SSD failure is imminent. Replace the SSD immediately.

Status	Description
Unknown	The controller cannot determine the SSD status. The SSD may not support SMART health monitoring, or an error occurred.

Partition operations are queued and sent to the controller for processing when you click **Apply**. To clear the queue and revert all pending changes, click **Reset**.

NOTE: When installing a new SSD without existing partitions, configure it using GPT partitioning rather than MBR.

View the SSD health and partition information

To view the SSD health status and partition information on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Storage Manager**.
   The Storage Manager page displays.
3. The **SATA SSD Health** section displays the overall health status of the installed SSD. The status can be Healthy, Degraded, Failing, or Unknown.
4. The table displays the partition name, disk utilization, used space, usage percentage, and file system for each entry.

Create a partition on the SSD

To create a new partition on the SSD installed in your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Storage Manager**.
   The Storage Manager page displays.
3. In the Disk Management table, click the **3 dots** icon next to a free space entry.
   A menu displays.
4. Select **Create Partition**.
   The Create Partition window displays.

5. Use the slider or enter a value in the **Partition Size** field to set the size of the new partition. The minimum partition size is 100 MB. The maximum size is limited by the available free space. The file system is set to EXT4 and cannot be changed.
6. Click the **Create** button.
   The operation is added to the queue. The Disk Management table updates to show the pending partition.
7. Click the **Apply** button.
   The controller creates the partition on the SSD.

Format a partition on the SSD

Formatting a partition erases all data on that partition and reformats it as EXT4. To format a partition on the SSD installed in your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Storage Manager**.
   The Storage Manager page displays.
3. In the Disk Management table, click the **3 dots** icon next to the partition you want to format.
   A menu displays.
4. Select **Format as ext4**.
   The operation is added to the queue.
5. Click the **Apply** button.
   The controller formats the partition as EXT4.

> ⚠ **CAUTION:** All data on the partition is permanently erased.

Delete a partition from the SSD

Deleting a partition permanently removes it and all data it contains. To delete a partition from the SSD installed in your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Storage Manager**.
   The Storage Manager page displays.

3. In the Disk Management table, click the **3 dots** icon next to the partition you want to delete.
   A menu displays.
4. Select **Delete**.
   The operation is added to the queue.
5. Click the **Apply** button.
   The controller deletes the partition from the SSD.

> ⚠ **CAUTION:** All data on the partition is permanently erased.

Manage the configuration file

You can download the configuration file to your local drive for backup or restore the configuration to the running configuration and startup configuration.

Download the configuration file

To download the configuration file from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Maintenance > Configuration Management**.
   The Configuration Management page displays.
3. In the Download section, click the **Download Configuration** button.
   The configuration downloads to your computer.

Restore the configuration file

To restore the configuration file from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Maintenance > Configuration Management**.
   The Configuration Management page displays.
3. In the Restore section, click the **Browse File** field and browse for a file.
4. Click the **Restore** button.
   The configuration restores to the running-config and the startup-config.

Use the main UI to restart the controller

If you can physically access the controller, you can restart the controller by pressing the multi-function **Reset** button on the front panel for less than 5 seconds.

NOTE: Do not press for more than 5 seconds.

To restart your controller from the main UI:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Click the **Reboot** button at the top of the page in the upper right corner.

Use the Reset button to restart the controller

To use the Reset button to restart your controller:

1. On the front of the controller, locate the recessed **Reset** button.
2. Using a straightened paper clip, press and hold the **Reset** button for less than 5 seconds.
3. Release the button.
   The Power LED fades white in and out, slowly, indicating the controller is restarting.
   The Power LED turns solid white once the controller has restarted.

Return the controller to its factory default settings

You can reset the controller to return it to factory default settings, using either the **Reset** button on the front of the controller, or the reset function in the device UI. If you have lost the password and cannot access the controller, use the **Reset** button.

Use the main UI to reset the controller to the factory default settings

You can reset the controller configuration to the factory default values. Resetting the controller to factory default settings erases all configuration and restores the original default settings. If the IP address changes, your web session might disconnect.

To reset your controller to factory default settings:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. Select **Settings > Maintenance > Factory Default**.
   The Factory Default page displays.
3. Click the **Factory Default** button.
   The Confirm Factory Reset pop-up window displays.
4. Click the **FACTORY DEFAULT** button to confirm.
   The controller erases all settings and restarts. A countdown timer displays while the controller restarts. When the countdown reaches zero, the Login page displays.

⚠ **CAUTION:** This action permanently erases all configuration settings.

Use the Reset button to reset the controller to factory default settings

To use the Reset button to reset your controller to factory default settings:

1. On the front of the controller, locate the recessed **Reset** button.
2. Using a straightened paper clip, press and hold the **Reset** button for more than 5 seconds.
   The Power LED fades in and out amber, fast.
3. Release the button.
   The Power LED fades white in and out, fast, indicating the controller is performing a factory reset.
   The Power LED turns solid white once the controller is back to the factory default setting.

Manage the Controller Security

This chapter includes the following sections:

- Manage the user accounts
- Change the password on the controller

Manage the user accounts

The controller supports multiple user accounts, allowing different users to access the management interface with their own credentials. Each user account is assigned a user type that determines the level of access that user has on the controller.
The following user types are available:

> **Administrator**
>
> Provides full administrative control over the controller, including access to all features and the ability to create and delete user accounts. Only admin accounts can access the Account Management section and the Active Sessions page. You can add a maximum of two admin accounts to the controller.
> A new controller installation must use the default username **admin**. The user type is read-only when editing the default admin account or the account of the currently logged-in user.

> **Local Site Manager**
>
> Provides read-only access to all features on the controller except Account Management and Active Session Management. A manager can view settings but cannot update, add, or delete configurations. You can add a maximum of three manager accounts to the controller.

> **Local Site Guest**
>
> Provides view-only access to a limited set of features on the controller. A guest can access the following features only:
> - Change password
> - Dashboard
> - Resource Manager
> - Engage
>
> You can add a maximum of five guest accounts to the controller. You cannot select a guest user type if five guest accounts already exist or if a guest password has not been configured for the site.

The Account Management page displays a table of all configured user accounts, including the username, user type, email address, and phone number for each entry. You can add, edit, and delete user accounts from this page.

NOTE: You cannot delete the default admin account.

Add a user

To add a user to your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Click the **Account** icon.
3. Select **Account Management**.
   The Account Management page displays.
4. Click the **Add User** button.
   The Add User window displays.
5. In the **Username** field, enter a username of up to 64 characters.
6. In the **Email** field, enter an email address for the user.
   This field is optional.
7. In the **Password** field, enter a password for the user.
8. In the **Confirm Password** field, re-enter the password to confirm it.
9. In the **Password Hint** field, enter a password hint of up to 64 characters.
   This field is optional.
10. In the **Phone No.** field, enter a phone number of up to 17 characters.
    This field is optional.
11. From the **User Type** menu, select one of the following:
    - **Administrator**: Full access to all settings and features on the controller.
    - **Local Site Manager**: Access to manage the local site settings on the controller.
    - **Local Site Guest**: Read-only access to the local site settings on the controller. The guest role is disabled if five guest users already exist or if the guest password has not been configured for the site.
12. Click the **Save** button.
    The user is added and displays in the Users table on the Account Management page. Your settings are saved.

Display and manage the active sessions of all users

You can view the users currently logged into the controller.

To display and manage the active sessions of all users on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Click the **Account** icon.
3. Select **Active Sessions**.
   The Active Sessions page displays where you can view other users on the controller.
4. Click the **SIGN OUT ALL OTHER USERS** button to end the sessions of all other users on the controller.
   Your settings are saved.

Change the password on the controller

You can change your password at any time.

To change the password on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Click the **Account** icon.
3. Select **Change Password**.
   The Change Password page displays.
4. Set the following information for the controller:
   - **Current Password**: Enter your current password.
   - **New Password**: Enter a new password.
   - **Confirm Password**: Confirm the new password.
   - **Password Hint**: Enter a password hint (optional).
5. Click the **SAVE** button.
   Your settings are saved.

Diagnostics and Troubleshooting

You can diagnose and troubleshoot the controller and its network.
This chapter includes the following sections:

- Send a ping, traceroute, or DNS lookup request to an IP address or host name
- Download diagnostics files for technical support
- Display the neighboring devices
- Display the resource manager
- Manage the controller's notifications

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

You can send a ping, trace a route, and look up a DNS on the controller. You can take the following actions independently of each other or simultaneously (or rather, one after the other):

- **Send a ping**: The controller 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 controller attempts to trace the route to a particular IP device to determine the precise path to the device.
- **Send a DNS lookup request**: The controller 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. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Troubleshoot**.
   The Troubleshoot page displays.
3. In the **IP Address/Host Name** field, specify the IP address or host name.
4. 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.

5. Click the **Run Test** button.
   The selected tests run one after the other. The results display in the result panes.
   Your settings are saved.

Download diagnostics files for technical support

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

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

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

To download the combined diagnostics files in a file:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Support Diagnostics**.
   The Support Diagnostics page displays.
3. Click the **Download Files** link.
   The log collection process can take several minutes to complete. The log file saves to your browser's Downloads folder.

Display the neighboring devices

You can use the controller to view LLDP-discovered neighboring devices.

To display the neighboring devices:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.

2. Select **Settings > Diagnostics > Neighbor**.
   The Neighbor page displays.
   You can view the port status of the controller on the device image. The following table describes the port status indicators:

Table 14.Port status

Indicator	Status	Description
Green outline	Connected	The port has an active link and is passing traffic.
Blue outline	Connected & Powered	The port is connected and supplying power through PoE.
Red outline	Error	The port has encountered an error condition.
Exclamation	Admin Down	The port has been manually disabled by an administrator.
No indicator	Available	The port is operational but no device is currently connected.
Port grayed out	Disabled	The port is disabled and not available for use.
LAG icon	LAG	The port is a member of a Link Aggregation Group.
A icon	Auto Trunk	The port is configured for automatic trunking.
M icon	Manual Trunk	The port is configured as a manual trunk.
S icon	1G SFP Fiber Port	The port is a 1G SFP fiber port.
S+ icon	10G SFP+ Fiber Port	The port is a 10G SFP+ fiber port.
Green outline power symbol	Powered by PoE	The controller is powered through PoE. No Ethernet link is established.

3. Scroll to the Neighbors section. For each detected device, the page displays the following:
   - **Port**: The port to which the device is attached.
   - **Host**: The system name of the device, if any.
   - **MAC Address**: The MAC address of the device.
   - **VLAN ID**: The VLAN ID of the port to which the device is attached.
   - **IP Address**: The IP address of the device.

   Each page shows a maximum of 10 entries, with additional entries moving to subsequent pages.

Display the resource manager

The resource manager displays real-time performance metrics for the controller, including CPU utilization, memory utilization, and network utilization.

To display the resource manager on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Resource Manager**.
   The Resource Manager page displays. The following tabs are available:
   - **CPU Utilization**: Displays CPU core loading as a percentage.
   - **Memory Utilization**: Displays memory usage as a percentage.
   - **Network Utilization**: Displays network traffic statistics for each port.

View the CPU utilization

The CPU Utilization tab displays real-time loading for each CPU core as a percentage.

To view the CPU utilization on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Resource Manager**.
   The Resource Manager page displays.
3. Select **CPU Utilization**.
   The CPU Utilization tab displays a chart showing the loading for each CPU core as a percentage.
4. To change the update interval, select **Every Second** or **Every Minute**.
   The default update interval is **Every Second**.
   Your settings are saved.

View the memory utilization

The Memory Utilization tab displays real-time memory usage as a percentage.

To view the memory utilization on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Resource Manager**.
   The Resource Manager page displays.
3. Select **Memory Utilization**.
   The Memory Utilization tab displays a chart showing current memory usage as a percentage.
4. To change the update interval, select **Every Second** or **Every Minute**.
   The default update interval is **Every Second**.
   Your settings are saved.

View the network utilization

The Network Utilization tab displays real-time traffic statistics for each port on the controller.

To view the network utilization on your controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Resource Manager**.
   The Resource Manager page displays.
3. Select **Network Utilization**.
   The Network Utilization tab displays traffic statistics for Port 1 through Port 6.

4. Select up to four metrics to display by clicking each metric name. The following metrics are available:
   - **RX**: Inbound traffic in Mbps.
   - **TX**: Outbound traffic in Mbps.
   - **RX Error**: Inbound error packets per second.
   - **TX Error**: Outbound error packets per second.
   - **RX Drop**: Inbound dropped packets per second.
   - **TX Drop**: Outbound dropped packets per second.
   - **RX Packets**: Inbound packets per second.
   - **TX Packets**: Outbound packets per second.

   NOTE: RX and TX display in Mbps and can only be selected together. All other metrics display in packets per second and can only be combined with other packets per second metrics.

5. To change the update interval, select **Every Second** or **Every Minute**.
   The default update interval is **Every Second**.
   Your settings are saved.

Manage the controller's notifications

You can manage the controller's message notifications, logs, and alarms.

Display message notifications

To display message notifications on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Notifications**.
   The Notifications page displays.

3. Select a notification to view the full message.
   The messages display the severity of the notification:
   - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
   - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
   - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
   - **Error**: Level 3, a device error occurred, such as a port being offline.
   - **Warning**: Level 4, the lowest level of a device warning.
   - **Notice**: Level 5, provides the network administrators with device information.
   - **Informational**: Level 6, provides device information. This is the default setting.
   - **Debug**: Level 7, provides detailed information about the log.
4. Filter the notifications by selecting the **Unread only** checkbox or by using the **Search** field.
5. To delete a notification, select the notification and click the **Delete** button.
6. To dismiss a notification, select the notification and click the **Mark as Read** button.
   Your settings are saved.

Display the notifications

To display the notifications on the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Click the **Notification** icon on the upper right corner of the page.
   The Notification page displays.
3. To dismiss the notifications, click the **Mark All as Read** button.
   The Mark All as Read page displays. Click the **CONFIRM** button.
   Your settings are saved.

Manage the message controller's logs

The controller 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.

Filter the logs

You can filter logs on the controller.

To filter the log results:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Logs**.
   The Logs page displays.
3. Click the **Filter** button.
4. From the **Severity** menu, select from the following options:
   - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
   - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
   - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
   - **Error**: Level 3, a device error occurred, such as a port being offline.
   - **Warning**: Level 4, the lowest level of a device warning.
   - **Notice**: Level 5, provides the network administrators with device information.
   - **Informational**: Level 6, provides device information. This is the default setting.
   - **Debug**: Level 7, provides detailed information about the log.

   NOTE: A log records messages equal to or above a configured severity threshold.
5. From the **Facility** menu, select from the following options:
   - System
   - DHCP
   - PTP
   - NTP
   - DNS
   - HTTP
   - mDNS
   - LLDP
6. From the **Time** menu, select a start and end time, in hour increments, within seven days from your current date.

7. Click the **Apply** button.
   Your settings are saved and the Logs page displays the filtered logs.

Download the logs on the controller

To download logs from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Logs**.
   The Logs page displays.
3. Click the **Download** button.
   The controller downloads all log messages from the system.
   Your settings are saved.

Refresh the logs on the controller

To refresh the logs from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Logs**.
   The Logs page displays.
3. Click the **Refresh** button.
   The controller refreshes the log messages on the system.
   Your settings are saved.

Clear logs from the controller

To clear logs from the controller:

1. Open a web browser and log in to the controller. For more information, see Log in to the controller on page 9.
   The Dashboard page displays.
2. Select **Settings > Diagnostics > Logs**.
   The Logs page displays.

3. Click the **Clear All** button.
   The controller deletes all log messages from the system.
   Your settings are saved.

Technical Specifications

This appendix includes the following sections:

- Access default settings for the controller main UI
- Network profile features default settings
- System features default settings
- Service features default settings
- General hardware technical specifications

NOTE: For more information about installing and using the controller, see the Installation Guide and Hardware Installation Guide. For more information about the controller's specifications and capabilities, including the maximum settings for many features, see the datasheet, which you can download by visiting netgear.com/support/enterprise.

Access default settings for the controller main UI

The following table describes the default settings for access to the controller main UI. View-only settings are not included in the table but might be included in the datasheet, which you can download by visiting netgear.com/support/enterprise.

Table 15.Default access settings

Feature	Default
IP address	192.168.1.250
Subnet mask	255.255.255.0
Default gateway	0.0.0.0
Management VLAN ID	1
Admin user	User name: admin (read/write access) Password: No password (that is, the password is blank), but upon first login, the admin user must specify a password. Encryption type: SHA512 Multifactor authentication mode: Disabled
Guest user	User name: guest (read-only access) Password: No password (that is, the password is blank), but upon first login, the guest user must specify a password. Encryption type: SHA512 Multifactor authentication mode: Disabled
Minimum length for admin	Eight characters

Feature	Default
and guest passwords	

Network profile features default settings

The following table describes the default settings for the network profile features that you can configure.

Table 16.Network profile default settings

Feature Name/Setting	Default value
Default profile	
Profile name	Default
Profile type	LAN
Profile template	Default
Ports	Port 1 to Port 6, all untagged
VLAN ID	1
Color	#000000
Management VLAN	Enabled
Internet access	Disabled
IP settings	Static IP
IP address	192.168.1.250
Subnet mask	255.255.255.0
Default route	None
DNS Server 1	None
DNS Server 2	None
Auto-Trunk	
Auto-Trunk	Enabled

System features default settings

The following table describes the default settings for the system features that you can configure.

Table 17.System default settings

FeatureName/Setting	Default value
System name	GB406
Timezone	(UTC-08:00) Baja California
Adjust for daylight saving time automatically	On
Link Aggregation	
Auto-LAG	Enabled
Auto-LAG hash	Layer 2; Source + Destination
Port Configuration	
Port description	Defaults to port number
Admin mode	Defaults to enable for all ports
Speed	Defaults to auto for all ports (copper ports 1 to 4 and fiber ports 5 to 6)
Certificate Management	
System default certificate	One system default certificate. Name: Default.

Service features default settings

The following table describes the default settings for the services features that you can configure.

Table 18.Services default settings

Feature Name/Setting	Default value
DHCP server	
DHCP server	Disabled
PTP server	
PTP service	Disabled
Syslog server	
Syslog service	Disabled
NTP server	
NTP server	Disabled
Enable logging	On

Feature Name/Setting	Default value
Enable SNTP client	On
NTP Source 1	time-a.netgear.com
NTP Source 2	time-b.netgear.com
NTP Source 3	time-c.netgear.com
NTP Source 4	time-d.netgear.com
Local reference clock	On
Local stratum	10
DNS server	
DNS server	Disabled
Recursive queries	On
Enable logging	On
Forwarders	None
HTTPS service	
Login session timeout	30 minutes
Enable logging	On
Certificate	Default Server Certificate
mDNS server	
mDNS service	Enabled
mDNS hostname	GB406
mDNS domain name	local
Enable logging	On
LLDP service	
LLDP service	Enabled
Enable logging	On
Transmit interval	30 seconds
Hold time multiplier	4
System description	NETGEAR Align Controller
LLDP enable (all ports)	On

General hardware technical specifications

Table 19.Hardware technical specifications

Feature	Description
Ethernet network interfaces	Ports 1 to 4: 100M/1G/2.5GBASE-T RJ-45 ports
SFP+ ports	Ports 5 to 6: 10G SFP+ ports
LCD display	Status user interface
Power adapter	54V @ 1.66A DC input
Power consumption	71W maximum
Dimensions (W x D x H)	8.7 x 9.1 x 1.7 in. (220 x 230.2 x 43.2 mm)
Weight with power adapter	4.6 lb (2096 g)
Operating temperature	32 to 113°F (0 to 45°C)
Operating humidity	10 to 90% relative humidity, noncondensing
Maximum operating altitude	10,000 ft. (3,000 m)
Storage temperature	–4 to 158°F (–20 to 70°C)
Storage humidity	5 to 95% relative humidity, noncondensing
Maximum storage altitude	10,000 ft. (3,000 m)

Revision History

Revision History

Publication Part Number	Publish Date	Comments
202-12891-03	November 2026	We updated the following section: • Activate the license from Insight Cloud on page 24 We added the following subsection: • Add a license key from Insight on page 25
202-12891-02	October 2026	We updated the following section and its subsections: • Manage Your Apps on the controller on page 24
202-12891-01	September 2026	First publication