

# Engage Controller Quick Start Guide

## Support and Community

Visit [netgear.com/support](https://netgear.com/support) to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at [community.netgear.com](https://community.netgear.com).

## Regulatory and Legal

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

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

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

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.

## Trademarks

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

## Revision History

| Publication Part Number | Publish Date | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 201-33590-01            | May 2026     | We updated the following sections:<br>1. <a href="#">Overview of preconfigured AV profile templates</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 201-30013-07            | March 2026   | We added the following chapter:<br><a href="#">Manage Virtual Sites and Devices</a> and subsections: <ul style="list-style-type: none"><li>• <a href="#">Configure virtual sites</a> and subsection:<ul style="list-style-type: none"><li>◦ <a href="#">Add a virtual site</a></li></ul></li><li>• <a href="#">Deploy a virtual site</a></li><li>• <a href="#">Configure virtual devices</a> and subsections:<ul style="list-style-type: none"><li>◦ <a href="#">Add a virtual device</a></li><li>◦ <a href="#">Provision a virtual device</a></li></ul></li><li>• <a href="#">Onboard a physical device using virtual device configurations</a></li><li>• <a href="#">Configure a virtual link</a> and subsection:<ul style="list-style-type: none"><li>◦ <a href="#">Create a virtual link</a></li></ul></li></ul> |

| Publication Part Number | Publish Date  | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         |               | We updated the following sections: <ol style="list-style-type: none"><li>1. <a href="#">Features</a></li><li>2. <a href="#">Overview of preconfigured AV profile templates</a></li></ol>                                                                                                                                                                                                                                                                                        |
| 201-30013-06            | December 2025 | We added new network profiles to the <a href="#">Overview of preconfigured AV profile templates</a> section.                                                                                                                                                                                                                                                                                                                                                                    |
| 201-30013-05            | October 2025  | We added new network profiles to the <a href="#">Overview of preconfigured AV profile templates</a> section.                                                                                                                                                                                                                                                                                                                                                                    |
| 201-30013-04            | May 2025      | We added the following section and subsection: <ul style="list-style-type: none"><li>• <a href="#">User Accounts</a></li><li>• <a href="#">Add a user account</a></li></ul> We updated the following sections: <ul style="list-style-type: none"><li>• <a href="#">Overview of preconfigured AV profile templates</a></li><li>• <a href="#">Add a network profile</a></li><li>• <a href="#">Add a physical site</a></li><li>• <a href="#">Add a site user account</a></li></ul> |
| 201-30013-03            | December 2024 | We updated the following sections: <ul style="list-style-type: none"><li>• <a href="#">Prepare your AV network for discovery</a></li><li>• <a href="#">Overview of preconfigured AV profile templates</a></li></ul>                                                                                                                                                                                                                                                             |
| 201-30013-02            | October 2024  | Major revision.<br><br>The Engage controller now also supports the NETGEAR Pro Router and NETGEAR access points, in addition to NETGEAR fully managed switches.                                                                                                                                                                                                                                                                                                                 |
| 201-30013-01            | October 2022  | Initial publication.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

# Contents

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| <b>Quick Start Guide</b> .....                                                             | 0  |
| <b>Introduction</b> .....                                                                  | 1  |
| Features .....                                                                             | 1  |
| What you can do with the controller .....                                                  | 2  |
| <b>Install or Update the Engage Controller Software Application</b> .....                  | 4  |
| Download and install the controller software application on a Windows-based computer ..... | 4  |
| Download and install the controller software application on a Mac .....                    | 5  |
| Recommendations for reinstalling the controller software application .....                 | 5  |
| Update the controller software application .....                                           | 6  |
| Update the controller software application from the controller itself .....                | 6  |
| Manually update the controller on a Mac .....                                              | 8  |
| Manually update the controller on a Windows-based computer .....                           | 8  |
| <b>Set Up the Controller</b> .....                                                         | 9  |
| Prepare your AV network for discovery .....                                                | 9  |
| DHCP server and IP address considerations .....                                            | 10 |
| Access the controller for the first time and set up the default site .....                 | 12 |
| Access the controller for the first time and import an existing site .....                 | 17 |
| <b>Manage Users</b> .....                                                                  | 19 |
| User Accounts .....                                                                        | 19 |
| Add a user account .....                                                                   | 20 |
| <b>Manage Devices</b> .....                                                                | 22 |
| Add one or more devices to a site .....                                                    | 22 |
| Add a single discovered device to a site .....                                             | 23 |
| Add multiple discovered devices to a site simultaneously .....                             | 24 |
| Add an undiscovered physical device to a site .....                                        | 26 |
| <b>Manage Network Profiles</b> .....                                                       | 28 |
| Overview of preconfigured AV profile templates .....                                       | 28 |
| About timing and clocks .....                                                              | 33 |
| About Audio video bridging .....                                                           | 33 |
| About PTP residency time stamping and network profiles .....                               | 33 |
| About the global site SSID .....                                                           | 34 |
| Add a network profile .....                                                                | 35 |
| Edit the controller's default network profile .....                                        | 39 |
| Edit a non-default network profile .....                                                   | 42 |

- Set up an open or secure WiFi network ..... 45
- Set up a WiFi network with Multi PSK ..... 49
- Manage Sites ..... 54**
  - Add a physical site ..... 54
  - Edit the network setup of a site ..... 57
  - Add a site user account ..... 59
- Manage Virtual Sites and Devices ..... 64**
  - Configure virtual sites ..... 64
    - Add a virtual site ..... 64
  - Deploy a virtual site ..... 66
  - Configure virtual devices ..... 68
    - Add a virtual device ..... 69
    - Provision a virtual device ..... 70
  - Onboard a physical device using virtual device configurations ..... 72
    - Auto-onboard a device ..... 73
  - Configure a virtual link ..... 74
    - Create a virtual link ..... 74

# Introduction

The NETGEAR Engage Controller provides central management and configuration of the following NETGEAR network devices through a free, audio-video (AV)-friendly, portable app for a Windows-based computer and Mac:

- **Pro Router:** PR460X
- **Access Points:** WBE718, WBE758, and WAX608Y
- **Fully Managed Switches:** M4250, M4300, M4350, and M4500 series For a list of NETGEAR M4250, M4300, M4350, and M4500 switch models with which the controller is compatible, visit [kb.netgear.com/000065072](http://kb.netgear.com/000065072).

Automatic device detection, centralized profile repository, firmware upgrades, and much more can now be realized across multiple NETGEAR devices on your AV network.

This quick start guide is intended for AV network administrators and describes how to install the software and get started quickly. For a complete description of the features and capabilities of the controller, see the NETGEAR Engage Controller User Manual, which you can download by visiting [netgear.com/support/download/](http://netgear.com/support/download/). The quick start guide does not provide unique information but is a subset of the user manual.

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

This chapter includes the following sections:

- [Features](#)
- [What you can do with the controller](#)

❗ **NOTE:** For more information about the topics that are covered in this manual, visit the support website at [netgear.com/support](http://netgear.com/support), enter your model number in the search box, and then select your product.

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

## Features

These are some of the main features of the controller:

- Automatically detects all Engage-manageable devices as well as other client devices in the network to which you connect it.
- Lets you centrally trigger a firmware upgrade for all Engage-manageable devices on the

network.

- Lets you use the integrated AV user interface (UI) with port-based profiles to configure each NETGEAR M4250, M4300, M4350, and M4500 series fully managed switch on your network.
- Collects the AV profiles of all onboarded fully managed switches and lets you select which profiles to share among the Engage-manageable devices on your AV network.
- Lets you configure basic settings for each onboarded Pro Router and access point, while still allowing configuration fine-tuning through the device UI.
- Lets you display your AV network layout (topology) for easier configuration across all Engage-manageable devices as well as other client devices in the network.
- Lets you leverage the unique Auto-LAG, Auto-Trunk, PTPv2 TC, and time configuration features for automated interconnection and timing between the Engage-manageable devices on your network.
- Lets you create virtual sites and add virtual devices to the controller to plan for future sites and installations.
- Centrally stores all your sites, credentials, and configurations.

The controller is a portable application that can reside on a USB thumb drive, so it can be easily moved to any network location. For a Windows-based computer, launch the app directly from the USB thumb drive, and save all configuration data to the same USB thumb drive. For a Mac computer, install the controller app on the computer, and then copy the locally saved configuration data back to the USB thumb drive for convenience.

## What you can do with the controller

You can use the Engage controller to onboard, configure, and manage NETGEAR devices for AV network installations at one or more sites, and then save your site configurations for future use. With the controller, you can update firmware for every Engage-manageable device as it is added to a site, and quickly apply preconfigured or custom network profiles at a site. After setup, you can view the site topology and neighbor devices, run tests, view device status, and manage the settings for an individual router or access point, and access the AV UI when you need to manage the settings on an individual fully managed switch.

You can view the following components of your AV network:

- **Site:** A configured network location to which you onboard and manage devices. When onboarding devices to the site, the controller updates firmware, and automatically collects AV profile templates from onboarded devices. You then can assign these network profiles to ports and VLANs at the site.

You can set up multiple sites and manage them all through the controller. For example, if a location has one large and one small auditorium with different AV requirements, you can set up two sites, one for each auditorium.

- **Site settings:** The AV network profiles and other configurations that you use for a site. NETGEAR Pro AV switches ship with a rich assortment of preconfigured profiles designed by NETGEAR and our Pro AV partners. You can also create custom network profiles (as opposed to predefined network profiles) or import existing profiles to assign to switch ports on the devices at your site.

For example, you might assign the Default network profile on selected switch ports of several switches and a customized network profile that is based on the Dante AV profile template for other switch ports of the same switches.

If your network includes access points (APs) that you want to add to a site, you must set up a global site SSID, which is the default WiFi network for the site. However, you can add multiple SSIDs and assign these to network profiles to fine-tune the WiFi needs for a site.

- **Devices:** The NETGEAR Engage-manageable devices that can be detected, onboarded and assigned to a site, and managed by the controller.

From the pool of all detected devices, you select which devices to add to the site. For example, if the controller detects eight switches and ten access points in the entire network that it can reach, you can assign six switches and seven access points to one site (such as the large auditorium) and keep the other two switches and three access points available for another site (such as the small auditorium).

- **Topology:** The network layout of a site. For each site, you can display the network layout of the switches, switch ports, and connected devices.

The first time that you log in to the controller, you must go through the Engage Onboarding process, a one-time process that lets you set an admin password for the controller and define a default site with switches and network profiles. For more information, see [Set Up the Controller](#) on page 9. Alternately, if you previously saved site settings, you can import existing site settings.

# Install or Update the Engage Controller Software Application

The controller is a software application for a Windows-based computer or Mac, offered free of charge.

You can install the controller software application on your computer hard drive, or run it from an external drive or USB stick for portability.

This chapter describes how to manage controller installations and includes the following sections:

- [Download and install the controller software application on a Windows-based computer](#)
- [Download and install the controller software application on a Mac](#)
- [Recommendations for reinstalling the controller software application](#)
- [Update the controller software application](#)

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

You can install the controller on your Windows-based computer or launch the app directly from a USB thumb drive, and save all configuration data to the same USB thumb drive.

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

1. Visit [netgear.com/support/product/engage-controller](https://netgear.com/support/product/engage-controller).

The NETGEAR Engage Controller Support page displays.

2. Download the installation file to a location on your computer.

An example of the name of the installation file is `Netgear-Engage-x.x.x.x.exe`.



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

3. Go to the location where you downloaded the installation file and do one of the following:
  - **Standard installation:** Double-click the .exe file and follow the prompts of the installer program to install the controller software.

The default installation location is `C:\Users\your-username\Netgear`. However, you can select another location.

After installation, the executable file that opens the controller is `Engage.exe`, and an executable icon is placed on your desktop.
  - **Custom installation:** Right-click the .exe file and select how you want to install the controller.

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

## Download and install the controller software application on a Mac

You can install the controller on your Mac, and optionally copy your locally saved configuration data to a USB thumb drive for convenience.

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

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



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

The Engage application user data is saved at the following path:

`/Users/<login_user_id>/Documents/Engage/`

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

## Recommendations for reinstalling the controller software application

If you reinstall the controller software application on a device on which it is already installed, we recommend the following:

- Close the controller software application before you reinstall it.
- If controller is installed on a Windows-based computer and you want to retain all existing settings and data, install the controller software application in the previous installation folder.

If the controller is installed on a Mac, you can either install the files in a new folder, or else save your site configuration files in a different directory, then manually remove the data files from the installation directory before you reinstall the application at the previous installation folder.

- To set up a new installation, install the controller in a new folder, and then either import an

existing site or configure a new site.

## Update the controller software application

You can update the controller software application manually.

If your Mac or Windows-based computer has Internet connectivity and the controller detects a new software version, you can initiate the software update from the controller user interface (UI). In such a situation, the Controller Management tab of the UI displays an *Update Available* message.

## Update the controller software application from the controller itself

After initial installation of the controller, if new firmware becomes available for the controller software application, the controller user interface (UI) displays a notice and the **Update Available** icon.

### To update the controller software application from the controller itself:

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

4. Select one of the following radio buttons and follow the associated steps:

- **Download and Upgrade:** The controller downloads the new firmware version and updates itself. This is the most efficient update method.

Do the following:

- a. Click the **Continue** button. The information in the window adjusts.
  - b. To display the release notes, click the **Release Notes** link.
  - c. Click the **Download** button. Wait for the download to complete.
  - d. Click the **Close and Install** button. When you log back in to the controller (see step 1 and step 2), the controller starts in the new firmware version.
- **Download only:** The controller downloads the new firmware version only. You must perform the update manually.

Do the following:

- a. Click the **Continue** button. The information in the window adjusts.
- b. To display the release notes, click the **Release Notes** link.
- c. Depending on the operating system (OS) on which the controller is installed, select the **Windows** or **macOS** radio button.
- d. Click the **Download** button. Depending on the configuration of your browser, the firmware file is downloaded to a preset location, or a pop-up window opens to let you navigate to and select a location. Wait for the download to complete.
- e. Depending on the OS on which the controller is installed, do the following:
  - **Windows:** Go to the location where you downloaded the installation file and do one of the following:
    - **Standard installation:** Double-click the .exe file and follow the prompts of the installer program to install the controller software.
    - **Custom installation:** Right-click the .exe file and select how you want to install the controller.

For either type of installation, you can either overwrite the current instance by overwriting the current version in the same directory or install a new instance of the controller in a different directory.

If you overwrite the current installation, the desktop icon is automatically overwritten. If you install a new instance, you must add a new desktop icon.

- **macOS:** Do the following:
  - i. Double click the **.dmg** file. The Engage application opens in a new window.
  - ii. Drag and drop the Engage application into the Applications folder.



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

## Manually update the controller on a Mac

### To update the controller software application on a Mac:

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



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

## Manually update the controller on a Windows-based computer

### To update the controller software application on a Windows-based computer:

1. Visit [netgear.com/support/product/engage-controller](https://netgear.com/support/product/engage-controller).  
The NETGEAR Engage Controller Support page displays.
2. Download the installation file to a location on your computer.  
An example of the name of the installation file is Netgear-Engage-x.x.x.x.exe.
3. Go to the location where you downloaded the installation file and do one of the following:
  - **Standard installation:** Double-click the .exe file and follow the prompts of the installer program to install the controller software.
  - **Custom installation:** Right-click the .exe file and select how you want to install the controller.

After installation, the executable file that opens the controller is Engage.exe, and an executable icon is placed on your desktop.

# Set Up the Controller

Setting up the controller for the first time is an automated process that guides you through the following steps:

1. **Admin password:** Set a new admin password for the controller.
2. **Default site:** Configure the default site settings, including a site password, name, and description.
3. **Network interface:** Select or configure the network interface that the controller must use to discover the devices.
4. **WiFi network:** As an option, set up a global WiFi network (SSID) that applies to the site. You can also do this after you have set up the controller.
5. **Discovered devices:** As an option, select which discovered devices the controller must onboard to the site. You can also do this after you have set up the controller.
6. **Network profile:** Display or add network profiles that the controller can push to all onboarded devices at the site. You can also do this after you have set up the controller.

This chapter includes the following sections:

- [Prepare your AV network for discovery](#)
- [DHCP server and IP address considerations](#)
- [Access the controller for the first time and set up the default site](#)
- [Access the controller for the first time and import an existing site](#)

## Prepare your AV network for discovery

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

- What is the default site name and site password that you want to use? The site that you set up during the controller onboarding process is referred to as the default site. Later, you can add more sites and change the default site.
- For each site, how can the computer on which the controller is installed reach the devices? Does the computer receive an IP address from a DHCP server in your network or does the computer require a static IP address?
- The controller can function as a DHCP server for the devices in the network. Is a DHCP server present in the network or does the controller need to function as a DHCP server?
- What is the local device password for each device that you want to add to the default site? This information is required for each device so that the controller can onboard and manage the device.
- If you plan to let the controller manage one or more access points, are these devices in factory default state, which is a requirement for onboarding?
- Do you want to set up a global WiFi network (SSID) for a site? If so, what must be the WiFi network name and WiFi password (passphrase) and to which VLAN must the WiFi network

be assigned?

- Which network profiles do you need for the default site?
- The controller and NETGEAR Insight are mutually exclusive. You cannot let the controller onboard a device that is managed by Insight, and the other way around.

If you want to let the controller onboard a device that is managed by Insight, remove the device from the Insight network location, and then remove the device from Insight. After you do so, we recommend that you reset the device to factory default settings (this a requirement for an access point).

## DHCP server and IP address considerations

How the controller performs device discovery depends on your network configuration. The controller and each device must have a unique IP address in the network. A unique IP address can be a static IP address or an IP address that is dynamically assigned by a DHCP server in the network.



**NOTE:** The controller IP address must be in the same subnet as the devices that the controller must be able to discover.

If a DHCP server is not present in the network, the controller itself can function as a DHCP server, *if* it can reach the devices on the network. The devices can be in factory default state or already operating in the network, except for access points, which must be in factory default state.

- **DHCP server in the network:**
  - The network can include a dedicated DHCP server (such as a router) that assigns IP addresses to the controller and the devices that the controller is supposed to control.
  - One of the devices can function as a DHCP server that assigns IP addresses to the controller and the other switches.
- **Static IP addresses:** If devices are configured with static IP addresses in a subnet, you can configure the controller with a static IP address in the same subnet.
- **No DHCP server in the network:** The controller itself can function as a DHCP server and assign IP addresses to the devices in the network.

If the controller does not receive an IP address from a DHCP server, it uses its default IP address of 192.168.0.100, and can assign IP addresses in that range to the devices in the network.

Table 1. Overview IP address options for switch discovery

| Network IP Address Assignment | Controller IP Address | Device IP Address | Result or Action                     |
|-------------------------------|-----------------------|-------------------|--------------------------------------|
| Network DHCP                  | Dynamic               | DHCP pool         | The controller and devices receive a |

| Network IP Address Assignment     | Controller IP Address   | Device IP Address                             | Result or Action                                                       |
|-----------------------------------|-------------------------|-----------------------------------------------|------------------------------------------------------------------------|
| server                            |                         |                                               | dynamic IP address from the network DHCP server.                       |
| Static IP addresses               | Static                  | Static                                        | Configure the controller IP address in the same subnet as the devices. |
| The controller is the DHCP server | Default (192.168.0.100) | DHCP pool:<br>192.168.0.101-<br>192.168.0.254 | The devices receive a dynamic IP address from the controller.          |



**NOTE:** The device IP addresses in a single network can also consist of mixture of DHCP-assigned IP addresses and static IP addresses, but they must be in the same subnet, and the IP address of the controller must also be in the same subnet.

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

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

- **Admin Password:** The password an administrator uses for future access to the controller.
- **Default site:** A name, description, and password for the default site. (The site that you set up during the controller onboarding process is referred to as the default site.)
- **Network interface:** The interface that lets the controller connect to the default site.
- **(Optional) WiFi network:** The global WiFi network (SSID) for the default site. By default, the WiFi security for the global SSID is WPA2-MPSK (Multi PSK, in short, MPSK), which lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. You cannot change the WiFi security for the global SSID, but you can expand the MPSK configuration. (For more information about MPSK, see [Set up a WiFi network with Multi PSK](#) on page 49.)

After you have set up the global site SSID, you can add additional SSIDs, but you cannot make another SSID the global site SSID. By default, the global SSID broadcasts on the 2.4 GHz and 5 GHz radio bands and is assigned to VLAN 1. You can change the 2.4 GHz and 5 GHz radio bands, change the VLAN ID, and disable the WLAN status for the global site SSID entirely.

- **Devices:** The devices that the controller discovers at the default site and that you can manage by letting the controller onboard the devices.
- **Network profiles:** The network profiles that are available for the default site. (The network profiles are pulled from the onboarded fully managed switches but you can also add a network profile.)



**NOTE:** For each device that you want to onboard, you must know the local device password. After the controller onboards the device, the controller replaces the local device password with the default site password. Access points must be in factory default state, which means that they are using the device default password.



**CAUTION:** The firmware that devices are running before being onboarded by the controller does not support the controller functions. When you let the controller onboard a device, the controller pushes the latest firmware *with* controller functions to the device. This firmware update is necessary because the controller cannot manage the device without the firmware update.

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

1. On your computer, in the folder in which you installed the controller application, click the **Engage.exe** application icon, or if you created a shortcut, click the **Engage** shortcut.  
The initial login page displays.  
  
The first time that you log in, no password is required. However, you then must specify a controller password to use each subsequent time that you log in.
2. In the **Login Name** field, enter **admin**, and click the **Login** button.  
The Engage Password page displays.
3. In the **New Password** field, set an admin password, repeat the password in the **Confirm Password** field, and click the **Next** button.  
The password must be 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.
4. Click the **Next** button.  
The Site Setup page displays.
5. Keep the **Default Site Configuration** radio button selected (it is selected by default) and set the following information for the default site:
  - a. **Site Name**: A name for identification purposes.
  - b. **Site Description**: A description for identification purposes.
  - c. **New Site 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 device local device password with the site password.
  - d. **Confirm Site Admin Password**: Repeat the password.
6. Click the **Next** button.  
The Network Setup page displays.

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

- **Dynamic IP Address:** From the **Engage Network Interface** menu, select the 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 the controller. 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 the controller and configure the computer as a DHCP server. The Network Setup page shows both how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for 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.

8. Click the **Next** button.

The Wireless Setup page displays.

9. Either click the **Skip >>** link to skip this step, or if your network includes access points, set up the global WiFi network (SSID) for the default site:

- a. In the **SSID Name** field, enter the name for the WiFi network (SSID).
- b. In the **Passphrase** field, enter the password for access to the WiFi network, which uses WPA-MPSK security. (For more information, see the introduction of this section.)
- c. From the **Region** menu, select the region for the country in which the default site is located. After setup, you cannot change the region.
- d. From the **Country** menu, select the country in which the default site is located. After setup, you cannot change the country.

10. Click the **Next** button.

The Device Setup page displays.

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.

11. 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. Specify the following information:

- a. **Device Admin User:** Enter **admin** as the user name for the device.
- b. **Device Password:** 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 [step 5](#).

- c. 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.

12. Repeat the previous step for each device that you want to let the controller onboard.

13. Click the **Next** button.

The Profile Setup page displays.

During the device onboarding process (see [step 11](#) and [step 12](#)), 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.

14. 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, do the following:

- a. Click the **Create Network Profile** link.
- b. Set up the network profile. For more information, see [Manage Network Profiles](#) on page 28.

15. Click the **Finish** button.

Your settings are saved. The devices are being onboarded. 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.



**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.

16. 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.

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

You can use this procedure only if you have used the controller before and exported a site configuration file. Otherwise, see [Access the controller for the first time and set up the default site](#) on page 12.

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

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

1. On your computer, in the folder in which you installed the controller application, click the **Engage.exe** application icon.  
The initial login page displays.  
The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.
2. In the **Login Name** field, enter **admin**, and click the **Login** button.  
The Engage Password page displays.
3. In the **New Password** field, set an admin password, repeat the password in the **Confirm Password** field, and click the **Next** button.  
The password must be 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.
4. Click the **Next** button.  
The Site Setup page displays.
5. Click the **Import Site Configuration** radio button.  
The page adjusts.
6. Click the **Browse** button and navigate to and select the site configuration file that you want to import.
7. In the **Site Configuration Password** field, enter the password for the site configuration file.

8. Click the **Finish** button.

Your settings are saved. The devices are being onboarded.

If any device does not yet support the controller, the controller pushes firmware *with* controller functions to the device. This firmware update is necessary because the controller cannot manage the device without the firmware update. 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.

9. 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.

# Manage Users

The controller lets you centrally configure user accounts, depending on what access rights you want to assign them. You can configure individual user access to the controller, or site-specific user accounts.

This chapter includes the following sections:

- [User Accounts](#)
- [Add a user account](#)

## User Accounts

The controller lets you create user accounts with different access permissions, such as read, write, or administrative rights. This ensures secure access control, and allows users to interact with the controller only with the functionalities that their role permits.

| User Role                 | Rights                                                                                                                                                                                                                                               | Number of roles allowed          | Supported models                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Administrator</b>      | This user has full administrative control, including creating and deleting user accounts and site operations. For example, they can add, edit, or delete a site.<br><br>You must use this role when you initially install and set up the controller. | Two for each controller          | <b>Fully managed switches:</b> M4250, M4300, M4350, M4500<br><b>Access points:</b> WBE718, WBE758<br><b>Pro Router:</b> PR460 |
| <b>Local Site Manager</b> | Can view, modify, and create data but does not have administrative control over users or site operations. For example, they cannot add, edit, or delete a site.                                                                                      | A maximum of five for each site. | <b>Fully managed switches:</b> M4250, M4300, M4350, M4500<br><b>Access points:</b> WBE718, WBE758                             |

| User Role               | Rights                                                   | Number of roles allowed           | Supported models                                                                                  |
|-------------------------|----------------------------------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Local Site Guest</b> | Can view data but cannot modify, add, or delete content. | A maximum of three for each site. | <b>Fully managed switches:</b> M4250, M4300, M4350, M4500<br><b>Access points:</b> WBE718, WBE758 |

## Add a user account

You can add a user account in the controller to assign specific access control permissions, ensuring users can only perform authorized actions.

### To add a user role:

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

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

3. If you set up more than one site, from the **Site** menu, select the site.  
The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. In the upper right of the page, click the **admin** menu, and select **Account Management**.  
The Account Management page displays.

5. Click the **+ Add User** icon.  
The Add User page displays.

6. In the **User Name** field, enter a user name.  
The user name can only contain letters, numbers, underscores (\_), and hyphens (-).

7. In the **Email** field, enter an email address.

8. In the **Password** field, enter a password, and repeat the password in the **Confirm Password** field.  
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.
9. In the **Password Hint** field, enter a password hint.  
The password hint displays on the controller login page.
10. In the **Phone no** field, enter a telephone number.  
This step is optional.
11. From the **User Type** menu, do one of the following:
  - Select **Administrator**, and from the **Default Site** menu, select a default site.
  - Select **Local Site Manager** and do the following:
    - a. From the **List of Managed Sites** menu, select managed sites.
    - b. From the **List of Guest Sites**, select guest sites.
    - c. From the **Default Site** menu, select a default site.
  - Select **Local Site Guest**, and from the **Default Site** menu, select a default site.
12. Click the **Add** button.  
Your settings are saved. The user account displays in the table on the Account Management page.

# Manage Devices

The controller lets you centrally configure managed devices listed in the Managed Devices table, or onboard devices from the Discovered Devices table. You can manage and configure both physical and virtual devices.

 **NOTE:** This chapter describes management options through the controller. For information about configuring *individual* devices after they are onboarded to the controller, see the user manual.

This chapter includes the following sections:

- [Add one or more devices to a site](#)
- [Add a single discovered device to a site](#)
- [Add multiple discovered devices to a site simultaneously](#)
- [Add an undiscovered physical device to a site](#)

## Add one or more devices to a site

Physical devices that the controller discovers are listed in the Discovered Devices table for a site. If a device does not display in the Discovered Devices table for a site, you can manually add the device as a managed device to the site by specifying the device IP address and access credentials.

You can add multiple virtual devices of the same model. You can also add multiple physical devices of the same model if the devices are listed in the Discovered Devices table for a site and are in factory default state or all have the same password.

During initial setup of the controller, if you already set up a global site SSID and specified the region and country for WiFi operation, or if you already added an access point (AP) to a site, you can use this procedure to add another AP to the site.

 **NOTE:** After the controller onboards the device, the controller replaces the device password with the site password.

 **CAUTION:** The firmware that a device is running before being onboarded by the controller does not support the controller functions. When you let the controller onboard a device, the controller pushes the latest firmware *with* controller functions to the device. This firmware update is necessary because the controller cannot manage the device without the firmware update.

If the device displays in the Discovered Devices table, see one of the following sections:

- [Add a single discovered device to a site](#) on page 23
- [Add multiple discovered devices to a site simultaneously](#) on page 24

If the device does not display in the Discovered Devices table, see [Add an undiscovered physical device to a site](#) on page 26.



**NOTE:** NETGEAR Insight and the controller are mutually exclusive management methods. If a device is already managed by NETGEAR Insight, the controller cannot onboard the device. For the controller to onboard the device, you must first disable NETGEAR Insight, or for an access point, reset the device to factory defaults.

## Add a single discovered device to a site

Devices that the controller discovers are generally listed in the Discovered Devices table for a site, that is, the device is a discovered device.

### To add a single discovered device to a site:

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

The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.  
The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select the check box to display **All**, **Physical Devices**, or **Virtual Devices**.  
By default, all managed devices display. Use the **Device Model** field to select individual devices.
5. Click the **Onboard** button for the device.  
A warning pop-up window displays.



**NOTE:** If the physical device matches a pre-configured virtual model name, serial number, or base MAC address of a virtual device, the Virtual Device Onboard pop-up window displays. Follow the steps in [Onboard a physical device using virtual device configurations](#) on page 72 to onboard a pre-configured virtual device to the new physical device.

6. Click the **Continue** button.

The Add Device pop-up window displays.

7. To let the controller onboard the device so that it can take control of the device, specify one of the following options for the device password:

- **Custom device password:** If the device uses a custom device password, enter it.
- **Default device password:** To automatically enter the default device password, turn on the **Use device default password** toggle so that it displays blue or green and is positioned to the right.

The device must be in factory default state.

If you are adding an AP, select this option. An AP must be in factory default state.

- **Site password:** To automatically enter the controller site password, turn on the **Use controller site password** toggle so that it displays blue or green and is positioned to the right.

8. Click the **Single** 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 the firmware version on the device does not support the controller, the controller automatically updates the firmware, after which the device restarts. When these processes are complete, the device becomes a managed device and moves to the Online state. This process might take up to 10 minutes.

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

## Add multiple discovered devices to a site simultaneously

Devices that the controller discovers are generally listed in the Discovered Devices table for a site, that is, the devices are discovered devices.

These are the requirements for adding multiple discovered devices to a site simultaneously:

- The devices must be of the same model, for example, the same model switch.
- The devices must have the same default password or custom password.

### To add multiple discovered devices to a site simultaneously:

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

The controller application opens and displays a login page.

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select the check box to display **All**, **Physical Devices**, or **Virtual Devices**.

By default, all managed devices display. Use the **Device Model** field to select individual devices.

5. Click the **Onboard** button for the device.

A warning pop-up window displays.



**NOTE:** If the physical device matches a pre-configured virtual model name, serial number, or base MAC address of a virtual device, the Virtual Device Onboard pop-up window displays. Follow the steps in [Onboard a physical device using virtual device configurations](#) on page 72 to onboard a pre-configured virtual device to the new physical device.

6. Click the **Continue** button.

The Add Device pop-up window displays.

7. To let the controller onboard the devices so that it can take control of the devices, specify one of the following options for the password of the devices:

- **Custom device password:** If the devices use a custom device password, enter it.
- **Default device password:** To automatically enter the default device password, turn on the **Use device default password** toggle so that it displays blue or green and is positioned to the right.

If you are adding multiple APs of the same model, select this option. Each AP must be in factory default state.

- **Site password:** To automatically enter the controller site password, turn on the **Use controller site password** toggle so that it displays blue or green and is positioned to the right.

8. Click the **Multiple** button.

Your settings are saved.

The devices are 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 devices (which replaces the local device password or default password). If the firmware version on the devices does not support the controller, the controller automatically updates the firmware, after which the devices restart. When these processes are complete, the devices become managed devices and move to the Online state. This process might take up to 10 minutes.

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

## Add an undiscovered physical device to a site

Physical devices that the controller discovers are listed in the Discovered Devices table for a site. If a device does not display in the Discovered Devices table for a site, the device is an undiscovered device. You can manually add the physical device as a managed device to the site by specifying the device IP address and access credentials.

### To add an undiscovered physical device to a site:

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

The controller application opens and displays a login page.

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Click the **Add Device** link.

The Add Device pop-up window displays.

Confirm the **Physical Device** radio button is selected on the pop-up window.

5. To let the controller onboard the device so that it can take control of the device, specify the following information:
  - a. Specify one of the following options for the device password:
    - **Custom device password:** If the device uses a custom device password, enter it.
    - **Default device password:** To automatically enter the default device password, turn on the **Use device default password** toggle so that it displays blue or green and is positioned to the right.

If you are adding an AP, select this option. An AP must be in factory default state.
    - **Site password:** To automatically enter the controller site password, turn on the **Use controller site password** toggle so that it displays blue or green and is positioned to the right.
  - b. In the **Device IP Address** field, type the IP address of the device. This step is required because the device is not automatically discovered by the controller.
6. Click the **Add** button.

Your settings are saved.



**NOTE:** If the physical device matches a pre-configured virtual model name, serial number, or base MAC address of a virtual device, the Virtual Device Onboard pop-up window displays. Follow the steps in [Onboard a physical device using virtual device configurations](#) on page 72 to onboard a pre-configured virtual device to the new physical device.

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 the firmware version on the device does not support the controller, the controller automatically updates the firmware, after which the device restarts. When these processes are complete, the device becomes a managed device and moves to the Online state. This process might take up to 10 minutes.

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

# Manage Network Profiles

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

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

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

During the device onboarding process (see [Set Up the Controller](#) on page 9), the controller does the following:

- Pulls all network profiles that are configured on the fully managed switches at the site.
- Pushes the collected network profiles to all onboarded devices at the site.

This chapter includes the following sections:

- [Overview of preconfigured AV profile templates](#)
- [About timing and clocks](#)
- [About the global site SSID](#)
- [Add a network profile](#)
- [Edit the controller's default network profile](#)
- [Edit a non-default network profile](#)
- [Set up an open or secure WiFi network](#)
- [Set up a WiFi network with Multi PSK](#)

## Overview of preconfigured AV profile templates

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

The controller provides the following preconfigured AV profile templates:

- **Allen & Heath gigaACE/GX:** Use this template to connect two audio devices from Allen & Heath in a Layer 2 VLAN only, across one or multiple switches. The supported protocols include gigaACE and GX.
- **AJA AV Network:** Use this template to connect AJA Dante AV systems for quick auto-detection and for ease of configuration..

- **Audio AES67:** Use this template to connect the switch to connect IP Audio AES67 InterComm devices and their controller. By default, this profile enables PTP TC.
- **AUDAC Audio and Control Network:** Use this template to connect AUDAC devices and AUDAC devices requiring separation of audio and control traffic into different VLANs. This profile is compatible with Dante and AES67. By default, this profile enables PTP TC.
- **Audio Audio-Technica:** Use this template to connect Audio-Technica Commercial Audio microphones, speakers, digital mixers, and wireless systems.
- **Audio Basalte Multiroom:** Use this template to connect IP Basalte Plano, Aalto, and Ceilo Speaker systems and controllers.
- **Audio Genelec Smart IP:** Use this template to connect Genelec Smart IP active PoE+ loudspeakers and various control systems.
- **Audio Dante:** Use this template to connect the switch to Dante audio devices and their controller. This template can support products such as Audinate, AED, Biamp, Bose, Genelec, Harman, RTS, Sennheiser, Shure, Trinnov Audio, and Waves. By default, this profile enables PTP TC.
- **Audio Q-SYS:** Use this template to connect the switch to IP Audio Q-SYS devices and their controller.
- **Audio Soundgrid:** Use this template to connect the switch to IP Audio SoundGrid devices and their controllers.
- **Audio Video AVB:** Use this template to connect an M4250 series or M4350 series switch to IP audio devices that support Audio Video Bridging (AVB). This profile does not support PTP TC. AVB is not supported on M4300 series and M4500 series switches.
- **Audio Video AVB MILAN:** Use this template to connect an M4250 series or M4350 series switch to IP audio devices that support Audio Video AVB MILAN.
- **Audio Video AVB MILAN with Dante PTPv1 PTPv2 or AES67:** Use this template to connect an M4250 series or M4350 series switch to IP audio devices that support Audio Video AVB and Dante or AES67. MTU is 1500 by default and PTP-TC is not configurable on that VLAN. AVB is not supported on M4300 series and M4500 series switches.
- **Audio Video SMPTE:** Use this template to connect AES67 Audio and ST 2110 Video devices and their controllers. This profile applies to M4350 series models M4350-16V4C, M4350-16V4C, M4350-40F4C, M4350-24F4X, M4350-8M2V, M4350-16M4V, M4350-24M4X4V, and M4350-40X4C. When you configure the PTPv2 BC/GM settings and select the PTPv2 profile (AES67, SMPTE-2059-2, or AES-R16-2016), these settings apply globally to the switch. For more information, see the user manual.
- **Avid S6L:** Use this template to connect the switch to Avid VENUE | S6L Live Sound Ethernet AVB ports “A” or “B” devices. This profile is supported on all M4250 Series and M4250 Series switches that support AVB and is supported on VLAN 1 (the default VLAN profile) only. Only one VLAN can exist on the switch when you use this profile. No other VLAN IDs are accepted. By default, this profile enables Redundancy Mode A. This means the switch with mode A is

the grandmaster clock and the switch with mode B is the grandmaster clock backup.

- **AVoIP Lightware AV Network:** Use this template to connect Lightware AVoIP endpoints and their control devices from the UBEX product family.
- **BirdDog AV Network:** Use this template to connect BirdDog AV systems for quick auto-detection and for ease of configuration. By default, this profile enables PTP TC.
- **BluOS AV:** Use this template to connect BluOS AV systems for quick auto-detection and for ease of configuration.
- **Blustream Multicast:** Use this template to connect Blustream Multicast Video over IP products, including those that feature Dante / AES67.
- **Crestron DigitalMedia AV Network:** Use this template to connect the switch to Crestron DM NVX (video), Crestron DM NAX (audio), Creston cameras (NDI), computers, computers, and other Crestron Control network devices.
- **Data:** Use this template to connect the switch to computers and other control network devices. CobraNet is supported in a VLAN other than VLAN 1. This profile does not support PTP TC.
- **Default:** Use this template as the default VLAN 1 profile. You can overwrite this profile with another profile on VLAN 1 after initial switch configuration. The default profile automatically applies after a factory reset. This profile does not support PTP TC.
- **DICENTIS Conference system profile:** Use this template to connect the switch to DICENTIS Conference system equipment with RPVSTP and IGMP support. By default, this profile enables PTP TC.

You cannot apply this profile on VLAN1 or the management VLAN.



**NOTE:** When you configure this profile on a site, the RPVSTP protocol is enabled. If you configure this profile on a site with more than 32 network profiles (VLANs), a warning pop-up displays advising that the protocol cannot operate successfully.



**NOTE:** This template is not supported on M4500 series switches. If you configure this profile on a site for an M4500 series switch, the controller applies the Audio Dante profile instead.

- **ETC Lighting:** Use this template to connect the switch to ETC Lighting and control devices. This profile does not support PTP TC.
- **G&D KVM-over-IP:** Use this template to connect the switch to Guntermann & Drunck KVM-over-IP Solutions devices. By default, this profile does not support PTP TC. However, you can manually enable PTP settings.
- **HARMAN Professional AV Network:** Use this template on the switch to connect HARMAN Professional product lines together. This profile does not support PTP TC.
- **Hybrid SMPTE AES67 Core and Audio AES67 Edge:** Use this template to connect a mixed configuration of an M4350 series core switch that has the SMPTE profile enabled and a PTPv2 BC/GM configuration and M4250, M4300, and M4350 series edge switches that have

the Audio AES67 profile enabled and a PTP TC configuration.

- **Kramer AV:** Use this template to connect Kramer AV over IP solutions for audio and video distribution over up to four different VLANs (video, control, audio, and aux).
- **Lighting:** Use this template to connect the switch to streaming ACN (sACN), Art-Net, and MA-NET3 lighting devices for controlling lighting equipments. This profile does not support PTP TC.
- **Nice Home Management:** Use this template to connect the switch to Nice Home Management systems, including IPD Dante with either unicast or multicast configurations. Auto-Provision automatically detects Nice devices on a factory-default switch by matching their MAC OUI (F8:57:2E) and creates a Nice network profile on VLAN 1 across all switch ports. When the switch is in factory default mode, Auto-Provision is enabled by default. By default, this profile enables PTP TC.
- **NUCLEUS Converged AV Network:** Use this template to connect the switch to EvertzAV NUCLEUS Session Manager and UXP gateways on a single converged network. This profile does not support PTP TC.
- **Pharos Lighting Control:** Use this template to connect the switch to Pharos Control devices. This profile does not support PTP TC.
- **Pharos Lighting Data:** Use this template to connect the switch to Pharos Lighting devices. This profile does not support PTP TC.
- **Poly StudioNet Modular Room:** Use this template to connect the switch to HP Poly StudioNet Modular Room peripherals. You can create multiple instances of this profile on a switch and it can coexist with other profiles on a switch. You can configure this profile on all switch models. By default, this profile enables PTP TC.
- **Shure Converged Audio and Control Network:** Use this template to connect the switch to Shure devices requiring audio and control traffic on a single VLAN. Compatible with Dante, AES67, QSYS, and Biamp Dante devices. By default, this profile enables PTP TC. This template is not supported on M4300 series switches.
- **Shure Split Audio and Control Network:** Use this template to connect the switch to Shure devices requiring separation of audio and control traffic into different VLANs. Compatible with Dante, AES67, QSYS, and Biamp Dante devices. This template is only supported on M4250 series switches.
- **Sennheiser TeamConnect Bar S - Single Domain Mode:** Use this template to connect the switch to a Sennheiser TeamConnect Bar S device in single domain mode. By default, this profile enables PTP TC.
- **Sonos:** Use this template to connect the switch to a Sonos smart home sound system. This profile does not support PTP TC.
- **Telos Alliance / Livewire+ AES67:** Use this template to connect Telos Alliance Livewire+ products and other products that are AES67 compliant. By default, this profile enables PTP TC.

- **Unite Audio:** Use this template to connect to Glidenet audio streaming products for PCM, multichannel, ultra high definition, and compressed bit-perfect audio over networks.
- **URC Automation:** Use this template to connect the switch to URC Automation HDA devices and their controllers. This profile is supported on all M4250 Series and M4350 Series switches that support AVB.
- **Video:** Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

This profile does not support PTP TC.

- **Video:** Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

This profile does not support PTP TC.

- **Video NDI4:** Use this template to connect the switch to video devices and cameras that support Network Device Interface (NDI) version 4 with multi-TCP (mTCP) transport. This template can support products from companies such as AVer, Avonic, BirdDog, Bolin, Canon, JVC, Kiloview, Lumens, Magewell, Ross, Panasonic, PTZOptics, Sony, and Vizrt, as well as products from other companies.

This profile does not support PTP TC.

- **Video NDI5 / NDI6 with Dante, Q-Sys or AES67 audio:** Use this template to connect the switch to video devices and cameras that support NDI version 5 or version 6 with Reliable User Datagram Protocol (RUDP). Audio Dante, Q-SYS, or AES67 is supported at the same time in the same VLAN. This template can support products from companies such as AVer, Avonic, BirdDog, Bolin, Canon, JVC, Kiloview, Lumens, Magewell, Ross, Panasonic, PTZOptics, Sony, and Vizrt, as well as products from other companies.
- **Video with AES67 audio:** Use this template to connect the switch to IP video devices and their controllers when AES67 audio is supported in the same VLAN. This template can support products such as NVX, AMX, ZeeVee-Kramer, Aurora, Atlona, ATEN, CYP, Liberty, Visionary, Wyrestorm, Yealink, Extron NAV, Dante AV, Muxlab, Netvio, VuWall, IPMX, and SDVoE.

By default, this profile enables PTP TC.

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

SDVoE.

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

The MTU for the packet is 1,500 bytes. For Jumbo Frames, use another profile template such as Video with AES67 audio or Dante.

- **Visionary AV Network:** Use this template to connect the switch to Visionary AV systems for quick auto-detection and for ease of configuration. This profile does not support PTP TC.
- **Visionary Advanced Multi-Domain:** Use this template to configure video, audio, and expansion together. This profile does not support PTP TC.

## About timing and clocks

The controller can support different types of timing and clock features.

## About Audio video bridging

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

AVB is supported on the following switches:

- M4250 series switches
- M4350 series switches

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

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

As of firmware version 13.0.4.17 for the M4250 series switches, a license is no longer required for the AVB feature. The M4350 series switches support AVB and do not require a license either.

## About PTP residency time stamping and network profiles

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

The switch supports a PTP end-to-end transparent clock that is used in the *PTP residency time stamping* feature. Most network profiles support PTP residency time stamping. Whether the feature is available, enabled by default, or disabled by default, depends on the network profile.

For more information, see [Overview of preconfigured AV profile templates](#) on page 28.

You can enable or disable PTP residency time stamping per network profile (see [Add a network profile](#) on page 35).

The following network profiles do not support PTP residency time stamping and you cannot configure the feature in the controller UI:

- Audio-Video AVB 802.1AS (audio video bridging, or AVB) is supported on the M4250 series and M4350 series switches but is incompatible with PTP residency time stamping. AVB is not supported on M4300 series and M4500 series switches. For more information, see [About Audio video bridging](#) on page 33.
- Data
- Lighting
- NUCLEUS Converged AV Network
- Sonos
- Video
- Video NDI4
- Visionary AV Network



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

## About the global site SSID

If you let the controller onboard one or more access points (APs), you must set up a global site SSID, which is the default WiFi network that is associated with the Default network profile with VLAN ID 1.

You can either add the global site SSID when you set up the controller (see [Access the controller for the first time and set up the default site](#) on page 12) or add it when you onboard the first AP at a site (for more information, see the user manual).

After setup, you cannot delete the global site SSID or change the type of WiFi security, but you can add other SSIDs (WiFi networks) and apply them to the Default network profile and other profiles. Although you cannot make another WiFi network the global site SSID, you do not need to use the global site SSID if its settings do not suit your needs at the site (that is, you can disable WiFi for the global site SSID).

The global site SSID has the following default settings:

- **VLAN:** The default VLAN is VLAN 1 with the name Default. You cannot change the VLAN ID.
- **Radio band:** The 2.4 GHz radio and 5 GHz radio are enabled, but you can disable one of the radios. If applicable to your AP, you cannot enable the 6 GHz radio for the global site SSID, but you can add another SSID with security settings that can be supported by the 6 GHz

radio.

- **Security:** The WiFi security is WPA2 - MPSK. You cannot change this type of security, but you can do the following:
  - Change the WiFi password for the global key name.
  - Enable or disable client isolation within an MPSK group and isolation from other groups.
  - Add, change, or remove additional MPSK groups, each consisting of a VLAN ID, key name, password, and isolation definition.

For more information about WPA2 - MPSK, see [Set up a WiFi network with Multi PSK](#) on page 49.

## Add a network profile

When you add a network profile, you are defining the PTP residency time stamping setting (depending on whether the profile supports this feature), the global site SSID or WiFi settings (depending on whether APs are present in your network), and the ports that participate in the profile. You can also configure routing and related features.

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

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

The controller application opens and displays a login page.

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Site Settings**.

The Network Profiles page displays.

5. Click the **Create New Profile** link.

The Create New Profile page displays the Profile Template section.

6. From the **Profile Templates** menu, select an AV profile template.

7. To use the network profile as the default VLAN profile for the site, turn on the **Use As Default VLAN Profile** toggle so that it displays blue or green and is positioned to the right.

8. Click the **Next** button.

The Create New Profile page displays the Profile Settings section.

9. In the **Profile Name** field, enter a name for identification purposes.



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

10. In the **VLAN ID** field, enter the VLAN ID to which the traffic of the profile must be assigned.

11. To add a color to the network profile for visual representation, click the box in the **Color** field, select a color, and click the **OK** button.

For more color options, click the drop-down arrow on the left of the Preset Colors window.

The unique color indicates what network profile a port supports when you tag a port to a network profile in [step 18](#).

The profile color also displays on the physical front panel LEDs of the following switches: M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

12. Depending on the AV profile template that you selected in [step 6](#), you can enable or disable PTP residency time stamping (TC) for the profile (for more information, see [About PTP residency time stamping and network profiles](#) on page 33):

- **Enable PTP TC:** Turn on the **PTP residency time stamping** toggle so that it displays blue or green and is positioned to the right.
- **Disable PTP TC:** Turn off the **PTP residency time stamping** toggle so that it displays gray and is positioned to the left.

13. Click the **Next** button.

The following occurs, depending on whether your network includes onboarded access points (APs):

- **APs in the network:** The Edit SSID pop-up window displays. All WiFi networks that use the same VLAN as the network profile display. Do the following:
  - a. In the SSID Name column, select a radio button for an existing SSID.
  - b. Click the **Apply** button. The Wireless Settings page displays.
- **No APs in the network:** The Port Assignment section displays. Go to [step 17](#).

14. (This step is for a network with APs.) To keep WiFi disabled for the network profile, leave the **WiFi** toggle disabled so that it displays gray and is positioned to the left, and then go to [step 16](#).

Otherwise, go to the next step.

15. (This step is for a network with APs.) To enable WiFi for the network profile, do the following:
- Click the **WiFi** toggle so that it displays blue or green and is positioned to the right.
  - Click one of the following mutually exclusive toggles so that the toggle displays blue or green and is positioned to the right:
    - **GLOBAL SITE SSID**: Use the global site SSID for the network profile. This is the default selection if you enable WiFi. With this selection, the **Dedicated SSID for this VLAN** toggle displays gray and is positioned to the left.
- ❗ **NOTE:** You can also click the **Add MPSK** link and add a new WiFi network. For more information, see the user manual.
- **Dedicated SSID for this VLAN**: Use a dedicated custom WiFi network for the network profile and associated VLAN. You must select the WiFi network from the **SSID** menu.
- With this selection, the **GLOBAL SITE SSID** toggle displays gray and is positioned to the left.
- ❗ **NOTE:** You can also click the **Add New SSID** link and add a new WiFi network. For more information, see the user manual.
16. Click the **Next** button.
- The Create New Profile page displays the Port Assignment section.
17. Click the graphical display of the switch on which you want to add ports to the network profile.
- The page adjusts to display the switch ports of the selected switch. If a switch is already tagged to a network profile, the port displays the unique color you set in [step 11](#).
18. To select all ports do the following:
- **Add all ports as untagged ports**: Click the **Untag all** button.  
All ports are flagged.
  - **Add all ports as tagged all ports**: Click the **Tag all** button.  
All ports are marked with a T (for tagged).
  - **Remove all ports**: Click the **Remove all** button.  
All ports are unflagged.
19. To select or change individual ports, do the following:
- **Add a port as an untagged port**: Click the port so that it is flagged.
  - **Add a port as a tagged port**: Click the port so that it is marked with a T (for tagged).
  - **Remove a port**: Click the port so that it is unflagged.
20. To add ports on another switch to the network profile, repeat the previous three steps.

21. When you are done adding ports to the network profile, click the **Apply** button.  
The Create New Profile pop-up window displays.
22. Click the **Yes** button.  
The VLAN Routing Planner pop-up window displays.
23. Do one of the following:
  - **Do not add routing to the network profile:** Click the **No** button.  
Your settings are saved but routing is not added to the network profile. (You can add routing later.) The profile is added to the table on the Network Profiles page. You completed this procedure.
  - **Add routing to the network profile:** Click the **Yes** button.  
Your settings are saved and the profile is added to the table on the Network Profiles page. The VLAN Routing Planner page displays. Continue with the following steps to add routing to the network profile.
24. To enable routing on all switches that use the network profile, select the **Enable Routing on all Switches** check box.
25. To configure the routing, DHCP server, and IGMP options for an individual switch that uses the network profile, click the graphical display of the switch.  
A pop-up window displays.
26. Select one or more of the following radio buttons:
  - **Enable Routing:** Select the radio button to enable routing on the switch. If you already routing on all switches in a previous step, the radio button is already selected.
  - **DHCP Server:** Select the radio button to configure the switch as the DHCP server in the routing VLAN. Routing must be enabled for the switch to function as a DHCP server.
  - **Core Switch:** Select the radio button to configure the switch as the core switch in the routing VLAN, which means that the routing, DHCP server, and IGMP querier options are automatically enabled.
  - **IGMP Querier:** Select the radio button to configure the switch as the IGMP querier for the network profile. Routing does not need to be enabled for a switch to function as the IGMP querier for a network profile (VLAN).
27. Click the **Apply** button.  
The pop-up window closes.
28. To configure the routing, DHCP server, and IGMP options for another switch, repeat the previous three steps.
29. When you have configured all switches, click the **Apply** button.  
A pop-up window displays.

30. Click the **Go to VLAN Routing** button.

The Basic Configuration page displays. Your routing settings, DHCP server setting, IGMP setting, or all of these settings are saved.



**NOTE:** For information about changing the DHCP server or IGMP querier settings, see the user manual.

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

## Edit the controller's default network profile

You can change the AV profile template, color, and switch port assignments for the network profile that is the *default* profile on the controller. The controller automatically assigns the default AV profile on VLAN 1 as the default for the Engage site and any new physical or virtual sites created.



**NOTE:** You can change the default network profile so that another profile than the controller's default profile becomes the default profile for your site.

The following rules apply to the controller's default network profile:

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

For information about editing a profile that is *not* the default profile, see [Edit a non-default network profile](#) on page 42.

For information about enabling VLAN routing for the network profile, see the user manual.

For information about setting the network profile as the management VLAN, see the user manual.

### To edit the default network profile:

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

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Site Settings > Network Profiles**.

The Network Profiles page displays.

5. In the table, for the default profile, click the **3 dots** icon and select **Edit**.

The Profile Template settings displays.

6. To change the AV profile template, from the **Profile Templates** menu, select another AV profile template.

The Profile Description section displays a summary of the network profile.

7. Click the **Next** button.

The Profile Settings section displays.

You cannot change the profile template and VLAN ID.

8. Change the following information as needed:

- **Profile Name:** A name for identification purposes.
- **Color:** Click the box in the **Color** field, and select a color. This unique color indicates what network profile a port supports when you want to tag a port to a network profile in [step 13](#).

The profile color also displays on the physical front panel LEDs of the following switches: M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

9. Depending on the AV profile template that you selected in [step 6](#), you can enable or disable PTP residency time stamping (TC) for the default profile (for more information, see [About PTP residency time stamping and network profiles](#) on page 33):

- **Enable PTP TC:** Turn on the **PTP residency time stamping** toggle so that it displays blue or green and is positioned to the right.
- **Disable PTP TC:** Turn off the **PTP residency time stamping** toggle so that it displays gray and is positioned to the left. By default, PTP TC is disabled.

10. Click the **Next** button.

The following occurs, depending on whether your network includes onboarded access points (APs):

- **APs in the network:** The Edit SSID pop-up window displays. All WiFi networks that use the same VLAN as the network profile display. Do the following:
  - a. In the SSID Name column, select a radio button for an existing SSID.
  - b. Click the **Apply** button. The Wireless Settings page displays.
- **No APs in the network:** The Port Assignment section displays. Go to [step 14](#).

11. (This step is for a network with APs.) To entirely disable WiFi for the network profile, click the **WiFi** toggle so that it displays gray and is positioned to the left, and then go to [step 13](#). Otherwise, go to the next step.

## 12. (This step is for a network with APs.) To keep WiFi enabled, click one of the following mutually exclusive toggles so that the toggle displays blue or green and is positioned to the right:

- **GLOBAL SITE SSID:** Use the global site SSID for the network profile. This is the default selection if you enable WiFi. With this selection, the **Dedicated SSID for this VLAN** toggle displays gray and is positioned to the left.



**NOTE:** You can also click the **Add MPSK** link and add a new WiFi network. For more information, see the user manual.

- **Dedicated SSID for this VLAN:** Use a dedicated custom WiFi network for the network profile and associated VLAN. You must select the WiFi network from the **SSID** menu. With this selection, the **GLOBAL SITE SSID** toggle displays gray and is positioned to the left.



**NOTE:** You can also click the **Add New SSID** link and add a new WiFi network. For more information, see the user manual.

13. Click the **Next** button.

The Port Assignment section displays.

14. To change port assignments for a switch, point to the switch and click.  
The switch ports display.

If a switch is already tagged to a network profile, the port displays the unique color you set in [step 8](#).

## 15. To select or unselect a port, click the port one or more times:

- **Check mark:** The port is selected and untagged.
- **Check mark with a T:** The port is selected and tagged.
- **No check mark:** The port is not selected.

16. To select or unselect all ports, click one of the following buttons:
  - **Untag all:** All ports are selected and untagged.
  - **Tag all:** All ports are selected and tagged.
  - **Remove all:** None of the ports are selected.
17. Click the **Apply** button.  
A pop-up window displays.
18. Click the **Confirm** button.  
Your settings are saved. The altered profile displays in the table on the Network Profile page.
19. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

## Edit a non-default network profile

You can change the profile name, color, and switch port assignments for a network profile that is *not* the default profile.

For information about editing the default profile, see [Edit the controller's default network profile](#) on page 39.

For information about enabling VLAN routing for the network profile, see the user manual.

For information about setting the network profile as the management VLAN, see the user manual.



**NOTE:** Because the following procedure is generic, it might include options that are *not* available for the network profile, or it might not include options that *are* available for the network profile, or the options are presented in a different order.

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

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

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Site Settings > Network Profiles**.

The Network Profiles page displays.

5. In the table, for the profile that you want to edit, click the **3 dots** icon and select **Edit**.

The Profile Template settings displays.

6. To change the AV profile template, from the **Profile Templates** menu, select another AV profile template.

The Profile Description section displays a summary of the network profile.

7. Click the **Next** button.

The Profile Settings section displays.

You cannot change the profile template and VLAN ID.

8. Change the following information as needed:

- **Profile Name:** A name for identification purposes.
- **Color:** Click the box in the **Color** field, and select a color.

This unique color indicates what network profile a port supports if you tag a port to a network profile in [step 15](#).

The profile color also displays on the physical front panel LEDs of the following switches: M4350-24F4X, M4350-8M2V, M4350-24M4X4V, and M4350-40F4C.

9. Depending on the AV profile template that you selected in [step 6](#), you can enable or disable PTP residency time stamping (TC) for the default profile (for more information, see [About PTP residency time stamping and network profiles](#) on page 33):

- **Enable PTP TC:** Turn on the **PTP residency time stamping** toggle so that it displays blue or green and is positioned to the right.
- **Disable PTP TC:** Turn off the **PTP residency time stamping** toggle so that it displays gray and is positioned to the left. By default, PTP TC is disabled.

10. Depending on the AV profile template that you selected in [step 6](#), you can enable or disable flood multicasting.

- **Enable multicast flooding:** Turn on the **Flood Multicast** toggle so that it displays green and is positioned to the left. This setting allows the switch to flood the multicast packets at the VLAN level.
- **Disable multicast flooding:** Turn off the **Flood Multicast** toggle so that it displays gray and is positioned to the left. By default, multicast flooding is disabled.



**NOTE:** The Force Multicast feature is not available on non-multicast network profiles.

11. Click the **Next** button.

The following occurs, depending on whether your network includes onboarded access points (APs):

- **APs in the network:** The Edit SSID pop-up window displays. All WiFi networks that use the same VLAN as the network profile display. Do the following:
  - a. In the SSID Name column, select a radio button for an existing SSID.
  - b. Click the **Apply** button. The Wireless Settings page displays.
- **No APs in the network:** The Port Assignment section displays. Go to [step 15](#).

12. (This step is for a network with APs.) To entirely disable WiFi for the network profile, click the **WiFi** toggle so that it displays gray and is positioned to the left, and then go to [step 14](#). Otherwise, go to the next step.

13. (This step is for a network with APs.) To keep WiFi enabled, click one of the following mutually exclusive toggles so that the toggle displays blue or green and is positioned to the right:

- **GLOBAL SITE SSID:** Use the global site SSID for the network profile. This is the default selection if you enable WiFi. With this selection, the **Dedicated SSID for this VLAN** toggle displays gray and is positioned to the left.



**NOTE:** You can also click the **Add MPSK** link and add a new WiFi network. For more information, .

- **Dedicated SSID for this VLAN:** Use a dedicated custom WiFi network for the network profile and associated VLAN. You must select the WiFi network from the **SSID** menu. With this selection, the **GLOBAL SITE SSID** toggle displays gray and is positioned to the left.



**NOTE:** You can also click the **Add New SSID** link and add a new WiFi network. For more information, see the user manual.

14. Click the **Next** button.

The Port Assignment section displays.

15. To change port assignments for a switch, point to the switch and click.  
The switch ports display.  
If a switch is already tagged to a network profile, the port displays the unique color you set in [step 8](#).
16. To select or unselect a port, click the port one or more times:
  - **Check mark:** The port is selected and untagged.
  - **Check mark with a T:** The port is selected and tagged.
  - **No check mark:** The port is not selected.
17. To select or unselect all ports, click one of the following buttons:
  - **Untag all:** All ports are selected and untagged.
  - **Tag all:** All ports are selected and tagged.
  - **Remove all:** None of the ports are selected.
18. Click the **Apply** button.  
A pop-up window displays.
19. Click the **Apply** button.  
Your settings are saved. The altered profile displays in the table on the Network Profile page.
20. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

## Set up an open or secure WiFi network

The information in this section applies only if your network includes access points (APs).

You can set up an open WiFi network without authentication and encryption, and open WiFi network without authentication but with encryption, or a WiFi network with both authentication and encryption.

If you plan to use WPA2 Enterprise security or WPA3 Enterprise security for your WiFi network, first set up RADIUS servers (for more information, see the user manual).

### To set up a WiFi network:

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

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Site Settings > Wireless**.

The SSID page displays.

5. Click the **+ Add New SSID** link.

The Create New SSID page displays.

6. In the **SSID** field, type the WiFi network name.

The SSID is the WiFi network name. Type a name for the SSID with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

For a WiFi device to be able to connect to the AP, the SSID on the WiFi device must match the SSID of the AP.

7. Select the WLAN Status **Enable** or **Disable** radio button, which determines if the SSID is enabled or disabled:

- **Enable:** After configuration, the SSID is enabled and can be used.
- **Disable:** After configuration, the SSID is disabled and cannot be used.

8. Depending on the capability of the AP, select the Radio Band **2.4 GHz**, **5 GHz**, or **6 GHz** check box, or a combination of these check boxes.

Your selection determines the radio band on which the SSID broadcasts and the WiFi security options that are available.

9. Specify the WiFi security by selecting an option from the **Security** menu and, if applicable, set a passphrase in the **Passphrase** field or select an option from the **Encryption** menu:
- **OPEN:** A legacy open WiFi network does not provide any security. Any WiFi device can join the network. Clients are not authenticated, traffic is not encrypted. We recommend that you do *not* use a legacy open WiFi network but configure WiFi security. However, a legacy open network might be appropriate for a WiFi hotspot.
  - **OWE:** The WiFi enhanced open feature is enabled. This feature is based on opportunistic wireless encryption (OWE). In the background, the encryption is set to CCM mode protocol (CCMP). The WiFi network can only accept clients that support the WiFi enhanced open feature.
  - **WPA2 - PSK:** For APs that support the 6 GHz band, this option is not available if the 6 GHz band is enabled. This option uses AES encryption. This type of security enables only WiFi devices that support WPA2 to join the VAP. In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To display the passphrase in clear text, click the eye icon.
  - **WPA2 - MPSK:** For APs that support the 6 GHz band, this option is not available if the 6 GHz band is enabled. Multi PSK (MPSK) lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. In a way, Multi PSK lets you create different sub WiFi networks on a single WiFi network. When connecting to the WiFi network, the passphrase that a user enters determines the VLAN that the WiFi client is placed in.

Because this security option is slightly more complex, it is documented separately. For more information, see [Set up a WiFi network with Multi PSK](#) on page 49. This option is also the default security option for the global site SSID (see [About the global site SSID](#) on page 34).

- **WPA2 - Enterprise:** For APs that support the 6 GHz band, this option is not available if the 6 GHz band is enabled. This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA2 Enterprise security to function, you must set up RADIUS servers (for more information, see the user manual).

From the **Encryption** menu, select the data encryption mode:

- **TKIP + AES.** This type of data encryption enables WiFi devices that support either WPA or WPA2 to join the controller's WiFi network. This is the default mode.
- **AES.** This type of data encryption provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. Therefore, if your network includes such older devices, select **TKIP + AES** encryption.
- **WPA3 - PSK:** This option is the most secure personal authentication option. WPA3 uses SAE encryption and enables only WiFi devices that support WPA3 to join the VAP. WPA3 provides a secure connection but some legacy WiFi devices do not detect WPA3

and support only WPA2. If your network also includes WPA2 devices, select **WPA3/WPA2 - PSK** authentication.

In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To display the passphrase in clear text, click the eye icon.

- **WPA3/WPA2 - PSK:** This option is the default setting. It enables WiFi devices that support either WPA3 or WPA2 to join the VAP. This option uses SAE and AES encryption. WPA2 - PSK (which uses AES) is less secure than WPA3 - PSK (which uses SAE).

In the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the VAP, a user must enter this passphrase. To display the passphrase in clear text, click the eye icon.

- **WPA3 - Enterprise:** This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For WPA3 Enterprise security to function, you must set up RADIUS servers (for more information, see the user manual).

When you select WPA3 Enterprise security, the encryption is automatically set to GCMP256, which is a 256-bit encryption protocol.

10. From the **VLAN ID** menu, select the VLAN to which the WiFi network must be assigned.

11. Click the **Save** button.

Your changes are saved.

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

13. Make sure that a WiFi client can connect to the new WiFi network.

If the client cannot connect to the new WiFi network, check the following:

- If the WiFi-enabled computer or mobile device is already connected to another WiFi network in the area, ask the user to disconnect it from that WiFi network and connect it to the correct WiFi network. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- If the WiFi-enabled computer or mobile device is trying to connect to the network with its old settings (before the user changed the settings) ask the user to update the WiFi network selection in the WiFi-enabled computer or mobile device to match the current settings for the network.
- Does the WiFi device display as a connected client? If it does, it is connected to the network.
- Does the user try to connect using the correct WiFi network name (SSID) and password?
- If the WiFi authentication and encryption is set to WPA3 Personal, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi-enabled computer or mobile device.

## Set up a WiFi network with Multi PSK

The information in this section applies only if your network includes access points (APs).

Multi PSK (MPSK) lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. In a way, Multi PSK lets you create different sub WiFi networks on a single WiFi network. When connecting to the WiFi network, the passphrase that a user enters determines the VLAN that the WiFi client is placed in.

In addition to a VLAN and passphrase, you can associate a key identifier with the VLAN-to-passphrase mapping. The key identifier lets you identify the VLANs in the WiFi network for network monitoring purposes. For example, when you display WiFi clients, the key identifier can also display.

As examples of key identifiers, you could use terms such as corporatenetwork\_22, corporatenetwork\_23, and corporatenetwork\_24. These key identifiers (or the associated VLAN IDs) are not visible to a user trying to connect to the WiFi network: the user sees the SSID and enters the passphrase.

If you enable Multi PSK, the WiFi network's passphrase and VLAN are replaced by the passphrases and VLANs that are part of the Multi PSK configuration.

In addition, the following restrictions apply to Multi PSK:

- You cannot enable Multi PSK for a WiFi network in the 6 GHz band.
- You can configure Multi PSK on a maximum of four WiFi networks on an AP.
- Each WiFi network on which you configure Multi PSK can support a maximum of eight VLAN-to-passphrase mappings. (Within each WiFi network, each passphrase and key identifier must be unique.) An AP can support a maximum of 32 Multi PSK VLAN-to-passphrase mappings. For example, four WiFi networks each can support eight Multi PSK VLAN-to-passphrase mappings.
- Within a Multi PSK on a single WiFi network, you can map the same VLAN ID to different passphrases. You can also use the same VLAN ID for Multi PSK in different WiFi networks.
- If inter-VLAN routing is disabled in the network to which an AP is connected, the following applies:
  - WiFi clients that are connected to different VLANs on the same WiFi network (that is, the WiFi clients use different passphrases to connect to the same WiFi network) cannot communicate with each other and remain isolated.
  - WiFi clients that are connected to the *same* VLAN on different WiFi networks *can* communicate with each other.
- Multi PSK and the following features (which you can configure using the AP's device UI) are mutually exclusive:
  - Multi-link operation
  - Captive portal
  - mDNS gateway
  - NAT mode

- Client isolation



**NOTE:** Multi PSK is not available if the 6 GHz band is enabled.



**NOTE:** You cannot change the WiFi security for the global site SSID, which uses WPA2-MPSK. Although you can add additional SSIDs, you cannot make another SSID the global site SSID.

### To set up a WiFi network with Multi PSK:

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

The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.  
The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Site Settings > Wireless**.

The SSID page displays.

5. Click the **+ Add New SSID** link.

The Create New SSID page displays.

6. Specify the WiFi network name (SSID) name.

The SSID is the WiFi network name of the VAP. Enter a name for the SSID with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

For a WiFi device to be able to connect to the VAP, the SSID on the WiFi device must match the SSID of the VAP.

7. Select the WLAN Status **Enable** or **Disable** radio button, which determines if the SSID is enabled or disabled:
  - **Enable:** After configuration, the SSID is enabled and can be used.
  - **Disable:** After configuration, the SSID is disabled and cannot be used.

8. Depending on the capability of the AP, select the Radio Band **2.4 GHz**, **5 GHz**, or **6 GHz** check box, or a combination of these check boxes.  
Your selection determines the radio band on which the SSID broadcasts.
9. From the **Security** menu, select **WPA2 - MP SK**.  
The page adjusts.
10. Click the **+ Add Row** link.
11. Add a Multi PSK group:
  - **VLAN ID**: The VLAN ID, which is the VLAN that is associated with the VAP and that a WiFi client becomes a member of. The VLAN ID must be between 1 and 4094.
  - **Key Name**: The name or phrase that lets you identify the VLAN in the WiFi network for monitoring purposes. The maximum length is 30 alphanumeric characters, including the following special characters: hyphen (-) and underscore (\_).
  - **Passphrase**: The unique passphrase (WiFi password) that a user must enter to let the WiFi client connect to the associated VLAN of the WiFi network. The passphrase must be between 8 and 63 characters.
  - **Client Isolation within the Group**: You can isolate clients within a single Multi PSK group so that they cannot directly communicate with each other, except for communication over the Internet, which remains possible.
    - **Isolation enabled**: Turn on the toggle so that it displays blue or green and is positioned to the right. For additional security, you can enable client isolation so that clients that are associated with the same or different WiFi networks cannot communicate with each other.
    - **Isolation disabled**: Turn off the toggle so that it displays gray and is positioned to the left. By default, client isolation is disabled for a WiFi network (SSID or VAP), allowing communication between WiFi clients that are associated with the same or different WiFi networks on the AP.
  - **Group Isolation from Other Group/PSKs**: You can isolate clients from different Multi PSK groups so that they cannot directly communicate with each other, except for communication over the Internet, which remains possible.
    - **Isolation enabled**: Turn on the toggle so that it displays blue or green and is positioned to the right.
    - **Isolation disabled**: Turn off the toggle so that it displays gray and is positioned to the left.
12. To accept the settings for a Multi PSK group, click the flag button at the right.
13. To add another Multi PSK group, repeat the previous three steps.

14. Click the **Save** button.

Your changes are saved.

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

16. Make sure that a WiFi client can connect to the new WiFi network.

If the client cannot connect to the new WiFi network, check the following:

- If the WiFi-enabled computer or mobile device is already connected to another WiFi network in the area, ask the user to disconnect it from that WiFi network and connect it to the correct WiFi network. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- If the WiFi-enabled computer or mobile device is trying to connect to the network with its old settings (before the user changed the settings), ask the user to update the WiFi network selection in the WiFi-enabled computer or mobile device to match the current settings for the network.
- Does the WiFi device display as a connected client? If it does, it is connected to the network.
- Does the user try to connect using the correct WiFi network name (SSID) and password?
- If the WiFi authentication and encryption is set to WPA3 Personal, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi-enabled computer or mobile device.

# Manage Sites

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

This chapter includes the following sections:

- [Add a physical site](#)
- [Edit the network setup of a site](#)
- [Add a site user account](#)

## Add a physical site

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

You can add multiple physical sites to the controller.

### To add a physical site to the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.  
The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.  
The Managed Devices page displays.
3. Select **Controller Management**.  
The Manage Site Configurations page displays.
4. Select the radio button to view **All** or **Physical Sites**. By default, the controller displays all sites.  
The page adjusts to display the selected sites.
5. Click the **Create New Site** link.  
The Create New Site pop-up window displays.  
Confirm the **Physical Site** radio button is selected on the pop-up window.

6. Set the information for the site by completing the following fields:
  - a. **Site Name:** A name for identification purposes.
  - b. **Site Description:** A description for identification purposes.
  - c. **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 switch that it onboards at the site and replaces the switch local device password with the site password.
  - d. **Confirm Site Admin Password:** Repeat the password.
  - e. **Password Hint:** Enter a password hint.
7. To configure a view-only guest user password for the site:
  - a. Select the **Configure a view-only guest user password for this site** check box.
  - b. **New Site Guest Password:** Enter a password for the guest account, and repeat the password in the **Confirm Site Guest Password** field.

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.
  - c. **Password Hint:** Enter a password hint.
8. In the Additional Switch User Accounts section, add a site user account. For more information, see [Add a site user account](#) on page 59.
9. Click the **Next** button.

The window adjusts and the Network Setup settings display.

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

- **Dynamic IP Address:** From the **Engage Network Interface** menu, select the 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 the controller. The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for 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 the controller and configure the computer as a DHCP server. The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for 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 switches at the site for fastest IP address assignment by the controller's DHCP server.

11. Click the **Next** button.

The window adjusts and the Wireless Setup settings display.

12. Either click the **Skip >>** link to skip this step, or if your network includes access points, set up the global WiFi network (SSID) for the site:
  - a. In the **SSID Name** field, enter the name for the WiFi network (SSID) or enable the **Use Controller Site Name** toggle.
  - b. In the **Passphrase** field, enter the password for access to the WiFi network, which uses WPA-MPSK security, or turn on the **Use Controller Site Password** toggle.

By default, the WiFi security for the global is SSID is WPA2-MPSK (Multi PSK, in short, MPSK), which lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. After you have set up the global site SSID, you cannot change the WiFi security for the global SSID, but you can expand the MPSK configuration. (For more information about MPSK, see [Set up a WiFi network with Multi PSK](#) on page 49.)
  - c. From the **Region** menu, select the region for the country in which the default site is located. After setup, you cannot change the region.
  - d. From the **Country** menu, select the country in which the default site is located. After setup, you cannot change the country.



**NOTE:** After you have set up the global site SSID, you can add additional SSIDs, but you cannot make another SSID the global site SSID. By default, the global SSID broadcasts on the 2.4 GHz and 5 GHz radio bands and is assigned to VLAN 1. You can change the 2.4 GHz and 5 GHz radio bands, change the VLAN ID, and disable the WLAN status for the global site SSID entirely.

13. Click the **Apply** button.

Your settings are saved. The site is added to the table on the Manage Site Configurations page.
14. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

## Edit the network setup of a site

You can change the network setup of a site:

### To edit the network setup of a site:

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

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

The Managed Devices page displays.

3. **Option 1:** Select the **Edit Network Setup** icon at the top of the page next to the **Lock Configuration** icon.

The Edit Network Setup pop-up window displays.

4. **Option 2:** Select **Controller Management**.

The Manage Site Configurations page displays.

- a. Select the radio button to view **All**, **Physical Sites**, or **Virtual Sites**. By default, the controller displays all sites.

The page adjusts to display the selected sites.

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

The Edit Network Setup pop-up window displays.

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

- **Dynamic IP Address:** From the **Engage Network Interface** menu, select the 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 the controller. The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for 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 the controller and configure the computer as a DHCP server. The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps 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 switches at the site for fastest IP address assignment by the controller's DHCP server.

6. Click the **Next** button.

The window adjusts and the Edit Wireless Setup settings display.

7. Optionally, change the SSID name and WiFi password of the global WiFi network (SSID) for the site:

- a. For the SSID name, do one of the following:

- **Use the site name:** Keep the associated toggle enabled so that it displays blue or green and is positioned to the right.
- **Use a unique name:** Turn off the associated toggle so that it displays gray and is positioned to the right, and in the **SSID** field, enter the name for the WiFi network (SSID).

- b. For the WiFi password, do one of the following:

- **Use the site password:** Keep the associated toggle enabled so that it displays blue or green and is positioned to the right.
- **Use a unique password:** Turn off the associated toggle so that it displays gray and is positioned to the right, and in the **Password** field, enter the password for access to the WiFi network, which uses WPA-MPSK security. (For more information, see [About the global site SSID](#) on page 34.)



**NOTE:** You cannot change the region and country after you have enabled WiFi for a site. Therefore, the **Region** and **Country** fields are masked.

8. Click the **Apply** button.

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

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

## Add a site user account

You can add a site user account in the controller to allow users to access devices in a site. You can assign either read or write permissions.

### To add a site user account:

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

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Controller Management**.

The Manage Site Configurations page displays.

5. Select the radio button to view **All**, **Physical Sites**, or **Virtual Sites**. By default, the controller displays all sites.

The page adjusts to display the selected sites.

6. Do one of the following:

- Use the **Create New Site** link:
  - a. Click the **Create New Site** link. The Create New Site pop-up window displays.  
Confirm the **Physical Sites** radio button is selected on the pop-up window.
  - b. Set the following information for the site:
    - i. **Site Name:** A name for identification purposes.
    - ii. **Site Description:** A description for identification purposes.
    - iii. **New Site Password:** The password must be eight characters or more. 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 switch that it onboards at the site and replaces the switch local device password with the site password.
    - iv. **Confirm Site Password:** Repeat the password.
- In the table, for the site that you want to add the user accounts to, click the **3 dots** icon and select **Edit**.

The Edit Site pop-up window displays.

7. In the **Additional Switch User Accounts** section, click the **Add Users** link.

The page adjusts to display the configurable user settings.

8. In the **Username** field, enter a user name.  
It is not possible to use **admin** or **guest** as a user name as they are reserved for the controller user accounts.
9. In the **Password** field, enter a password, and repeat the password in the **Confirm Password** field.  
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.
10. From the **Access Mode** menu, select **Read-Only** or **Read\_Write**.
11. Click the green **checkmark** icon.  
Your settings are saved. The new site user account displays in the table on the Additional Switch User Accounts page.
12. Click the **Next** button.  
The window adjusts and the Network Setup settings display.

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

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



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

14. Click the **Next** button.

The window adjusts and the Wireless Setup settings display.

15. Either click the **Skip >>** link to skip this step, or if your network includes access points, set up the global WiFi network (SSID) for the site:
- In the **SSID Name** field, enter the name for the WiFi network (SSID).
  - In the **Passphrase** field, enter the password for access to the WiFi network, which uses WPA-MPSK security. By default, the WiFi security for the global is SSID is WPA2-MPSK (Multi PSK, in short, MPSK), which lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. After you have set up the global site SSID, you cannot change the WiFi security for the global SSID, but you can expand the MPSK configuration. (For more information about MPSK, see [Set up a WiFi network with Multi PSK](#) on page 49.)
  - From the **Region** menu, select the region for the country in which the default site is located. After setup, you cannot change the region.
  - From the **Country** menu, select the country in which the default site is located. After setup, you cannot change the country.



**NOTE:** After you have set up the global site SSID, you can add additional SSIDs, but you cannot make another SSID the global site SSID. By default, the global SSID broadcasts on the 2.4 GHz and 5 GHz radio bands and is assigned to VLAN 1. You can change the 2.4 GHz and 5 GHz radio bands, change the VLAN ID, and disable the WLAN status for the global site SSID entirely.

16. Click the **Apply** button.
- Your settings are saved. The site is added to the table on the Manage Site Configurations page.
17. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

# Manage Virtual Sites and Devices

Use the controller to plan installations by creating virtual sites and configuring virtual devices before adding physical devices.

A virtual site represents a planned location and is defined by a site name and description. You can duplicate, export, and deploy virtual site plans as physical sites to apply the planned configurations. The controller can deploy the same virtual site plan to multiple physical sites.

A virtual device represents a planned physical device. Use virtual devices to configure the device settings during planning. The controller can onboard and apply your planned configuration when a physical device is installed.

This chapter includes the following sections:

- [Configure virtual sites](#)
- [Deploy a virtual site](#)
- [Configure virtual devices](#)
- [Onboard a physical device using virtual device configurations](#)
- [Configure a virtual link](#)

## Configure virtual sites

The controller lets you plan a new virtual site without needing to add physical devices. After you add a virtual site, you can associate multiple virtual devices to the site.

The controller can duplicate one virtual site into multiple physical sites. The original virtual site remains until you delete it manually.

You can create multiple virtual sites on the controller to plan for various types of site installations.

After you add a virtual site, you can configure the site in the same way as a physical site. For more configuration options, see [Manage Sites](#) on page 54.

## Add a virtual site

You can add multiple virtual sites to the controller.

### To add a virtual site to the controller:

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

The Managed Devices page displays.

3. Do one of the following:
  - **Select the Virtual Device and Virtual Site icon at the top of the page next to the Lock Configuration icon.** Click the **Create a Virtual Site** button.
    - The Create Virtual Site pop-up window displays. Confirm the **Virtual Site** radio button is selected on the pop-up window.
  - **Select Controller Management.** The Manage Site Configurations page displays.
    - Select the radio button to view **All** or **Virtual Sites**. By default, the controller displays all sites.  
The page adjusts to display the selected sites.
    - Click the **Create New Site** link. The Create Virtual Site pop-up window displays.  
Confirm the **Virtual Site** radio button is selected on the pop-up window.
4. Set the information for the site by completing the following fields:
  - a. **Site Name:** A name for identification purposes. The site name must start with VR- followed by letters or numbers.
  - b. **Description:** A description for identification purposes.
5. To enable wireless features and add virtual access points to virtual sites, select the **Wireless** toggle so that it displays blue or green and is positioned to the right. Set the information for the wireless virtual site by completing the following fields:
  - a. In the **Global Site SSID** field, enter the name for the WiFi network (SSID) or enable the **Use Controller Site Name** toggle.
  - b. **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.
  - c. From the **Region** menu, select the region for the country in which the default site is located. After setup, you cannot change the region.
  - d. From the **Country** menu, select the country in which the default site is located. After setup, you cannot change the country.
6. Click the **Save** button.
7. A pop-up window displays where you can choose to switch to the virtual site and add virtual devices to it.
  - Click the **Yes** button to add virtual devices and follow the steps in [Add a virtual device](#) on page 69.
  - Click the **No, I will do it later** button to save your settings.

Your settings are saved. The site is added to the table on the Manage Site Configurations page.

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

## Deploy a virtual site

Deploying a virtual site transfers the configurations of that virtual site to a physical site. You can deploy the same virtual site configurations to multiple physical sites.

### To deploy a virtual site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.  
The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.  
The Managed Devices page displays.
3. Select **Controller Management**.  
The Manage Site Configurations page displays.
4. Select the radio button to view **All** or **Virtual Sites**. By default, the controller displays all sites.  
The page adjusts to display the selected sites.
5. In the table, for the site that you want to edit, click the **3 dots** icon and select **Deploy**.  
The Deploy Virtual Site pop-up window displays.
6. Set the information for the site by completing the following fields:
  - a. **Site Name**: A name for identification purposes.
  - b. **Site Description**: A description for identification purposes.
  - c. **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 switch that it onboards at the site and replaces the switch local device password with the site password.
  - d. **Confirm Site Admin Password**: Repeat the password.
  - e. **Password Hint**: Enter a password hint.

7. To configure a view-only guest user password for the site:
  - a. Select the **Configure a view-only guest user password for this site** check box.
  - b. **New Site Guest Password:** Enter a password for the guest account, and repeat the password in the **Confirm Site Guest Password** field.

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.

- c. **Password Hint:** Enter a password hint.

8. In the Additional Switch User Accounts section, add a site user account. For more information, see [Add a site user account](#) on page 59.

9. Click the **Next** button.

The window adjusts and the Network Setup settings display.

10. Specify how the computer on which the controller is installed can connect to the AV network at the site by selecting a radio button:
  - **Dynamic IP Address:** From the **Engage Network Interface** menu, select the 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 the controller. The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for 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 the controller and configure the computer as a DHCP server. The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for 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 switches at the site for fastest IP address assignment by the controller's DHCP server.

11. Click the **Next** button.

The window adjusts and the Wireless Setup settings display.

12. Either click the **Skip >>** link to skip this step, or if your network includes access points, set up the global WiFi network (SSID) for the site:

- In the **SSID Name** field, enter the name for the WiFi network (SSID) or enable the **Use Controller Site Name** toggle.
- In the **Passphrase** field, enter the password for access to the WiFi network, which uses WPA-MPSK security, or turn on the **Use Controller Site Password** toggle.

By default, the WiFi security for the global is SSID is WPA2-MPSK (Multi PSK, in short, MPSK), which lets you segregate a single WiFi network into different VLANs, each accessible with a unique passphrase. After you have set up the global site SSID, you cannot change the WiFi security for the global SSID, but you can expand the MPSK configuration. (For more information about MPSK, see [Set up a WiFi network with Multi PSK](#) on page 49.)

- From the **Region** menu, select the region for the country in which the default site is located. After setup, you cannot change the region.
- From the **Country** menu, select the country in which the default site is located. After setup, you cannot change the country.



**NOTE:** After you have set up the global site SSID, you can add additional SSIDs, but you cannot make another SSID the global site SSID. By default, the global SSID broadcasts on the 2.4 GHz and 5 GHz radio bands and is assigned to VLAN 1. You can change the 2.4 GHz and 5 GHz radio bands, change the VLAN ID, and disable the WLAN status for the global site SSID entirely.

13. Click the **Deploy** button.

A confirmation pop-up window displays.

14. Do one of the following:

- **Click the Yes button:** Deploy the site but retain the virtual site configuration and keep a copy of the virtual site.
- **Click the No button:** Deploy the site and delete the virtual site.

Your settings are saved. The site is added to the table on the Manage Site Configurations page.

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

## Configure virtual devices

A virtual device is one that you create using the controller.

The controller lets you add new virtual devices without needing to add physical devices. Virtual devices let you plan and configure devices before any physical hardware is installed or discovered. You add virtual devices to a virtual site to build a site plan, configure your intended settings for the device, and refine the configuration over time.

Virtual devices do not appear in the Discovered Devices section, which only lists physical devices that the controller discovers on the network.

After you add a virtual device, you can configure the device in the same way as a physical device. For more configuration options, see [Manage Devices](#) on page 22.

## Add a virtual device

You can manually add a virtual device as a managed device to the site by specifying the device IP address and access credentials.

### To add a virtual device to a site:

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

The controller application opens and displays a login page.

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Do one of the following:

- **Select the Virtual Device and Virtual Site icon at the top of the page next to the Lock Configuration icon.** The Virtual Device and Virtual Site pop-up window displays.
  - Click the **Create Virtual Devices on the site** button. The Add Device pop-up window displays.
- **On the Managed Devices page, click the Add Device link.** The Add Device pop-up window displays.

5. Select the radio button to display **Virtual Devices**.

6. From the list of virtual devices, select the model you want to add and the number of devices. Use the **Search Devices** field to search for a specific device.
7. Do one of the following:
  - **Click the Add button:** The device is added and in an Inactive state. Your settings are saved.  
You can provision the device by clicking the **Provision** button and following the steps in [Provision a virtual device](#) on page 70.
  - **Click the Continue button:** The Provision Virtual Devices page displays. Follow the steps in [Provision a virtual device](#) on page 70 to provision the device.  
Your settings are saved.  
The device is moved to the Managed Devices table, and the onboarding process is now in progress.
8. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

## Provision a virtual device

When you add a new virtual device to the controller, the device remains on the Managed Devices page in an Inactive state. Use the provision option on a virtual device to create a planned configuration, even when there is no physical device online yet.

See [Onboard a physical device using virtual device configurations](#) on page 72 for more information about adding your virtual device configurations to a physical device.

You can provision multiple virtual devices at the same time.

### To provision one or more virtual devices:

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

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select the check box to display **All**, **Physical Devices**, or **Virtual Devices**.

By default, all managed devices display. Use the **Device Model** field to select individual devices.

5. Do one of the following:

- **If the virtual device has an Inactive lifecycle state:** Click the **Provision** button

The Provision Virtual Devices page displays.

- **If you want to add a new virtual device:** Click the **Add Device** link.

The Add Device pop-up window displays.

- Select the radio button to display **Virtual Device**.
- From the list of virtual devices, select the device you want to add and the number of devices.
- Click the **Continue** button to provision the device.
- Select the device or devices you want to provision. You can provision one selected device, or choose to provision multiple devices at once.
- Click the **Provision** button. The Provision Virtual Devices page displays.

6. Use the default information or specify the following information:

- Device name
- Serial number
- MAC address
- IP address

Optional: Click the **Export** button to export the virtual device details and save or edit the information. Click the **Import** button to upload the saved virtual device details.

7. Choose whether to select the **Auto Onboard** toggle.

For more information about auto-onboarding a device, see [Auto-onboard a device](#) on page 73.

8. Do one of the following:

- **Add the device:** Click the **Save & Skip** button to add the device.
- **Add the device and create a virtual link:** Click the **Link Configuration** button and follow the steps in [Create a virtual link](#) on page 74.

Your settings are saved. The virtual device status changes to Standalone and you can now configure the device.

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

## Onboard a physical device using virtual device configurations

You can use the controller to onboard a physical device which matches a preconfigured virtual model name, serial number, or base MAC address. The controller replaces the newly discovered physical device with the existing virtual device configurations.



**NOTE:** You must add a physical device to the controller before onboarding.

Use the auto-onboarding option to let the controller automatically onboard a physical device with preconfigured settings. For more information, see [Auto-onboard a device](#) on page 73.

### To manually onboard a physical device using existing virtual device configurations:

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

The controller application opens and displays a login page.

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select the check box to display **All**, **Physical Devices**, or **Virtual Devices**.

By default, all managed devices display. Use the **Device Model** field to select individual devices.

5. In the Discovered Devices table, click the **Onboard** button next to the device you want to onboard using existing virtual device configurations.  
The Virtual Device Onboard pop-up window displays.
6. Enter the password in the **Device Password** field.
7. Click the **Single** button.
8. Select the virtual device you want to replace with a physical device.  
The controller automatically transfers the configuration to the physical device, replacing the virtual one.
9. Click the **Confirm** button.  
Your settings are saved. The new physical device configurations are replaced with the pre-existing virtual device configurations.
10. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

## Auto-onboard a device

You can enable auto-onboarding to preconfigure details of a virtual device and apply its settings to a physical device when the controller discovers the device on the network.

For auto-onboarding to succeed, a physical device must be in a factory default state or have an admin password that matches the site password. If the password or device details do not match, you can update the device information in the Edit Virtual Devices window. You can also export the device list, correct the details, import the updated device list, and then enable auto-onboarding.

When auto-onboarding is enabled, the controller automatically onboards a discovered physical device that matches one of the following identifiers:

- Model and serial number.
- Model and MAC address.

The controller onboards the physical device using the virtual device's preconfigured details.

### To auto-onboard a physical device using existing virtual device configurations:

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

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. In the table, for the virtual device that you want to auto-onboard, click the **3 dots** icon and select **Edit**.

The Edit Virtual Devices pop-up window displays.

5. Select the check box for the virtual device you want to auto-onboard.

6. Click the **Proceed** button.

7. Select the **Auto Onboard** toggle.

When auto-onboarding is enabled, the toggle displays blue and is positioned on the right.

8. Optional: Click the **Export** button to export the virtual device configuration onto your device.

9. Click the **Save & Skip** button to finish editing the device.

Your settings are saved.

When the controller discovers a matching physical device, the physical device automatically onboards with the preconfigured virtual device settings.

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

## Configure a virtual link

Virtual links provide logical connectivity and activate virtual devices, without requiring physical port configuration. A virtual link connects:

- A physical device to one or more virtual devices.
- A virtual device to one or more other virtual devices.

When a virtual device is connected through a virtual link, the device state changes from Standalone to Active. This indicates the device is participating in virtual traffic forwarding. You can configure a virtual link so that it is set up for supporting either a single link or a LAG.

## Create a virtual link

You can create a virtual link from the controller.

**To create a virtual link on a device from the Managed Devices table:**

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

The controller application opens and displays a login page.

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

The Managed Devices page displays.

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

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site:** Click the **Apply** button.
- **Change the network setup for the site:** See the information in [Edit the network setup of a site](#) on page 57. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select the check box to display **All**, **Physical Devices**, or **Virtual Devices**.

By default, all managed devices display. Use the **Device Model** field to select individual devices.

5. In the table, for the device that you want to manage, click the **3 dots** icon and select **Link Configuration**.

The Configure Virtual Link pop-up window displays.

6. In the table, select the radio button for the device you want to use as the source device. Click the **Next** button.

7. In the table, select the radio button for the device you want to use as the target device. Click the **Next** button.



**NOTE:** You must select a switch as either the source or the destination device.

8. Select the radio button for the connection type:

- **Single:** A single link represents a unique connection to the connected device.
- **LAG:** A link aggregation group of up to eight physical connections to the device.

9. Select a target port by clicking the port on the switch image.

Click the **Next** button.

10. Select the link speed for the connection type from the menu.

11. Click the **Finish** button.

You can view the virtual link between two devices on the Site Topology page.

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