NETGEAR®

Insight
Mobile App and Cloud Portal
User Manual

February 2018
202-11872-01

350 E. Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product. You can visit *www.netgear.com/support* to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11872-01	February 2018	First publication.

Contents

Introduction

1

NETGEAR Insight is a cloud-based management platform that lets you set up and configure NETGEAR Insight Managed access points, switches, and ReadyNAS storage systems. With the advantage of unified setup and configuration of devices through the cloud, Insight provides simplified ongoing maintenance, continuous visibility and control, remote access, and scalability.

This chapter includes the following sections:

Overview

NETGEAR Insight enables unified multidevice configuration of NETGEAR Insight managed wireless, switching, and ReadyNAS storage devices. Insight provides network management, monitoring, and service deployment across multiple remote locations.

Insight provides the following features:

- Simplified device setup
- One-tap registration
- Email and push notifications for all Insight managed devices for network problems
- Management of multiple network locations
- Unified visibility and management of your entire network with a single password
- Management and monitoring of all your network locations from a single Insight account
- Remote firmware updates
- No need for a cloud controller, appliance, server, network portal, or additional software application

Network Location Provisioning Concepts

With the Insight cloud-based management application, the provisioning process is network location based.

Similar types of Insight managed devices at one network location (for example, all Insight Managed switches at one network location) share the same configuration with the exception of their IP addresses and device names.

If you create a VLAN for a network location, you can assign that VLAN to both Insight Managed switches and Insight Managed access points. A WiFi network (SSID) that you configure for one access point at a network location is automatically broadcast by all access points at that location.

You also can simultaneously configure features for multiple switches at a network location and you can simultaneously configure features for multiple access points at a network location.

Insight Mobile App and Insight Cloud Portal

You can access the Insight cloud-based management platform in two ways. You can use the Insight mobile app installed on a smartphone or tablet and, if you are an Insight Premium subscriber (see *Insight Subscription Plans* on page 9), you can use the Insight Cloud Portal in addition to the Insight mobile app:

- **Insight mobile app**. The Insight mobile app is an application that is available for iOS and Android devices and supports the following features for Insight managed devices for all subscriber plans:
  - Guided installation and configuration.
  - Secure remote access.
  - Instant alerts for critical events.
  - Access to logs and traffic history.

  - Self-help and click-to-connect support portal.
  - Support for an unlimited number of devices and locations. (Insight Basic is free for the first two devices. Insight Premium requires a subscription fee for each device. For more information, see *Insight Subscription Plans* on page 9.)

- **Insight Cloud Portal**. The Insight Cloud Portal lets you access and manage your Insight devices online from a web browser. The Insight Cloud Portal is available only to Insight Premium subscribers. The Cloud Portal supports the following features for Insight managed devices:

  - Feature parity with the Insight app for device configuration and management. (Feature parity does not apply to the Orbi Pro WiFi systems.)
  - A granular dashboard on which you can customize how your Insight diagnostics display.
  - A layout that takes advantage of your computer's screen size to display more information at one time.

The Insight mobile app and the Insight Cloud Portal are different interfaces into the same cloud-based management platform. The cloud-based management platform applies the configuration changes in the order that it receives them. However, we do not recommend that different users configure the same Insight network simultaneously, one using the Insight mobile app and the other using the Insight Cloud Portal or another instance of the Insight mobile app.

Insight Subscription Plans

Paid Insight subscriptions apply only to Insight managed devices. NETGEAR does not require paid subscriptions for non-Insight managed devices, even though Insight can discover, register, and, in some cases, even perform basic monitoring of such devices.

NETGEAR offers two Insight subscription plans: Insight Basic and Insight Premium. Both subscription plans include the following features:

- Guided installation and configuration
- Secure remote access
- Instant alerts for critical events
- Access to logs and traffic history
- Self-help and click-to-connect support portal
- Capacity to support an unlimited number of locations and devices (the number of supported devices depends on the subscription plan)

The subscription plans differ as follows:

- Insight Basic:

  - Insight Basic includes access to the Insight mobile app only.
  - Insight Basic is free for the first two devices.

  - Each additional device requires a per-year, per-device subscription fee.
  - The Insight Basic level of support can accommodate many small business without any additional fees.

- Insight Premium:

  - Insight Premium grants access to both the Insight mobile app and the Insight Cloud Portal, which allows you to access and manage your Insight devices from a web browser.
  - Insight Premium also grants access to Premium-only features such as Smart WiFi roaming and PoE scheduling. Additional Premium features are on the development roadmap.
  - Each device requires a subscription fee.
  - Insight Premium is available in both monthly and yearly subscription plans.
  - Insight Premium is an upgrade and does not provide any free devices, unlike Insight Basic.

For information about subscriptions and pricing, visit *insight.netgear.com* and the NETGEAR Insight knowledge base at *netgear.com/support/product/insight.aspx*.

Supported Devices

Using Insight, you can discover many NETGEAR business products on your network and register them through your NETGEAR account. However, monitoring, management, and setup functions are available on certain devices only. The following table provides specific information.

Table 1. Insight supported devices

Product Line or Devices	Available Actions				
	Set Up	Manage	Monitor	Discover	Register
Insight Managed Switches	X	X	X	X	X
Insight Managed Access Points	X	X	X	X	X
Orbi Pro WiFi systems		X[1]	X	X	X
ReadyNAS 300, 400, 500, 600, 700, 2000, 3000, and 4000 series storage systems		X	X	X	X
Smart Managed Plus Switches			X	X	X
Smart Managed Pro Switches			X	X	X
Fully Managed Switches				X	X
ReadyNAS 200 series storage systems				X	X

Table 1. Insight supported devices (Continued)

Product Line or Devices	Available Actions				
	Set Up	Manage	Monitor	Discover	Register
WAC 100 and 700 series access points				X	X
Unmanaged switches					X

[1] Limited management for an Orbi Pro WiFi system is available in the Insight mobile app only. At this time, you cannot manage an Orbi Pro WiFi system through the Insight Cloud Portal.

Note If a device can be managed in Insight, then it counts towards your total devices on your Insight subscription plan. If a device can only be discovered, registered, and monitored in Insight, then it does not count toward your device total for your Insight subscription. For information about pricing, see *insight.netgear.com* and the NETGEAR Insight knowledge base at *netgear.com/support/product/insight.aspx*.

Insight Cloud Portal Dashboard

The Insight Cloud Portal, which is available to Insight Premium subscribers, provides a dashboard that lets you view the system and client health for each network location. The dashboard also provides access to detailed information about each device at a network location.

You can customize the dashboard by adding or removing predefined widgets. In a widget, you can customize the information that displays in the widget.

Insight and the Local Browser–Based Management Interface

You can configure Insight managed devices through the Insight mobile app on a smartphone or tablet. If you are an Insight Premium subscriber, you can also manage Insight managed devices from the Insight Cloud Portal, which is accessible from a web browser on your Windows-based computer, Mac, or tablet.

Insight managed devices also provide a traditional, local browser–based management interface that functions independently of the Insight cloud-based management platform. This hybrid model lets you manage your device either with the local browser interface or with Insight. However, if you intend to use Insight, we do not recommend that you set up a device in “offline” mode because any configuration changes are not pushed to the Insight cloud-based management platform and are therefore not reflected in the Insight mobile app and Insight Cloud Portal.

If you configure a device through the local browser interface and then enable the Insight management mode, all settings except for the device IP address and device name are reset to their factory default settings. The same situation occurs the other way around: If you configure a device in Insight management mode and then enable the local browser interface mode, all settings except for the device IP address and device name are reset to their factory default settings.

Note Changes to Insight-manageable settings from the local browser interface might also create conflicts with the rest of the Insight-managed network to which the device is connected. While you manage a device with the local browser interface, you cannot use the Insight mobile app or Insight Cloud Portal.

Get Started

2

This chapter describes how to install the Insight mobile app and access the Insight Cloud Portal, create an account, create an Insight network location, and discover, add, and register devices. The chapter also describes how to manage your notifications.

This chapter includes the following sections:

The following is an explanation of terms and abbreviations that we use in this manual:

- **Insight**. Insight is the cloud-based management platform.
- **Insight mobile app**. The Insight mobile app (or abbreviated as the Insight app) is the application for Android and iOS smartphones. The Insight app provides access to the Insight cloud-based management platform.
- **Insight Cloud Portal**. The Insight Cloud Portal (or abbreviated as the Cloud Portal), is the web page that provides access to the Insight cloud-based management platform. The Cloud Portal is available to Insight Premium subscribers.

Install the Insight App

You can install the NETGEAR Insight app on an iOS or Android mobile device.

To install the Insight app:

On your mobile device, go to the *Apple App Store* or the *Google Play Store*, search for NETGEAR Insight, and download the app.

Access the Insight Cloud Portal

The Insight Cloud Portal is available for Insight Premium subscribers at *https://insight.netgear.com/#/login*.

To access the Insight Cloud Portal:

1. Visit *https://insight.netgear.com/#/login*.
   The Insight Cloud Portal web page displays.
2. Select **Login**.
   The NETGEAR Account Sign-In page displays.
3. Enter your Insight email address and password.
   If you do not own an Insight account, see *Create an Insight Account Using the Cloud Portal* on page 16.
4. Click the **NETGEAR Sign In** button.
   You can now manage your locations and devices and do more.

Create an Insight Account

You can use one account for all NETGEAR apps and for the Insight Cloud Portal. If you already set up a MyNETGEAR account for another NETGEAR app such as NETGEAR Up or NETGEAR WiFi Analytics, you can use that account to access the NETGEAR Insight app.

If you did not set up an account for a NETGEAR app, you must create a new MyNETGEAR account.

Create an Insight Account Using the Insight App

You can create an Insight account using the Insight app.

To create an Insight account using the Insight app and sign in to your new account:

1. Download the Insight app from the *Apple App Store* or the *Google Play Store*.
2. Launch the Insight app.
3. Tap **CREATE MYNETGEAR ACCOUNT**.
   The Create a MyNETGEAR ACCOUNT page displays.
4. Complete the required fields and select your country.
   The password that you specify must be at least six characters in length and must contain one uppercase, one lowercase, and one numerical character. The following special characters are allowed: ! @ # $ % ^ & * ( )
5. Tap **NEXT**.
   The Insight Terms and Conditions page displays.
6. Read the terms and conditions and, if you agree, tap **I AGREE**.
   A verification email is sent to the email address that you used to set up your Insight account.
7. In your email program, open the email from NETGEAR Support and click the **Verify your email address** link.
   A web page opens with the message Your Email verification has been completed.
8. Either launch the Insight app again or go back to the page that allows you to set up a new account or sign in.
9. Tap **SIGN IN**.
   The Account Sign In page displays.
10. Enter the email address and password that you used to set up your new Insight account.
11. Tap **SIGN IN**.
    Information about your new Insight account displays.
12. Tap **OK**.
    You are now ready to set up an Insight network location, let the Insight app discover your devices, and add devices to the network.

    For more information, see the following sections:

    - *Create an Insight Network Location* on page 17
    - *Discover, Add, and Register Devices* on page 18

Create an Insight Account Using the Cloud Portal

You can create an Insight account using the Cloud Portal.

To create an Insight account using the Cloud Portal and sign in to your new account:

1. Visit *https://insight.netgear.com/#/login*.
   The Insight Cloud Portal web page displays.
2. Select **Login**.
   The NETGEAR Account Sign-In page displays.
3. Click the **Create NETGEAR account** link.
   The Create a MyNETGEAR ACCOUNT page displays.
4. Complete the required fields and select your country.
   The password that you specify must be at least six characters in length and must contain one uppercase, one lowercase, and one numerical character. The following special characters are allowed: ! @ # $ % ^ & * ( )
5. Click the **Terms and Conditions** link.
   The terms and conditions display.
6. Read the terms and conditions and, if you agree, click the **By Signing up I agree to the Terms and Conditions** check box.
   A verification email is sent to the email address that you used to set up your Insight account.
7. Click the **NETGEAR Sign-Up** button.
   A confirmation page displays. You must confirm your email address.
8. In your email program, open the email from NETGEAR Support and click the **Verify your email address** link.
   A web page opens with the message Your Email verification has been completed.
9. Visit *https://insight.netgear.com/#/login*.
   The Insight Cloud Portal web page displays.
10. Select **Login**.
    The NETGEAR Account Sign-In page displays.
11. Enter the email address and password that you used to set up your new Insight account.
12. Click the **NETGEAR Sign In** button.
    You are now ready to set up an Insight network location and add devices to the network.

    For more information, see the following sections:

    - *Create an Insight Network Location* on page 17
    - *Discover, Add, and Register Devices* on page 18

Create an Insight Network Location

An Insight network location is a collection of devices in the same physical location that use the same administrator password and can be monitored simultaneously in Insight. If you want to monitor and manage Insight devices in more than one physical location, you must create a new Insight network location for each physical location.

Create an Insight Network Location Using the Insight App

You can create an Insight network location using the Insight app.

To create an Insight network location using the Insight app:

1. Launch the Insight app.
2. Tap the menu in the upper middle of the screen and then tap **Create New Network Location**.
3. In the **Network Location Name** field, enter a name for your new network location.

   The name must be 3 to 24 characters long, letters and numbers only. If you plan to set up more than one Insight network location, be sure that you create descriptive names that can help you remember which network location is which, such as 2nd Floor Marketing, Mowry Avenue, or Richmond Office.
4. In the **Device Admin Password** field, enter the password that you want to use for your Insight network location.

   This device admin password replaces the administrative password on all devices added to this network location. The password must be 6 to 20 characters long.
5. Select the country and time zone for your new Insight network location and tap **Next**.
6. Read the pop-up notification about password changes to devices on the network and tap **OK**.

   Your Insight network location is now set up. You can view your network location at any time on the Networks page. Tap the menu in the upper middle of the screen, tap the network location that you want to view, and in the menu at the bottom, tap **Networks**.

For information about adding devices to your network location, see *Discover, Add, and Register Devices* on page 18.

Create an Insight Network Location Using the Cloud Portal

You can create an Insight network location using the Cloud Portal.

To create an Insight network location using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.
2. If the network menu at the top of the page does not show All Locations, click the network menu and select **See all locations**.
3. Click **+** above the network locations.

   The Setup a New Network Location pop-up window opens.

4. In the **Network Location Name** field, enter a name for your new network location.

   The name must be 3 to 24 characters long, letters and numbers only. If you plan to set up more than one Insight network location, be sure that you create descriptive names that can help you remember which network location is which, such as 2nd Floor Marketing, Mowry Avenue, or Richmond Office.

5. In the **Device Admin Password** field, enter the password that you want to use for your Insight network location.

   This device admin password replaces the administrative password on all devices added to this network location. The password must be 6 to 20 characters long.

6. As an option, add the street, city, and state for your new network location.
7. Select the country and time zone for your new network location.
8. To upload an image for your new network location, click the **Choose a file** button, locate the image, and upload it.
9. Click the **Save** button.

   You settings are saved and your new Insight network location is set up.

For information about adding devices to your network location, see *Discover, Add, and Register Devices* on page 18.

Discover, Add, and Register Devices

You can add a device to Insight using the Insight app in four different ways. You can add a device to Insight using the Cloud Portal only by entering the serial number of the device.

IMPORTANT:
For you to be able to add a device to Insight, the device must be connected to the Internet, the default gateway and DNS servers that are being used for the Internet connection must be defined correctly, and a firewall must not be blocking the traffic between the device and the Insight cloud-based management platform.

When you add a device to your Insight account, the device is automatically registered to you.

Note When you add a device for the first time, Insight pushes firmware updates to the device, which causes the device to be reconfigured and might cause it to reboot multiple times. The entire process of adding a device for the first time might take up to 20 minutes.

Before you can add a device in the Insight app or through the Insight Cloud Portal, you must complete the following steps:

1. Create an Insight account.
   For more information, see *Create an Insight Account Using the Insight App* on page 15 or *Create an Insight Account Using the Cloud Portal* on page 16.
2. Create an Insight network location.
   For more information, see *Create an Insight Network Location Using the Insight App* on page 17 or *Create an Insight Network Location Using the Cloud Portal* on page 17.

The following sections describe the ways in which you can add devices in the Insight app or through the Cloud Portal:

Add a Device by Scanning Your Network With the Insight App

If you connect your mobile device to the same WiFi network that your new device is connected to, the Insight app can reach the device and you can scan your network for the new device.

To add a device by scanning your network with the Insight app:

1. Launch the Insight app.
2. Tap **+** in the upper right corner of the screen.
3. Tap **Scan Network**.

   Insight scans for devices on the network that your mobile device is connected to.
4. Select the check box next to the device that you want to add and tap **Next**.
5. Select a network location.
6. Name your device and tap **Next**.
7. Tap **Continue**.
8. If you are adding an Insight Managed switch or access point, follow the onscreen instructions to set up your device.

   It might take up to 20 minutes for the status of your device to turn green in the Insight app and in the Cloud Portal.

Add a Device by Scanning Its QR Code With the Insight App

To add a device by scanning its QR code with the Insight app:

1. Locate the product label on the rear or bottom of your device.
2. Launch the Insight app.
3. Tap **+** in the upper right corner of the screen.
4. Tap **Scan QR Code**.
5. Point the camera of your mobile device at the QR code on the product label.

   The Insight app automatically recognizes a valid QR code.
6. Select a network location.
7. Name your device and tap **Next**.

8. Tap **Continue**.
9. If you are adding an Insight Managed switch or access point, follow the onscreen instructions to set up your device.

   It might take up to 20 minutes for the status of your device to turn green in the Insight app and in the Cloud Portal.

Add a Device by Scanning Its Barcode With the Insight App

To add a device by scanning its barcode with the Insight app:

1. Locate the product label on the rear or bottom of your device.
2. Launch the Insight app.
3. Tap **+** in the upper right corner of the screen.
4. Tap **SCAN BARCODE**.
5. Point the camera of your mobile device at the barcode on the product label.

   The Insight app automatically recognizes a valid barcode and places the associated serial number in the **Enter Serial Number** field.
6. To the right of the **Enter Serial Number** field, tap **GO**.
7. Select a network location.
8. Name your device and tap **Next**.
9. Tap **Continue**.
10. If you are adding an Insight Managed switch or access point, follow the onscreen instructions to set up your device.

    It might take up to 20 minutes for the status of your device to turn green in the Insight app and in the Cloud Portal.

Add a Device by Entering Its Serial Number in the Insight App

To add a device by entering its serial number in the Insight app:

1. Locate the product label on the rear or bottom of your device.
2. Launch the Insight app.
3. Tap **+** in the upper right corner of the screen.
4. Enter the serial number of your device in the **Enter Serial Number** field and, to the right of the field, tap **GO**.
5. Select a network location.
6. Name your device and tap **Next**.
7. Tap **Continue**.
8. If you are adding an Insight Managed switch or access point, follow the onscreen instructions to set up your device.

It might take up to 20 minutes for the status of your device to turn green in the Insight app and in the Cloud Portal.

Add a Device by Entering Its Serial Number Using the Cloud Portal

To add a device by entering its serial number using the Cloud Portal:

1. Locate the product label on the rear or bottom of your device.
2. Access the Insight Cloud Portal.
   All network locations display.
3. Select a network location.
4. At the top right of the page, click the **+** (**Add Device**) button.
   The Add a New Device pop-up window opens.
5. Enter the serial number of your device in the **Serial Number** field and click **GO**.
   If the serial number is validated, the Device Name field displays.
6. In the **Device Name** field, name your device.
7. Click the **Save** button.
   Your settings are saved and your device is added to the network.
8. If you are adding an Insight Managed switch or access point, follow the instructions on the page to set up your device.
   It might take up to 20 minutes for the status of your device to turn green in the Insight app and in the Cloud Portal.

Access Your Network and Devices Remotely

Insight is a cloud-based management platform, so you can monitor and manage your devices (see *Supported Devices* on page 10) from anywhere using the Insight app or the Cloud Portal.

However, to add a device to an Insight network location, you must either be able to physically access the device, your smartphone or tablet must be on the same network as the device, or you must add the serial number of the device through the Cloud Portal (see *Discover, Add, and Register Devices* on page 18).

Access Your Network and Devices Remotely Using the Insight App

You can access your network and devices remotely using the Insight app.

Note The following remote access instructions apply only *after* you create an account, create a network location, and set up a device.

To access your network and devices remotely using the Insight app:

1. Launch the Insight app.

   If you already added at least one device in the Insight app, the first page that you see is the Devices page, which shows all of your Insight-connected devices.

2. To monitor or manage a device, tap it in the Devices page.
3. To monitor or manage a network location, do the following:

   a. Tap **Networks**.

   b. If you set up more than one Insight network location, at the top of the page, select the network that you want to monitor or manage.

Access Your Network and Devices Remotely Using the Cloud Portal

You can access your network and devices remotely using the Cloud Portal.

> **Note** The following remote access instructions apply only *after* you create an account, create a network location, and set up a device.

To access your network and devices remotely using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.

2. To monitor or manage a device, do the following:

   a. At the top of the page, select **My Devices**.
   The page displays headings for the network locations with active devices.

   b. For the network to which you assigned the device, click **+** to the right of the heading.
   The page expands and displays all devices in the network.

   c. Point to the device and click the **pencil** icon at the right of the page.
   The page that displays shows details about the device and provides access to other pages with more details.

3. To monitor or manage a network location, click the network location, or if the network locations no longer display, select the network from the network menu at the top of the page.

Interpret the Green, Red, Orange, and Gray Circles Next to a Device

On the Devices page in the Insight app and for a selected network on the My Devices page in the Cloud Portal, the colored circle to the left of each device indicates the current status of the device as follows:

- **Green**. The device is connected to the Insight cloud-based management platform.
- **Red**. The device is disconnected from the Insight cloud-based management platform.
- **Orange**. The device is connected to the Insight cloud-based management platform but with limited support only.
- **Gray**. The status of the device is unknown.

View and Manage Insight Notifications

Insight sends you three categories of notifications:

- **Critical**. Insight sends a critical notification whenever an Insight Managed device loses connection with the Insight cloud.
- **Warning**. Insight sends a warning notification when it detects an error or a problem in your Insight network.
- **Notifications**. Insight sends regular notifications when new firmware is available, when a device reconnects to the Insight cloud, when you edit administrator settings, when a device is rebooted, and for other regular system events.

You can view and manage your notifications in the Insight app and Cloud Portal, including turning each category of notifications on or off for each network location.

View or Delete Your Notifications Using the Insight App

To view or delete your notifications using the Insight app:

1. Launch the Insight app.
2. Tap **Notifications** in the lower right corner of the page.
3. To filter by device, severity, or time received, tap **...** in the upper right corner of the page and tap **Filter**.
4. Tap each category of notifications (**Device**, **Severity**, and **Time**) to view or hide notifications in that category.
5. In each category, clear the check box for the type of notifications that you do not want to view.
6. Tap **Apply**.
7. To delete a notification, do the following:
   a. Tap and hold the notification and move it to the left.
   b. Tap the red **trash can** icon.

View or Delete Your Notifications in the Cloud Portal

To view or delete your notifications in the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Click the **Notification** icon in the upper right corner of the page.
   The notifications pop-up window opens.
3. Scroll down and click the **See All** button.
   The Notifications page displays.
4. Click the **Filter** icon.
   A pop-up window opens.
5. Click the button for each type of notification that you do want to view.
   By default, all notifications display. If you select a button, the button displays green and only the associated notifications display. You can select multiple buttons.
6. Click the **Apply** button.
   Your settings are saved.
7. To delete a notification, point to the notification, and click the red **x** that displays on the right.
   The notification is deleted.

Manage Your Insight Notifications Using the Insight App

To manage your Insight notifications using the Insight app:

1. Launch the Insight app.
2. Tap the menu button in the upper left corner of the screen.
3. Tap **Account Management > Manage Notifications**.
4. To edit smartphone or tablet push notification settings, do the following:
   a. Tap **Push Notifications**.
   b. Tap the button to turn all push notifications on or off.
   c. If you want to receive some push notifications and not others, tap each network location and then tap the buttons for **Critical**, **Warning**, and **Notifications** to turn them on or off.
   d. Tap the arrow at the top of the page to return to the previous page.
5. To edit email notification settings, do the following:
   a. Tap **Email Notifications**.
   b. Tap the button to turn all push notifications on or off.

Note To change the email address that receives email notifications, you must change the email address that is associated with your Insight account, which, in turn, changes your login credentials.

c. If you want to receive some email notifications and not others, tap each network location and then tap the buttons for **Critical**, **Warning**, and **Notifications** to turn them on or off.

d. Tap the arrow at the top of the page to return to the previous page, and tap the arrow again to return to the page that lets you manage your account settings.

Manage Your Insight Notifications Using the Cloud Portal

To manage your Insight notifications using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Click the **account** icon in the upper right corner of the page.
   A pop-up window opens.
3. Select **Account Management**.
   The Update Profile page displays.
4. Select **Manage Notifications**.
   By default, the push notification settings display and the push notifications are enabled (the **Push Notifications** button displays green).
5. To edit smartphone or tablet push notification settings, do the following:
   a. To turn off push notifications, click the **Push Notifications** button so that it displays gray.
   b. If you want to receive some push notifications and not others, click each network location and then click the buttons for **Critical**, **Warning**, and **Notifications** to turn them on or off.
   c. Click the **Save** button at the bottom of the page.
      Your settings are saved.
6. To edit email notification settings, do the following:
   a. To the right of the Email Notifications heading, click **+**.
      The email notification settings display. By default, the email notifications are enabled (the **Email Notifications** button displays green).

Note To change the email address that receives email notifications, you must change the email address that is associated with your Insight account, which, in turn, changes your login credentials.

   b. To turn off email notifications, click the **Email Notifications** button so that it displays gray.

c. If you want to receive some email notifications and not others, click each network location and then click the buttons for **Critical**, **Warning**, and **Notifications** to turn them on or off.

d. Click the **Save** button at the bottom of the page.

   Your settings are saved.

Maintain Your Insight Managed Devices and Network Locations

3

This chapter describes how to maintain your Insight managed devices and network locations.

The chapter includes the following sections:

Update Device Firmware

If firmware updates are available for managed devices, Insight detects and lists the updates and lets you update the firmware on individual devices. If you enable Insight notifications, email notifications, or both, you receive notification of the new firmware.

Update Device Firmware Using the Insight App

If firmware updates are available for managed devices, the Insight app detects and lists the updates and lets you update the firmware on individual devices. You cannot manually download a firmware version to the Insight app and upload it to a device.

To update the firmware for a device using the Insight app:

1. Launch the Insight app.
2. In the menu at the bottom, tap **Networks**.
3. If you set up more than one network in Insight, at the top of the page, select your network.
4. Tap **Firmware Management**.

   If any firmware updates are available, the page shows the devices for which the updates are available. For those devices, the current firmware version and the update firmware version are listed.
5. If multiple devices are shown, select the device for which you want to update the firmware and tap **UPDATE**.

   The Update firmware page displays.
6. Read the warning and tap **CONTINUE**.

   The firmware update process starts. A progress bar shows the progress of the update. The process takes a few minutes.

   When the firmware update is complete, the device automatically reboots, causing it to temporarily disconnect from the cloud. Unless you disabled notifications, the Insight app notifies you when the device is reconnected to the cloud and to the Insight app.
7. Tap the arrow at the top of the page to return to the previous page.
8. In the menu at the bottom, tap **Devices**.
9. Select the device for which you just updated the firmware.
10. Verify that the updated firmware version is listed under the image of the device.

Update Device Firmware Using the Cloud Portal

If firmware updates are available for managed devices, the Insight Cloud Portal detects and lists the updates and lets you update the firmware on individual devices. You cannot manually download a firmware version to the Cloud Portal and upload it to a device.

To update the firmware for a device using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Firmware**.
   The page displays the devices in the network, their current firmware versions, and the date that the firmware was last updated.

   If any firmware updates are available, the page shows the devices for which the updates are available. For those devices, the current firmware version and the update firmware version are listed.
4. Click the **update** icon to the right of the device for which you want to update the firmware.
   The Update firmware pop-up window opens.
5. Read the warning, and click the **Yes, update firmware** button.
   The firmware update process starts. A progress bar shows the progress of the update. The process takes a few minutes.

   When the firmware update is complete, the device automatically reboots, causing it to temporarily disconnect from the cloud. Unless you disabled notifications, the Cloud Portal notifies you when the device is reconnected to the cloud.
6. Verify that the updated firmware version is listed next to the device by doing one of the following:

   - If you did not close the page, refresh the page.
   - If you closed the page, do the following:

     a. From the network menu at the top of the page, select your network.
     The Summary page displays.

     b. Select **Firmware**.
     The page displays the device with the updated firmware version listed next to it.

Reboot a Device Remotely

You can reboot a device remotely using the Insight app or Cloud Portal.

Reboot a Device From the Insight App

To reboot a device from the Insight app:

1. Launch the Insight app.
2. To sort your devices or filter them, tap the icon to the left of + at the top of the screen.
3. Select the device that you want to remove from the Insight app.

4. Tap **Reboot**.
5. Tap **Continue** to confirm that you want to reboot the device.

   The device reboots, disconnects from Insight, and reconnects to Insight. Depending on the type of device, this process takes three to four minutes.

Reboot a Device From the Cloud Portal

To reboot a device from the Cloud Portal:

1. Access the Cloud Portal.

   All network locations display.
2. At the top of the page, select **My Devices**.

   The page displays headings for the network locations with active devices.
3. For the network to which you assigned the device, click **+** to the right of the heading.

   The page expands and displays all devices in the network.

   If you are not sure to which network you assigned the device, click the **Filter Devices** button, click the button for the type of device, and click the **Apply** button. Now only devices of the filtered type display on the page.

   If you do know the network but many devices are assigned to the network, you can also filter on device type within that network.
4. Point to the device and click the **pencil** icon at the right of the page.

   The page that displays shows details about the device.
5. At the upper right of the page, click the **Reboot** button.

   The Device Reboot pop-up window opens.
6. Click the **Continue** button.

   The device reboots, disconnects from Insight, and reconnects to Insight. Depending on the type of device, this process takes three to four minutes.

Reload the Last Saved Configuration on an Insight Managed Device

For Insight Managed switches and Insight Managed access points, you can use the Insight app to reload the configuration to restore the last saved configuration for the device. This is the configuration that was last saved on the Insight cloud-based management platform. If you use the Cloud Portal, you can restore the last saved configuration on Insight Managed switches but not on Insight Managed access points. However, for Insight Managed access points, you can reset the configuration to default settings (see *Reset an Insight Managed Access Point to Factory Default Settings Using the Cloud Portal* on page 33).

Reload the Configuration on a Device Using the Insight App

To reload the configuration on a device using the Insight app:

1. Launch the Insight app.
2. To sort your devices or filter them, tap the icon to the left of + at the top of the screen.
3. Select the device for which you want to reload the configuration.
4. Tap **Diagnostics**.
5. Tap **Reload**.
6. Tap **Reload** to confirm that you want to reload the configuration.

   The configuration is reloaded. When the reload process is complete, the device restarts, reconnects to Insight, and becomes available again in the same network. This process can take up to 10 minutes.

Reload the Configuration on an Insight Managed Switch Using the Cloud Portal

Note This procedure applies to Insight Managed switches. It does not apply to Insight Managed access points and Insight Managed ReadyNAS storage systems.

To reload the configuration on an Insight Managed switch using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.
2. At the top of the page, select **My Devices**.

   The page displays headings for the network locations with active devices.
3. For the network to which you assigned the device, click **+** to the right of the heading.

   The page expands and displays all devices in the network.

   If you are not sure to which network you assigned the device, click the **Filter Devices** button, click the button for the type of device, and click the **Apply** button. Now only devices of the filtered type display on the page.

   If you do know the network but many devices are assigned to the network, you can also filter on device type within that network.
4. Point to the device and click the **pencil** icon at the right of the page.

   The page that displays shows details about the device.
5. At the upper right of the page, click the **Reload** button.

   The Reload Configuration pop-up window opens.
6. Click the **Yes, reload** button.

   The configuration is reloaded. When the reload process is complete, the device restarts, reconnects to Insight, and becomes available again in the same network. This process can take up to 10 minutes.

Reset an Insight Managed Device to Factory Default Settings

You can reset an Insight Managed switch or Insight Managed access point to factory default settings.

If you use the Cloud Portal, you can reset the device through the portal and do not need physical access to the device.

If you use the Insight app, you must remove the device from Insight, physically reset the device, add the device to Insight again, and then add the device to the network location again.

WARNING:
Returning your device to factory default settings erases all configured settings. Do not follow this procedure unless you are sure that you want to return all settings to their factory defaults.

If you want to remove a device from your Insight account so that you can assign it to another Insight network location or place it in standalone mode so that it does not connect to Insight, see *Remove a Device From Your Insight Account Using the Cloud Portal* on page 35.

Reset a Device That You Manage in the Insight App to Factory Default Settings

You cannot reset a device to factory defaults using the Insight app. You must physically reset the device. However, before you do so, you must first remove the device from Insight. After you reset the device, you can add the device back to Insight.

To reset a device that you manage in the Insight app to factory default settings:

1. Launch the Insight app.
2. Select the device that you want to reset to factory default settings.
3. Tap **Remove**.
4. Tap **Remove** again to confirm that you want to remove the device from your Insight account.
5. Locate the device **Reset** button.
6. Using a straightened paper clip, press and hold the **Reset** button for at least 10 seconds.
7. Release the **Reset** button.

   The configuration is reset to factory default settings. When the reset is complete, the device reboots. This process takes several minutes.

WARNING:
To avoid the risk of corrupting the firmware, do not interrupt the reset process. Do not turn off the device. Wait until the device finishes restarting and the Power LED turns solid green.

8. Connect the device to a network and complete the setup process using the Insight App or Cloud Portal, or use the local browser interface to put the device in standalone mode so that it does not connect to Insight.

Note If you add the device to an existing Insight network location, it inherits the configuration of that network location. If you do not want the device to inherit that network configuration, you can create a new network location, add the device to that network location, and then reconfigure the device.

For more information about adding your device to Insight again, see *Discover, Add, and Register Devices* on page 18.

Reset an Insight Managed Access Point to Factory Default Settings Using the Cloud Portal

After you reset an Insight Managed access point to factory default settings using the Cloud Portal, the access point restarts, reconnects to Insight, and becomes available again in the same network. However, if you do not want the access point to reconnect to the same network, do not follow this procedure but remove the access point from Insight (see *Remove a Device From Your Insight Account Using the Cloud Portal* on page 35).

Note This procedure applies to Insight Managed access points. It does not apply to Insight Managed switches and Insight Managed ReadyNAS storage systems.

To reset an Insight Managed access point to factory default settings using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. At the top of the page, select **My Devices**.
   The page displays headings for the network locations with active devices.
3. For the network to which you assigned the device, click **+** to the right of the heading.
   The page expands and displays all devices in the network.
   If you are not sure to which network you assigned the device, click the **Filter Devices** button, click the button for the type of device, and click the **Apply** button. Now only devices of the filtered type display on the page.
   If you do know the network but many devices are assigned to the network, you can also filter on device type within that network.
4. Point to the device and click the **pencil** icon at the right of the page.

The page that displays shows details about the device.

5. At the upper right of the page, click the **Reset** button.
   The Factory reset pop-up window opens.
6. Click the **Yes, reset** button.
   The configuration is reset to factory default settings. When the reset is complete, the device restarts, reconnects to Insight, and becomes available again in the same network. This process can take up to 10 minutes.

Remove a Device From Your Insight Account

You can remove a device from your Insight account so that you can assign it to another Insight network location or place it in standalone mode so that it does not connect to Insight.

Tip When you add a device to an existing Insight network location, it inherits the configuration of that network location. If you do not want the device to inherit that network configuration, you can remove the device from your Insight account, create a new network location, add the device to that network location, and then reconfigure the device.

Remove a Device From Your Insight Account Using the Insight App

To remove a device from your Insight account using the Insight app:

1. Launch the Insight app.
2. To sort your devices or filter them, tap the icon to the left of + at the top of the screen.
3. Select the device that you want to remove from your Insight account.
4. Tap **Remove**.
5. Tap **Remove** again to confirm that you want to remove the device from your account.
   After the device restarts and goes online, the device displays in the Insight app under INSIGHT MANAGEABLE DEVICES as an unclaimed device. For information about adding the device to an Insight network location, see *Add a Device by Scanning Your Network With the Insight App* on page 19.

Note If want to use the device in standalone mode, access the local browser interface of the device and change the management mode of the device.

Remove a Device From Your Insight Account Using the Cloud Portal

To remove a device from your Insight account using the Cloud Portal:

1. Access the Cloud Portal.
   All network locations display.
2. At the top of the page, select **My Devices**.
   The page displays headings for the network locations with active devices.
3. For the network to which you assigned the device, click **+** to the right of the heading.
   The page expands and displays all devices in the network.
   If you are not sure to which network you assigned the device, click the **Filter Devices** button, click the button for the type of device, and click the **Apply** button. Now only devices of the filtered type display on the page.
   If you do know the network but many devices are assigned to the network, you can also filter on device type within that network.
4. Point to the device and click the **pencil** icon at the right of the page.
   The page that displays shows details about the device.
5. At the upper right of the page, click the **Delete** button.
   For a switch or ReadyNAS storage system, the Delete pop-up window opens. For an access point, the Remove Device pop-up window opens.
6. Depending on the type of device, do one of the following:.
   - For a switch or ReadyNAS storage system, click the **Yes, continue** button.
   - For an access point, click the **Remove** button.

   Your settings are saved and the device is removed from your Insight account.
   For information about adding the device to Insight again so that you can assign the device to another Insight network location, see *Add a Device by Entering Its Serial Number Using the Cloud Portal* on page 21.

Note If want to use the device in standalone mode, access the local browser–based management interface of the device and change the management mode of the device.

Display or Change the Device Admin Password for a Network Location

By default, the factory default password for a device is **password**. This password lets you access the local browser interface for the device, if you choose to use that management method.

However, after you add a device to a network location through the Insight app or Cloud Portal, you must use the admin password for that Insight network location, even to log in to the local browser interface. That is, you no longer need to use the factory default password for that device or a custom password that you already set up through the local browser interface for that device. For *all* devices that you add through the Insight app or Cloud Portal to one particular network location, you can now use a single password, which is the device admin password for the network location in Insight.

Display or Change the Device Admin Password for a Network Location Using the Insight App

To display or change the device admin password for a network location using the Insight app:

1. Launch the Insight app.
2. In the menu at the bottom, tap **Networks**.
3. If you set up more than one network in Insight, at the top of the page, select the network for which you want to display the device admin password.
4. Tap **Edit Network**.
   The Edit Network page displays.
5. Tap the **eye** icon to the right of the **Device Admin Password** field.
   The device admin password for the network displays.
6. To change the device admin password, do the following:
   a. Tap the password.
      A pop-up window opens.
   b. Type a new password in the **Device Admin Password** field.
   c. Tap **Save**.

Display or Change the Device Admin Password for a Network Location Using the Cloud Portal

To display or change the device admin password for a network location using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. If the network menu at the top of the page does not shows All Locations, click the network menu and select **See all locations**.
3. For the network location that you want to view or change, click the **…** button and select **Edit location** from the pop-up menu.
   The Network Location Settings page displays.
4. Click the **eye** icon to the right of the **Device Admin Password** field.

The device admin password for the network displays.

5. To change the device admin password, do the following:

   a. Type a new password in the **Device Admin Password** field.

   b. Click the **Save** button.
   Your settings are saved.

Manage 802.1x Network Access Authentication With RADIUS Servers

The following features use 802.1x access authentication with RADIUS servers:

- WPA2 Enterprise WiFi security (supported on Insight Managed access points)
- MAC ACLs with RADIUS authentication (supported on Insight Managed access points)

If your network uses *one* of these features (they are mutually exclusive), you must set up RADIUS servers. You can set up primary and secondary RADIUS servers. By default, accounting is enabled, but you cannot set up separate RADIUS accounting servers. You can also disable accounting.

Note Insight does not support 802.1x access authentication with RADIUS servers for Insight Managed switches. Support might be added in a future release.

Set Up RADIUS Servers for a Network Location Using the Insight App

To set up RADIUS servers for a network location using the Insight app:

1. Launch the Insight app.
2. In the menu at the bottom, tap **Networks**.
3. If you set up more than one network in Insight, at the top of the page, select the network for which you want to display the device admin password.
4. Tap **Edit Network**.
   The Edit Network page displays.
5. Tap **RADIUS**.
6. Tap the **802.1x Access Authentication** button so that the button displays green.
   The fields become editable.
7. Specify the primary and secondary RADIUS servers and the reauthentication time.
   Be sure that the IP addresses that you specify are reachable from your network.
   By default, the reauthentication time is 3600 seconds.
8. To disable accounting, tap the **Accounting** button so that the button displays white.

By default, the button is green and accounting is enabled.

9. Tap **Save**.

Set Up RADIUS Servers for a Network Location Using the Cloud Portal

To set up RADIUS servers for a network location using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. If the network menu at the top of the page does not shows All Locations, click the network menu and select **See all locations**.
3. For the network location for which you want to set up RADIUS servers, click the **…** button and select **Edit location** from the pop-up menu.
   The Network Location Settings page displays.
4. Select **Radius**.
   The RADIUS settings display.
5. Click the **802.1x Access Authentication** button so that the button displays green.
   The fields become editable.
6. Specify the primary and secondary RADIUS servers and the reauthentication time.
   Be sure that the IP addresses that you specify are reachable from your network.
   By default, the reauthentication time is 3600 seconds.
7. To disable accounting, click the **Accounting** button so that the button displays gray.
   By default, accounting is enabled and the button displays green.
8. Click the **Save** button.
   Your settings are saved.

Manage VLANs and VLAN-Based Features

4

Virtual LANs (VLANs) are network-specific. You can use a switch or a WiFi access point to set up a VLAN for an Insight network location, but the VLAN applies to the entire network location to which the switch or WiFi access point belongs.

This chapter includes the following sections:

VLAN Concepts

You can define a local area network (LAN) as a broadcast domain. Hubs, bridges, switches, and WiFi access points in the same physical segment or segments connect all end nodes. End nodes can communicate with each other without a router. Routers connect LANs, routing the traffic to each appropriate port.

A virtual LAN (VLAN) is a local area network that maps devices on a basis other than geographic location, for example, by department, type of user, or primary application. Traffic that flows between different VLANs must go through a router, just as if the VLANs are on two separate LANs.

A VLAN is a group of network devices (computers, servers, and other resources) that behave as if they are connected to a single network segment, even though they might not be. For example, the marketing personnel might be located throughout a building, but if they are all assigned to a single VLAN, they can share resources and bandwidth as if they are connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specific individuals, depending on how you set up the VLAN.

VLANs provide a number of advantages:

- **VLANs let you easily segment your network**. You can group users who communicate most frequently with each other in a common VLAN, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- **VLANS are easy to manage**. You can quickly add or change network nodes and make other network changes through the Insight mobile app or Cloud Portal.
- **VLANs provide increased performance**. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- **VLANs enhance network security**. VLANs create virtual boundaries that can be crossed only through a router. Therefore, you can use standard, router-based security measures to restrict access to a VLAN.

Plan the VLANs in Your Insight Network

Before you set up VLANs, we recommend that you plan the entire physical and logical setup for the network (known as network topology) carefully. VLAN configuration mistakes can cause serious connectivity and security problems on your network. If you are not experienced setting up computer networks, consider hiring an IT or network professional.

We also recommend that you plan your network's logical topology (which devices must be connected to each other) before you plan the physical topology (where each device must go, how to run the Ethernet cables).

When multiple VLANs exist on your network, decide which ports must be members of each VLAN. All ports that are members of a VLAN receive traffic that is sent on that VLAN. Then, you must decide whether each port must be a tagged member or an untagged member of the VLAN. A port is tagged for a VLAN when traffic that leaves the switch through that port includes an IEEE 802.1Q header with that VLAN's numerical identifier (VLAN ID) on it. If a port is an untagged member of a VLAN, the switch removes the existing 802.1Q header before sending traffic through that port.

VLAN Membership and Tagging

The following are basic principles of VLAN membership and tagging:

- Each port can be a member of an unlimited number of VLANs, but traffic on that port will be slow if it is a member of several busy VLANs. If you plan to make a port a member of multiple VLANs, consider setting up a link aggregation group (LAG) for increased bandwidth and throughput over that connection.
- Each port can be an untagged member of a single VLAN only. If a port is already an untagged member of a VLAN, you cannot add it as an untagged member of any other VLANs.
- All untagged traffic that enters the switch is assigned to the default or native VLAN, which is VLAN 1. VLAN 1 is also the management VLAN on switches that support management VLANs.
- If a port is a member of a LAG or you plan to add it to a LAG, do not add it to a VLAN or tag it individually. You must add the LAG to the VLAN as a single unit.
- We recommend that you classify each port as either an access port or a trunk port. An access port is a member of a single VLAN and connects to a computer, printer, or other device on the edge of a network. A trunk port connects the switch to a router, to other switches, or to access points. A trunk port must participate in multiple VLANs because all traffic that passes between the switch and the rest of the network must go through that port.
- Some networked devices recognize 802.1Q tagging, and some do not. If a device does not recognize tags, it rejects any tagged traffic that it receives, so it can be only an untagged member of a VLAN.
- If you are not sure whether a device supports 802.1Q tagging, see the device's documentation. The following list contains general guidelines that are not applicable in all cases:

  - Most printers do not recognize 802.1Q tags.
  - If a computer must be a tagged member of a VLAN, you must configure a VLAN ID on the network interface controller (NIC) of the computer. All other computers must be untagged.
  - Most network attached storage (NAS) devices either support 802.1Q tagging, support multiple NICs with multiple Ethernet ports (which can be added to different VLANs), or both.
  - Most Voice over Internet Protocol (VoIP) phones recognize 802.1Q tags.
  - Most WiFi access points recognize 802.1Q tags.
  - Unmanaged switches and some switches with limited management functions do not recognize 802.1Q tags.
  - Most business routers recognize 802.1Q tags. Most home routers do not.

Management VLAN Concepts

A management virtual local area network (VLAN) is a much smaller network that is contained within your regular network. The primary benefit of using a management VLAN is improved network security. When all management traffic is on a separate VLAN, it is much harder for unauthorized users to make changes to your network or monitor network traffic.

Another potential benefit is that a management VLAN can help you minimize the impact of a broadcast storm on other VLANs by giving you a separate path to access your network.

On NETGEAR devices that support management VLANs, the management VLAN, VLAN 1, is also the native or default VLAN. By default, all ports are members of the default VLAN. For the management VLAN to be secure, it must be used only for controlling and managing your network devices. You must restrict access to the management VLAN and configure other VLANs to carry all regular network traffic.

If you decide to restrict access to the management VLAN, especially with an access control list (ACL), make sure that you make your computer or device a member of the VLAN and add its MAC address to the ACL (if applicable). Otherwise, you must log in from an allowed device or lose access to the management functions of the switch. If you are unable to log in on an allowed device, you must reset the switch to factory default settings to regain management access.

How a VLAN Works on an Insight Managed Switch

A smart switch treats incoming packets in the following way:

- If an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID. Each port is assigned a default VLAN ID that you can configure. The default setting is 1.
- If a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID. The packet proceeds to the VLAN that is specified by the VLAN ID in the packet.
- If a packet enters through a port that is a member of the VLAN that is specified by the VLAN ID in the packet, the packet can be sent to other ports with the same VLAN ID.
- If a packet enters through a port that is not a member of the VLAN that is specified by the VLAN ID in the packet, the packet is dropped.
- Packets that leave the switch are either tagged (T) or untagged (U), depending on the VLAN to which the port belongs.

Create a Custom VLAN

After you create a custom VLAN, configure the port VLAN IDs (PVIDs) for the new VLAN (see *Configure Port VLAN IDs for Switch Ports* on page 61).

CAUTION:

In the following procedures, do not enable MAC address authentication or IP address filtering unless you are sure that you understand the consequences for your network. If you are not sure, consult your IT department.

Create a Custom VLAN Using the Insight App

To create a custom VLAN using the Insight app:

1. Launch the Insight app.
2. Click **Networks** in the menu at the bottom of the page.
3. If you set up more than one Insight network location, at the top of the page, select the network for which you want to set up the VLAN.

4. Tap **Wired Settings**.
5. At the top of the Wired Settings page, tap **VLAN**.
6. Tap **+** in the upper right corner of the page.
7. Tap **Custom Setup**.
8. Enter a name for your VLAN.
9. Enter a VLAN ID.

   VLAN IDs can be any number from 1 to 4093 *except* the IDs that are already reserved. The following VLAN IDs are reserved:

   - 1 (management VLAN)
   - 4088 (voice VLAN)
   - 4089 (Auto-Video VLAN)

10. Tap **QoS (Traffic Priority)** and tap a priority from 0 to 7 to specify how important the traffic on this VLAN is.

    The highest priority is 7.

11. Tap **Port Members**.

    The page displays each switch at the network location.

WARNING:
Configuring a VLAN on the network uplink port (the port that connects your device to the Internet) might disconnect your device from the Insight cloud. We recommend that you do not configure a VLAN on the cloud uplink port until you configure an alternate network cloud uplink.

Note If you tag a port that is a member of a link aggregation group (LAG), all member ports of that LAG are automatically tagged.

12. Select the switch ports that must be members of the VLAN by using the following options:

    - **Individual port**. Tap an individual port on an individual switch to select the port. Tapping a selected port again clears the port.
      A selected port is indicated by a green check mark.
    - **Select All**. Tap **Select All** above an individual switch to select all ports on that switch. After you tap **Select All**, the button changes to a **Deselect All** button, allowing you to clear the selection of the ports.
    - **Delete**. Below all switches, tap **Delete** to clear all selected ports on all switches.
    - **Access Port**. Tap individual ports on individual switches and, below all switches, tap **Access Port** to make the selected ports access ports.

An access port is a port on which traffic is untagged. An access port is intended for a connection between the switch and an end device, for which the port does not need to process tagged frames because all traffic belongs to the same VLAN.

- **Trunk Port**. Tap individual ports on individual switches and, below all switches, tap **Trunk Port** to make the selected ports trunk ports.
  A trunk port is a port on which traffic can be tagged. A trunk port is intended for a connection between two switches (or a switch and a WiFi access point), for which the port must be capable of processing tagged frames to segment the traffic for different VLANs.

13. To enable MAC address authentication for the new VLAN, tap **MAC Authentication**, and do the following:

    a. Select one of the following modes:

       - **Allow**. No devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
       - **Deny**. All devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    b. Tap **Add Devices**. From the list of devices that are automatically detected, select the check boxes with the MAC addresses of the devices that you want to add, and tap **ADD**.

    c. To add a device manually, tap **Manual**, enter a name in the **Device Name** field, enter a MAC address in the **MAC Address** field, and tap **ADD**.

    Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the MAC address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable MAC authentication.

    d. Tap the **Enable MAC Authentication** button.
    If MAC authentication is enabled, the button displays green.

14. To enable IP address filtering for the new VLAN, tap **IP Filtering**, and do the following:

    a. Select one of the following modes:

       - **Allow**. No devices are allowed to connect, except for devices for which you specify the IP addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
       - **Deny**. All devices are allowed to connect, except for devices for which you specify the IP addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    b. Tap **Add Devices**. From the list of devices that are automatically detected, select the check boxes with the IP addresses for the devices that you want to add, and tap **ADD**.

    c. To add a device manually, tap **Manual**, enter a device name or a range name in the **Device Name** field, and add a single IP address or a range of IP addresses by doing one of the following:

- **Single IP address**. In the **IP Address** field, enter an IP address, clear the **Add range of devices** check box, and tap **ADD**.
- **Range of IP addresses**. Keep the **Add range of devices** check box selected, enter a network mask address in the **IP Mask** field, and tap **ADD**.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the IP address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable IP filtering.

d. Tap the **Enable IP Filtering** button.
If IP filtering is enabled, the button displays green.

15. Tap **Save**.
Your settings are saved but it might take up to 20 seconds for the new settings to be applied.

Note For information about assigning port VLAN IDs (PVIDs) for the new VLAN, see *Configure the Port VLAN ID Using the Insight App* on page 62.

Create a Custom VLAN Using the Cloud Portal

To create a custom VLAN using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.
2. Select your network.
The Summary page displays.
3. Select **Wired**.
The Wired page displays.
4. At the top right of the page, click the **Settings** button.
The VLAN page displays.
5. At the top right of the page, click the **+** (**Add VLAN**) button.
The Create VLAN pop-up window opens.
6. Select **Custom Setup** and click the **Next** button.
The settings page for creating a VLAN displays.
7. In the **VLAN Name** field, enter a name for your VLAN.
8. In the **VLAN ID** field, enter a VLAN ID.
VLAN IDs can be any number from 1 to 4093 *except* the IDs that are already reserved. The following VLAN IDs are reserved:

- 1 (management VLAN)
- 4088 (Auto-VoIP VLAN)
- 4089 (Auto-Video VLAN)

9. From the **QoS (Traffic Priority**) menu , select a priority from 0 to 7 to specify how important the traffic on this VLAN is.

   The highest priority is 7.

10. Click **+** to the right of the Port Members heading.

    Graphics of the switches in the network display.

WARNING:
Configuring a VLAN on the network uplink port (the port that connects your device to the Internet) might disconnect your device from the Insight cloud. We recommend that you do not configure a VLAN on the cloud uplink port until you configure an alternate network cloud uplink.

Note If you tag a port that is a member of a link aggregation group (LAG), all member ports of that LAG are automatically tagged.

11. Select the switch ports that must be members of the VLAN by using the following options:

    - **Individual port**. Click an individual port to select it. Clicking a selected port again clears the port. A selected port is indicated by a green check mark.
    - **Select All**. Click the **Select All** button under a switch to select all ports on that switch. After you click the **Select All** button, the button changes to a **Deselect All** button, allowing you to clear the selection of the ports on that switch.
    - **Delete**. Click the **Delete** button under a switch to clear all selected ports on that switch.
    - **Access Port**. Click an individual port and then click the **Access Port** button under the switch to make the selected port an access port on that switch.
      An access port is a port on which traffic is untagged. An access port is intended for a connection between the switch and an end device, for which the port does not need to process tagged frames because all traffic belongs to the same VLAN.
    - **Trunk Port**. Click an individual port and then click the **Trunk Port** button under the switch to make the selected port a trunk port on that switch.
      A trunk port is a port on which traffic can be tagged. A trunk port is intended for a connection between two switches (or a switch and a WiFi access point), for which the port must be capable of processing tagged frames to segment the traffic for different VLANs.

12. Click the **Save** button.

    Your settings are saved. The VLAN page displays and shows the new VLAN.

13. Point to the new VLAN and click the **pencil** icon at the right of the page.

    The settings page for editing a VLAN displays.

14. To enable IP address filtering for the new VLAN, do the following:

a. Select **IP Filtering**.
The IP filtering settings display.

b. From the **Policy** menu, select one of the following modes:

- **Allow**. No devices are allowed to connect, except for devices for which you specify the IP addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
- **Deny**. All devices are allowed to connect, except for devices for which you specify the IP addresses and that are then denied access. To enable this mode, you must add at least one denied device.

c. Click the **Add Devices** button. In the Access Management pop-up window, which shows automatically detected devices, select the check boxes with the IP addresses for the devices that you want to add, and click the **Add** button.

d. To add a device manually, click the **Manual** button. In the Manual Access Management pop-up window, enter a device name or a range name in the **Device Name** field, and add a single IP address or a range of IP addresses by doing one of the following:

- **Single IP address**. In the **IP Address** field, enter an IP address, and click the **Add** button.
- **Range of IP addresses**. Select the **Add range of devices** check box, enter a network mask address in the **IP Mask** field, and click the **Add** button.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the IP address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable IP filtering.

e. Click the **Enable IP Filtering** button.
If IP filtering is enabled, the button displays green.

15. To enable MAC address authentication for the new VLAN, do the following:

a. Select **Mac Authentication**.
The MAC address authentication settings display.

b. From the **Policy** menu, select one of the following modes:

- **Allow**. No devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
- **Deny**. All devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then denied access. To enable this mode, you must add at least one denied device.

c. Click the **Add Devices** button. In the Access Management pop-up window, which shows automatically detected devices, select the check boxes with the MAC addresses of the devices that you want to add, and click the **Add** button.

d. To add a device manually, click the **Manual** button. In the Manual Access Management pop-up window, enter a name in the **Device Name** field, enter a MAC address in the **MAC Address** field, and click the **Add** button.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the MAC address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable MAC authentication.

e. Click the **Enable MAC Authentication** button.
If MAC authentication is enabled, the button displays green.

Note For information about assigning port VLAN IDs (PVIDs) for the new VLAN, see *Configure the Port VLAN ID for One or More Ports on the Same Switch Using the Cloud Portal* on page 62 or *Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal* on page 63.

Create a VoIP VLAN

Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, setting up a voice VLAN helps to provide a classification mechanism for voice packets so that they can be prioritized above data packets.

Insight supports VoIP optimization on one VLAN per network location. VLAN ID 4088 is reserved for the voice VLAN. However, you can change that ID.

After you create a voice VLAN, configure the port VLAN IDs (PVIDs) for the new VLAN (see *Configure Port VLAN IDs for Switch Ports* on page 61).

CAUTION:

In the following procedures, do not enable MAC address authentication or IP address filtering unless you are sure that you understand the consequences for your network. If you are not sure, consult your IT department.

Create a Voice VLAN Using the Insight App

To create a voice VLAN using the Insight app:

1. Launch the Insight app.
2. Click **Networks** in the menu at the bottom of the page.
3. If you set up more than one Insight network location, at the top of the page, select the network for which you want to set up the VLAN.
4. Tap **Wired Settings**.
5. At the top of the Wired Settings page, tap **VLAN**.
6. Tap **+** in the upper right corner of the page.

7. Tap **Voice VLAN**.
8. In the **VLAN Name** field, enter a name for the voice VLAN, or use the name default name of Voice VLAN.
9. In the **VLAN ID** field, enter a VLAN ID, or use the default voice VLAN ID of 4088.

   VLAN IDs can be any number from 1 to 4093 *except* the IDs that are already reserved. The following VLAN IDs are reserved:

   - 1 (management VLAN)
   - 4088 (voice VLAN)
   - 4089 (Auto-Video VLAN)

   Note We recommend that you keep VoIP optimization for the voice VLAN enabled. Be sure that the **Voice Optimization** button displays green.

10. If you do not want to use the default priority value of 5, tap **QoS (Traffic Priority)** and tap a priority from 0 to 7.

    The IEEE default priority value for VoIP traffic is 5. The highest priority is 7.

11. Tap **Port Members**.

    The page displays each switch at the network location.

    WARNING:
    Configuring a VLAN on the network uplink port (the port that connects your device to the Internet) might disconnect your device from the Insight cloud. We recommend that you do not configure a VLAN on the cloud uplink port until you configure an alternate network cloud uplink.

    Note By default, all switch ports are preselected as members of the voice VLAN. If you untag a port that is a member of a link aggregation group (LAG), all member ports of that LAG are automatically untagged.

12. Select the switch ports that must be members of the VLAN by using the following options:

    - **Individual port**. Tap an individual port on an individual switch to select the port. Tapping a selected port again clears the port.
      A selected port is indicated by a green check mark.
    - **Select All**. Tap **Select All** above an individual switch to select all ports on that switch. After you tap **Select All**, the button changes to a **Deselect All** button, allowing you to clear the selection of the ports.
    - **Delete**. Below all switches, tap **Delete** to clear all selected ports on all switches.
    - **Access Port**. Tap individual ports on individual switches and, below all switches, tap **Access Port** to make the selected ports access ports.

An access port is a port on which traffic is untagged. An access port is intended for a connection between the switch and an end device, for which the port does not need to process tagged frames because all traffic belongs to the same VLAN.

- **Trunk Port**. Tap individual ports on individual switches and, below all switches, tap **Trunk Port** to make the selected ports trunk ports.
  A trunk port is a port on which traffic can be tagged. A trunk port is intended for a connection between two switches (or a switch and a WiFi access point), for which the port must be capable of processing tagged frames to segment the traffic for different VLANs.

13. To enable MAC address authentication for the new VLAN, tap **MAC Authentication**, and do the following:

    a. Select one of the following modes:

       - **Allow**. No devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
       - **Deny**. All devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    b. Tap **Add Devices**. From the list of devices that are automatically detected, select the check boxes with the MAC addresses of the devices that you want to add, and tap **ADD**.

    c. To add a device manually, tap **Manual**, enter a name in the **Device Name** field, enter a MAC address in the **MAC Address** field, and tap **ADD**.

    Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the MAC address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable MAC authentication.

    d. Tap the **Enable MAC Authentication** button.
    If MAC authentication is enabled, the button displays green.

14. To enable IP address filtering for the new VLAN, tap **IP Filtering**, and do the following:

    a. Select one of the following modes:

       - **Allow**. No devices are allowed to connect, except for devices for which you specify the IP addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
       - **Deny**. All devices are allowed to connect, except for devices for which you specify the IP addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    b. Tap **Add Devices**. From the list of devices that are automatically detected, select the check boxes with the IP addresses for the devices that you want to add, and tap **ADD**.

    c. To add a device manually, tap **Manual**, enter a device name or a range name in the **Device Name** field, and add a single IP address or a range of IP addresses by doing one of the following:

- **Single IP address**. In the **IP Address** field, enter an IP address, clear the **Add range of devices** check box, and tap **ADD**.
- **Range of IP addresses**. Keep the **Add range of devices** check box selected, enter a network mask address in the **IP Mask** field, and tap **ADD**.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the IP address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable IP filtering.

d. Tap the **Enable IP Filtering** button.
If IP filtering is enabled, the button displays green.

15. Tap **Save**.
Your settings are saved but it might take up to 20 seconds for the new settings to be applied.

Note For information about assigning port VLAN IDs (PVIDs) for the new VLAN, see *Configure the Port VLAN ID Using the Insight App* on page 62.

Create a Voice VLAN Using the Cloud Portal

To create a voice VLAN using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.
2. Select your network.
The Summary page displays.
3. Select **Wired**.
The Wired page displays.
4. At the top right of the page, click the **Settings** button.
The VLAN page displays.
5. At the top right of the page, click the **+** (**Add VLAN**) button.
The Create VLAN pop-up window opens.
6. Select **Voice VLAN** and click the **Next** button.
The settings page for creating a voice VLAN displays.
7. Enter a name for the voice VLAN, or use the name default name of Voice VLAN.
8. In the **VLAN ID** field, enter a VLAN ID.
VLAN IDs can be any number from 1 to 4093 *except* the IDs that are already reserved. The following VLAN IDs are reserved:

- 1 (management VLAN)
- 4088 voice VLAN)
- 4089 (Auto-Video VLAN)

Note We recommend that you keep VoIP optimization for the voice VLAN enabled. Be sure that the **Voice Optimization** button displays green.

9. If you do not want to use the default priority value of 5, from the **QoS (Traffic Priority**) menu, select a priority from 0 to 7.

   The IEEE default priority value for VoIP traffic is 5. The highest priority is 7.

10. Click **+** to the right of the Port Members heading.

    Graphics of the switches in the network display.

WARNING:
Configuring a VLAN on the network uplink port (the port that connects your device to the Internet) might disconnect your device from the Insight cloud. We recommend that you do not configure a VLAN on the cloud uplink port until you configure an alternate network cloud uplink.

Note By default, all switch ports are preselected as members of the voice VLAN. If you untag a port that is a member of a link aggregation group (LAG), all member ports of that LAG are automatically untagged.

11. Select the switch ports that must be members of the VLAN by using the following options:

    - **Individual port**. Click an individual port to select it. Clicking a selected port again clears the port. A selected port is indicated by a green check mark.
    - **Select All**. Click the **Select All** button under a switch to select all ports on that switch. After you click the **Select All** button, the button changes to a **Deselect All** button, allowing you to clear the selection of the ports on that switch.
    - **Delete**. Click the **Delete** button under a switch to clear all selected ports on that switch.
    - **Access Port**. Click an individual port and then click the **Access Port** button under the switch to make the selected port an access port on that switch.
      An access port is a port on which traffic is untagged. An access port is intended for a connection between the switch and an end device, for which the port does not need to process tagged frames because all traffic belongs to the same VLAN.
    - **Trunk Port**. Click an individual port and then click the **Trunk Port** button under the switch to make the selected port a trunk port on that switch.
      A trunk port is a port on which traffic can be tagged. A trunk port is intended for a connection between two switches (or a switch and a WiFi access point), for which the port must be capable of processing tagged frames to segment the traffic for different VLANs.

12. Click the **Save** button.

Your settings are saved. The VLAN page displays and shows the new VLAN.

13. Point to the new VLAN and click the **pencil** icon at the right of the page.
    The settings page for editing a VLAN displays.

14. To enable IP address filtering for the new VLAN, do the following:

    a. Select **IP Filtering**.
    The IP filtering settings display.

    b. From the **Policy** menu, select one of the following modes:

    - **Allow**. No devices are allowed to connect, except for devices for which you specify the IP addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
    - **Deny**. All devices are allowed to connect, except for devices for which you specify the IP addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    c. Click the **Add Devices** button. In the Access Management pop-up window, which shows automatically detected devices, select the check boxes with the IP addresses for the devices that you want to add, and click the **Add** button.

    d. To add a device manually, click the **Manual** button. In the Manual Access Management pop-up window, enter a device name or a range name in the **Device Name** field, and add a single IP address or a range of IP addresses by doing one of the following:

    - **Single IP address**. In the **IP Address** field, enter an IP address, and click the **Add** button.
    - **Range of IP addresses**. Select the **Add range of devices** check box, enter a network mask address in the **IP Mask** field, and click the **Add** button.

    Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the IP address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable IP filtering.

    e. Click the **Enable IP Filtering** button.
    If IP filtering is enabled, the button displays green.

15. To enable MAC address authentication for the new VLAN, do the following:

    a. Select **Mac Authentication**.
    The MAC address authentication settings display.

    b. From the **Policy** menu, select one of the following modes:

    - **Allow**. No devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
    - **Deny**. All devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then denied access. To enable this mode, you must add at least one denied device.

c. Click the **Add Devices** button. In the Access Management pop-up window, which shows automatically detected devices, select the check boxes with the MAC addresses of the devices that you want to add, and click the **Add** button.

d. To add a device manually, click the **Manual** button. In the Manual Access Management pop-up window, enter a name in the **Device Name** field, enter a MAC address in the **MAC Address** field, and click the **Add** button.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the MAC address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable MAC authentication.

e. Click the **Enable MAC Authentication** button.
If MAC authentication is enabled, the button displays green.

Note For information about assigning port VLAN IDs (PVIDs) for the new VLAN, see *Configure the Port VLAN ID for One or More Ports on the Same Switch Using the Cloud Portal* on page 62 or *Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal* on page 63.

Configure the Default Auto-Video VLAN

Insight Managed switches support video prioritization using Internet Group Management Protocol (IGMP) snooping. IGMP specifies how a host, such as a computer, can register with a router to receive specific multicast traffic (streaming media is the most common type of multicast traffic). IGMP snooping improves network congestion and streaming performance by sending multicast traffic only to the ports that want to receive it instead of to all ports.

Insight Managed switches provide a default Auto-Video VLAN, which is optimized for video. The Auto-Video VLAN ID is 4089. You can configure the Auto-Video VLAN but cannot change the VLAN ID.

After you configure the Auto-Video VLAN, configure the port VLAN IDs (PVIDs) for the Audio-Video VLAN (see *Configure Port VLAN IDs for Switch Ports* on page 61).

CAUTION:

In the following procedures, do not enable MAC address authentication or IP address filtering unless you are sure that you understand the consequences for your network. If you are not sure, consult your IT department.

Configure the Default Auto-Video VLAN Using the Insight App

To configure the Auto-Video VLAN using the Insight app:

1. Launch the Insight app.
2. Click **Networks** in the menu at the bottom of the page.

3. If you set up more than one Insight network location, at the top of the page, select the network for which you want to set up the VLAN.
4. Tap **Wired Settings**.
5. At the top of the Wired Settings page, tap **VLAN**.
6. Tap **Video VLAN**.
7. To give your VLAN a different name, enter it in the **VLAN Name** field.
   The default name is Video VLAN.

Note The VLAN ID is 4089. You cannot change the ID for the Auto-Video VLAN.

Note We recommend that you keep video optimization (IGMP Snooping) for the Auto-Video VLAN enabled. Be sure that the **Video Optimization (IGMP Snooping)** button displays green.

8. If you do not want to use the default priority value of 4, tap **QoS (Traffic Priority)** and tap a priority from 0 to 7.
   The IEEE default priority level for video VLANs is 4. The highest priority is 7.
9. Tap **Port Members**.
   The page displays each switch in at the network location.

WARNING:
Configuring a VLAN on the network uplink port (the port that connects your device to the Internet) might disconnect your device from the Insight cloud. We recommend that you do not configure a VLAN on the cloud uplink port until you configure an alternate network cloud uplink.

Note If you tag a port that is a member of a link aggregation group (LAG), all member ports of that LAG are automatically tagged.

10. Select the switch ports that must be members of the VLAN by using the following options:

- **Individual port**. Tap an individual port on an individual switch to select the port. Tapping a selected port again clears the port.
  A selected port is indicated by a green check mark.
- **Select All**. Tap **Select All** above an individual switch to select all ports on that switch. After you tap **Select All**, the button changes to a **Deselect All** button, allowing you to clear the selection of the ports.
- **Delete**. Below all switches, tap **Delete** to clear all selected ports on all switches.
- **Access Port**. Tap individual ports on individual switches and, below all switches, tap **Access Port** to make the selected ports access ports.

An access port is a port on which traffic is untagged. An access port is intended for a connection between the switch and an end device, for which the port does not need to process tagged frames because all traffic belongs to the same VLAN.

- **Trunk Port**. Tap individual ports on individual switches and, below all switches, tap **Trunk Port** to make the selected ports trunk ports.
  A trunk port is a port on which traffic can be tagged. A trunk port is intended for a connection between two switches (or a switch and a WiFi access point), for which the port must be capable of processing tagged frames to segment the traffic for different VLANs.

11. To enable MAC address authentication for the Auto-Video VLAN, tap **MAC Authentication**, and do the following:

    a. Select one of the following modes:

       - **Allow**. No devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
       - **Deny**. All devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    b. Tap **Add Devices**. From the list of devices that are automatically detected, select the check boxes with the MAC addresses of the devices that you want to add, and tap **ADD**.

    c. To add a device manually, tap **Manual**, enter a name in the **Device Name** field, enter a MAC address in the **MAC Address** field, and tap **ADD**.

    Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the MAC address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable MAC authentication.

    d. Tap the **Enable MAC Authentication** button.
    If MAC authentication is enabled, the button displays green.

12. To enable IP address filtering for the Auto-Video VLAN, tap **IP Filtering**, and do the following:

    a. Select one of the following modes:

       - **Allow**. No devices are allowed to connect, except for devices for which you specify the IP addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
       - **Deny**. All devices are allowed to connect, except for devices for which you specify the IP addresses and that are then denied access. To enable this mode, you must add at least one denied device.

    b. Tap **Add Devices**. From the list of devices that are automatically detected, select the check boxes with the IP addresses for the devices that you want to add, and tap **ADD**.

    c. To add a device manually, tap **Manual**, enter a device name or a range name in the **Device Name** field, and add a single IP address or a range of IP addresses by doing one of the following:

- **Single IP address**. In the **IP Address** field, enter an IP address, clear the **Add range of devices** check box, and tap **ADD**.
- **Range of IP addresses**. Keep the **Add range of devices** check box selected, enter a network mask address in the **IP Mask** field, and tap **ADD**.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the IP address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable IP filtering.

d. Tap the **Enable IP Filtering** button.
If IP filtering is enabled, the button displays green.

13. Tap **Save**.
Your settings are saved but it might take up to 20 seconds for the new settings to be applied.

Note For information about assigning port VLAN IDs (PVIDs) for the Auto-Video VLAN, see *Configure the Port VLAN ID Using the Insight App* on page 62.

Configure the Default Auto-Video VLAN Using the Cloud Portal

To configure the default Auto-Video VLAN using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.
2. Select your network.
The Summary page displays.
3. Select **Wired**.
The Wired page displays.
4. At the top right of the page, click the **Settings** button.
The VLAN page displays.
5. Point to Video VLAN and click the **pencil** icon at the right of the page.
The settings page for editing a VLAN displays.
6. In the **VLAN Name** field, enter a name for the Auto-Video VLAN, or use the name default name of Video VLAN.

Note The VLAN ID is 4089. You cannot change the ID for the Auto-Video VLAN.

Note We recommend that you keep video optimization (IGMP Snooping) for the Auto-Video VLAN enabled. Be sure that the **Video Optimization (IGMP Snooping)** button displays green.

7. If you do not want to use the default priority value of 4, select a priority from 0 to 7 from the **QoS (Traffic Priority**) menu.

   The IEEE default priority level for video VLANs is 4. The highest priority is 7.

8. Click **+** to the right of the Port Members heading.

   Graphics of the switches in the network display.

WARNING:
Configuring a VLAN on the network uplink port (the port that connects your device to the Internet) might disconnect your device from the Insight cloud. We recommend that you do not configure a VLAN on the cloud uplink port until you configure an alternate network cloud uplink.

Note If you tag a port that is a member of a link aggregation group (LAG), all member ports of that LAG are automatically tagged.

9. Select the switch ports that must be members of the VLAN by using the following options:

   - **Individual port**. Click an individual port to select it. Clicking a selected port again clears the port. A selected port is indicated by a green check mark.
   - **Select All**. Click the **Select All** button under a switch to select all ports on that switch. After you click the **Select All** button, the button changes to a **Deselect All** button, allowing you to clear the selection of the ports on that switch.
   - **Delete**. Click the **Delete** button under a switch to clear all selected ports on that switch.
   - **Access Port**. Click an individual port and then click the **Access Port** button under the switch to make the selected port an access port on that switch.
     An access port is a port on which traffic is untagged. An access port is intended for a connection between the switch and an end device, for which the port does not need to process tagged frames because all traffic belongs to the same VLAN.
   - **Trunk Port**. Click an individual port and then click the **Trunk Port** button under the switch to make the selected port a trunk port on that switch.
     A trunk port is a port on which traffic can be tagged. A trunk port is intended for a connection between two switches (or a switch and a WiFi access point), for which the port must be capable of processing tagged frames to segment the traffic for different VLANs.

10. Click the **Save** button.

    Your settings are saved. The VLAN page displays and shows the configured VLAN.

11. Point again to Video VLAN and click the **pencil** icon at the right of the page.

    The settings page for editing a VLAN displays again.

12. To enable IP address filtering for the Auto-Video VLAN, do the following:

    a. Select **IP Filtering**.
       The IP filtering settings display.

    b. From the **Policy** menu, select one of the following modes:

- **Allow**. No devices are allowed to connect, except for devices for which you specify the IP addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
- **Deny**. All devices are allowed to connect, except for devices for which you specify the IP addresses and that are then denied access. To enable this mode, you must add at least one denied device.

c. Click the **Add Devices** button. In the Access Management pop-up window, which shows automatically detected devices, select the check boxes with the IP addresses for the devices that you want to add, and click the **Add** button.

d. To add a device manually, click the **Manual** button. In the Manual Access Management pop-up window, enter a device name or a range name in the **Device Name** field, and add a single IP address or a range of IP addresses by doing one of the following:

- **Single IP address**. In the **IP Address** field, enter an IP address, and click the **Add** button.
- **Range of IP addresses**. Select the **Add range of devices** check box, enter a network mask address in the **IP Mask** field, and click the **Add** button.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the IP address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable IP filtering.

e. Click the **Enable IP Filtering** button.
If IP filtering is enabled, the button displays green.

13. To enable MAC address authentication for the Auto-Video VLAN, do the following:

a. Select **Mac Authentication**.
The MAC address authentication settings display.

b. From the **Policy** menu, select one of the following modes:

- **Allow**. No devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then allowed access. To enable this mode, you must add at least one allowed device.
- **Deny**. All devices are allowed to connect, except for devices for which you specify the MAC addresses and that are then denied access. To enable this mode, you must add at least one denied device.

c. Click the **Add Devices** button. In the Access Management pop-up window, which shows automatically detected devices, select the check boxes with the MAC addresses of the devices that you want to add, and click the **Add** button.

d. To add a device manually, click the **Manual** button. In the Manual Access Management pop-up window, enter a name in the **Device Name** field, enter a MAC address in the **MAC Address** field, and click the **Add** button.

Note If you set up a list with allowed devices, no matter how you add devices, be sure that you add the MAC address of the device that you are using to configure the VLAN, or you will lose access to the VLAN after you enable MAC authentication.

e. Click the **Enable MAC Authentication** button.
If MAC authentication is enabled, the button displays green.

Note For information about assigning port VLAN IDs (PVIDs) for the Auto-Video VLAN, see *Configure the Port VLAN ID for One or More Ports on the Same Switch Using the Cloud Portal* on page 62 or *Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal* on page 63.

Configure VLAN-Based Quality of Service on a Switch

You can configure VLAN-based Quality of Service (QoS) on an Insight Managed switch.

For each VLAN, you can set an 802.1p traffic priority class value from 0 (low) through 7 (high). This type of QoS is referred to as Class of Service (CoS) queuing because, in effect, you assign a class value to one of eight hardware queues on each port that is a member of the VLAN.

CoS queueing enables the switch to group various types of traffic (for example, data or voice) based on their VLAN and latency requirements and give preference to time-sensitive traffic. For example, traffic with a priority value of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority value, such as 5, might be time-sensitive traffic, such as voice or video.

Configure VLAN-Based Quality of Service on a Switch Using the Insight App

To configure QoS for an existing VLAN using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Tap **VLANs In Use**.
   The VLANs display. The Management VLAN and the Video VLAN are default VLANs. If you added any custom VLANs, they also display.
5. Select the VLAN that you want to configure.
   The VLAN configuration options display.
6. Next to Traffic Priority, tap the down arrow.
   Class values from 0 (low priority) to 7 (high priority) display.
7. Select a value.
8. Tap **Save**.

Your settings are saved.

Configure VLAN-Based Quality of Service on a Switch Using the Cloud Portal

To configure QoS for an existing VLAN using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. At the top right of the page, click the **Settings** button.
   The VLAN page displays.
5. Point to the VLAN that you want to configure and click the **pencil** icon at the right of the page.
   The settings page for editing a VLAN displays.
6. From the **Traffic Priority** menu, select a priority from 0 to 7.
   The highest priority is 7.
7. Click the **Save** button.
   Your settings are saved and the switch restarts.

Configure Port VLAN IDs for Switch Ports

By default, all switch ports are members of VLAN 1 and are assigned a port VLAN ID (PVID) of 1. If you set up other VLANs, you can assign a different PVID to a port. The following requirements apply to PVIDs:

- Each port must be assigned a PVID (by default, PVID 1).
- If no other value is specified, the default VLAN PVID is used.
- To change a port's default PVID, you must first create a VLAN that includes the port as a member.

You can use the Insight app or the Cloud Portal to configure a PVID through the following options:

- You can configure an individual port.
- You can configure a batch of ports on the same switch.
- You can configure a group of ports on different switches in the same network.

Configure the Port VLAN ID Using the Insight App

To configure the port VLAN ID (PVID) for a single port or the same PVID for a group of ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.

   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.

   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap **Default VLAN (PVID)**.
8. Swipe up or down to select a VLAN.

   By default, the management VLAN with ID 1 is assigned to a port, so the PVID for the port is 1.
9. Tap **Save**.

   Your settings are saved.

Configure the Port VLAN ID for One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you set the port VLAN ID (PVID) for a single port or the same PVID for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To configure the PVID for one or more ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.
2. Select your network.

   The Summary page displays.
3. Select **Wired**.

   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.

   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:

   - **Select a single port**. Do the following:

a. In the graphic, click the port that you want to configure.
The Summary page for the port displays.

b. Select **Settings**.
The Settings page for the port displays.

- **Select a group of ports**. Do the following:

a. In the graphic, click any port.
The Summary page for the port displays.

b. Select **Settings**.
The Settings page for the port displays.

c. Click the **Batch port configuration** button.
A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.

d. Click the **Yes, Open Batch Config** button.
A graphic displays again.

e. In the graphic, select the ports that you want to configure.
Selected ports display green.

6. From the **Default VLAN (PVID)** menu, select a VLAN.
By default, the management VLAN with ID 1 is assigned to a port, so the PVID for the port is 1.

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

Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you set the same port VLAN ID (PVID) for a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To configure the PVID for a group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.

2. Select your network.
The Summary page displays.

3. Select **Wired**.
The Wired page displays.

4. At the top right of the page, click the **Settings** button.
The VLAN page displays.

5. Select **Group Port Config**.
   The Group Port Config page displays.
6. In the graphic for each switch that you want to configure, select the ports that you want to configure.
   Selected ports display green.
7. From the **Default VLAN** menu, select a VLAN.
   By default, the management VLAN with ID 1 is assigned to a port, so the PVID for the port is 1.
8. Click the **Save** button.
   Your settings are saved.

Manage Switch Features

5

This chapter describes how you can manage features that are specific to Insight Managed switches.

The chapter includes the following sections:

Configure Switch Ports

You can use the Insight app or the Cloud Portal to enable or disable ports and set the egress rate limit, storm rate limit, duplex mode, maximum Ethernet frame size, and speed for ports.

You can use the Insight app or the Cloud Portal to configure switch ports through the following options:

- You can configure an individual port.
- You can configure a batch of ports on the same switch.
- You can configure a group of ports on different switches in the same network.

Note In this section, each switch port feature is described in a separate subsection. However, if you are familiar with these features, which are common to many switches, you can simultaneously configure multiple features on multiple ports.

This section includes the following subsections:

- *Enable or Disable One or More Ports*
- *Set the Storm Rate Limit for Incoming Traffic for One or More Ports*
- *Set the Bandwidth Limit for Outgoing Traffic for One or More Ports*
- *Set the Duplex Mode for One or More Ports*
- *Set the Maximum Ethernet Frame Size for One or More Ports*
- *Set the Speed for One or More Ports*

For more information about configuring switch ports, see the following sections:

- For information about managing Power over Ethernet (PoE) for PoE-capable ports, see *Manage Power over Ethernet* on page 82.
- For information about configuring port VLAN IDs (PVIDs), which is a topic that is related to the configuration of VLANs, see *Configure Port VLAN IDs for Switch Ports* on page 61.

Enable or Disable One or More Ports

By default, all switch ports are enabled. You can disable ports (shut them down) and you can reenable ports (bring them up).

Note If you are familiar with switch port features, you can also simultaneously configure rate limits, the default VLAN, the duplex mode, the frame size, and the port speed for multiple ports.

Enable or Disable One or More Ports Using the Insight App

To enable or disable one or more ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.

4. Scroll down and tap **CONFIG PORTS**.
   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.
   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap the **Enable Port** button to enable or disable the ports.
   By default, all ports are enabled. If the button displays green, the selected ports are enabled. If the button displays white, the selected ports are disabled.
8. Tap **Save**.
   Your settings are saved.

Enable or Disable One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you enable or disable a single port or a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To enable or disable one or more ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:

   - **Select a single port**. Do the following:

     a. In the graphic, click the port that you want to configure.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

   - **Select a group of ports**. Do the following:

a. In the graphic, click any port.
The Summary page for the port displays.

b. Select **Settings**.
The Settings page for the port displays.

c. Click the **Batch port configuration** button.
A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.

d. Click the **Yes, Open Batch Config** button.
A graphic displays again.

e. In the graphic, select the ports that you want to configure.
Selected ports display green.

6. Click the **Enable Port** button to enable or disable the selected ports.
By default, all ports are enabled. If the button displays green, the selected ports are enabled. If the button displays gray, the selected ports are disabled.

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

Enable or Disable a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you enable or disable a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To enable or disable a group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.

2. Select your network.
The Summary page displays.

3. Select **Wired**.
The Wired page displays.

4. At the top right of the page, click the **Settings** button.
The VLAN page displays.

5. Select **Group Port Config**.
The Group Port Config page displays.

6. For each switch that you want to configure, in the graphic of the switch, select the ports that you want to configure.
Selected ports display green.

7. Click the **Enable Port** button to enable or disable the selected ports.

By default, all ports are enabled. If the button displays green, the selected ports are enabled. If the button displays gray, the selected ports are disabled.

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

Set the Storm Rate Limit for Incoming Traffic for One or More Ports

A broadcast storm is the result of an excessive number of broadcast packets that are simultaneously transmitted across a network by a single port. Forwarded broadcast packets can overload network resources and cause other problems. The storm rate specifies the maximum available bandwidth for incoming broadcast, multicast, and unknown unicast packets. If the rate that you specify is exceeded, the packets are discarded.

Set the Storm Rate Limit for Incoming Traffic for One or More Ports Using the Insight App

To set the storm rate limit for incoming traffic for one or more ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.
   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.
   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap **Storm Control Rate**.
   This setting specifies the maximum available bandwidth for incoming broadcast, multicast, and unknown unicast packets on the selected ports.
8. Move the slider to specify the limit as a percentage from 1 percent to 100 percent.
   By default, the rate is 100 percent. The selected percentage sets the allowable speed in relation to the available speed for the selected ports.
9. Tap **Save**.
   Your settings are saved.

Set the Storm Rate Limit for Incoming Traffic for One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you set the storm rate limit for incoming traffic for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To set the storm rate limit for incoming traffic for a single port or for a group of ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:
   - **Select a single port**. Do the following:
     a. In the graphic, click the port that you want to configure.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
   - **Select a group of ports**. Do the following:
     a. In the graphic, click any port.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
     c. Click the **Batch port configuration** button.
        A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.
     d. Click the **Yes, Open Batch Config** button.
        A graphic displays again.
     e. In the graphic, select the ports that you want to configure.
        Selected ports display green.
6. If the rate limit settings do not display, to the right of the Rate Limit heading, click **+**.
   The rate limit settings display.
7. Move the **Storm Rate Limit** slider to specify the limit as a percentage from 1 percent to 100 percent.
   By default, the rate is 100 percent. The selected percentage sets the allowable speed in relation to the available speed for the selected ports.
8. Click the **Save** button.
   Your settings are saved.

Set the Storm Rate Limit for Incoming Traffic for a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you set the storm rate limit for incoming traffic for a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To set the storm rate limit for incoming traffic for group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. At the top right of the page, click the **Settings** button.
   The VLAN page displays.
5. Select **Group Port Config**.
   The Group Port Config page displays.
6. For each switch that you want to configure, in the graphic of the switch, select the ports that you want to configure.
   Selected ports display green.
7. If the rate limit settings do not display, to the right of the Rate Limit heading, click **+**.
   The rate limit settings display.
8. Move the **Storm Rate Limit** slider to specify the limit as a percentage from 1 percent to 100 percent.
   By default, the rate is 100 percent. The selected percentage sets the allowable speed in relation to the available speed for the selected ports.
9. Click the **Save** button.
   Your settings are saved.

Set the Bandwidth Limit for Outgoing Traffic for One or More Ports

The bandwidth limit for a port is typically used to shape the egress (outgoing or outbound) traffic transmission rate. The default value is 100 percent, which means that no maximum limit is set for the speed, that is, the port uses the line rate. You can set values from 1 percent to 100 percent.

Set the Bandwidth Limit for Outgoing Traffic for One or More Ports Using the Insight App

To set the bandwidth limit for outgoing traffic for one or more ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.

   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.

   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap **Egress Rate Limit**.

   This setting specifies the maximum available bandwidth for outgoing traffic on the selected ports.
8. Move the slider to specify the limit as a percentage from 1 percent to 100 percent.

   By default, the rate is 100 percent. The selected percentage sets the allowable speed in relation to the available speed for the selected ports.
9. Tap **Save**.

   Your settings are saved.

Set the Bandwidth Limit for Outgoing Traffic for One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you set the bandwidth limit for outgoing traffic for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To set the bandwidth limit for outgoing traffic for a group of ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.
2. Select your network.

   The Summary page displays.
3. Select **Wired**.

   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.

   The Summary page for the switch displays.

5. Either select a single port or select a group of ports:

   - **Select a single port**. Do the following:

     a. In the graphic, click the port that you want to configure.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

   - **Select a group of ports**. Do the following:

     a. In the graphic, click any port.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

     c. Click the **Batch port configuration** button.
     A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.

     d. Click the **Yes, Open Batch Config** button.
     A graphic displays again.

     e. In the graphic, select the ports that you want to configure.
     Selected ports display green.

6. If the rate limit settings do not display, to the right of the Rate Limit heading, click **+**.
   The rate limit settings display.

7. Move the **Egress Rate Limit** slider to specify the limit as a percentage from 1 percent to 100 percent.
   By default, the rate is 100 percent. The selected percentage sets the allowable speed in relation to the available speed for the selected ports.

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

Set the Bandwidth Limit for Outgoing Traffic for a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you set the bandwidth limit for outgoing traffic for a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To set the bandwidth limit for outgoing traffic for a group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.

2. Select your network.
   The Summary page displays.

3. Select **Wired**.
   The Wired page displays.
4. At the top right of the page, click the **Settings** button.
   The VLAN page displays.
5. Select **Group Port Config**.
   The Group Port Config page displays.
6. For each switch that you want to configure, in the graphic of the switch, select the ports that you want to configure.
   Selected ports display green.
7. If the rate limit settings do not display, to the right of the Rate Limit heading, click **+**.
   The rate limit settings display.
8. Move the **Egress Rate Limit** slider to specify the limit as a percentage from 1 percent to 100 percent.
   By default, the rate is 100 percent. The selected percentage sets the allowable speed in relation to the available speed for the selected ports.
9. Click the **Save** button.
   Your settings are saved.

Set the Duplex Mode for One or More Ports

By default, all switch ports are enabled. You can disable ports (shut them down) and you can reenable ports (bring them up).

Note If you are familiar with switch port features, you can also simultaneously enable or disable ports and configure rate limits, the default VLAN, the frame size, and the port speed for multiple ports.

Set the Duplex Mode for One or More Ports Using the Insight App

To set the duplex mode for one or more ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.
   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.
   The Port Config Wizard page displays.
6. Select the ports that you want to configure.

7. Tap **Duplex Mode**.
8. Swipe **Auto**, **Full**, or **Half** into the selection field.

   - **Auto**. The duplex mode is set by the autonegotiation process. This is the default setting.
   - **Full**. The port transmits between the devices in both directions simultaneously.
   - **Half**. The port transmits between the devices in only one direction at a time.

9. Tap **Save**.
   Your settings are saved and the switch restarts.

Set the Duplex Mode for One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you set the duplex mode for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To set the duplex mode for a single port or for a group of ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:

   - **Select a single port**. Do the following:

     a. In the graphic, click the port that you want to configure.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

   - **Select a group of ports**. Do the following:

     a. In the graphic, click any port.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

     c. Click the **Batch port configuration** button.

A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.

d. Click the **Yes, Open Batch Config** button.
A graphic displays again.

e. In the graphic, select the ports that you want to configure.
Selected ports display green.

6. From the **Duplex Mode** menu, select a mode:

- **Auto**. The duplex mode is set by the autonegotiation process. This is the default setting.
- **Full**. The port transmits between the devices in both directions simultaneously.
- **Half**. The port transmits between the devices in only one direction at a time.

7. Click the **Save** button.
Your settings are saved and the switch restarts.

Set the Duplex Mode for a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you set the duplex mode for a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To set the duplex mode for group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.

2. Select your network.
The Summary page displays.

3. Select **Wired**.
The Wired page displays.

4. At the top right of the page, click the **Settings** button.
The VLAN page displays.

5. Select **Group Port Config**.
The Group Port Config page displays.

6. For each switch that you want to configure, in the graphic of the switch, select the ports that you want to configure.
Selected ports display green.

7. From the **Duplex Mode** menu, select a mode:

- **Auto**. The duplex mode is set by the autonegotiation process. This is the default setting.
- **Full**. The port transmits between the devices in both directions simultaneously.
- **Half**. The port transmits between the devices in only one direction at a time.

8. Click the **Save** button.
   Your settings are saved and the switch restarts.

Set the Maximum Ethernet Frame Size for One or More Ports

By default, the frame size for an Ethernet port is 1518 bytes. You can set a frame size of up and including to 9216 bytes.

> **Note** If you are familiar with switch port features, you also can simultaneously enable or disable ports and configure rate limits, the default VLAN, the duplex mode, and the port speed for multiple ports.

Set the Maximum Ethernet Frame Size for One or More Ports Using the Insight App

To set the maximum Ethernet frame size for one or more ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.
   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.
   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Move the slider to specify the maximum Ethernet frame size from 1518 bytes to 9216 bytes.
   By default, the setting is 1518 bytes.
8. Tap **Save**.
   Your settings are saved.

Set the Maximum Ethernet Frame Size for One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you set the maximum Ethernet frame size for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To set the maximum Ethernet frame size for one or more ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:
   - **Select a single port**. Do the following:
     a. In the graphic, click the port that you want to configure.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
   - **Select a group of ports**. Do the following:
     a. In the graphic, click any port.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
     c. Click the **Batch port configuration** button.
        A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.
     d. Click the **Yes, Open Batch Config** button.
        A graphic displays again.
     e. In the graphic, select the ports that you want to configure.
        Selected ports display green.
6. Move the slider to specify the maximum Ethernet frame size from 1518 bytes to 9216 bytes.
   By default, the setting is 1518 bytes.
7. Click the **Save** button.
   Your settings are saved.

Set the Maximum Ethernet Frame Size for a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you set the maximum Ethernet frame size for a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To set the maximum Ethernet frame size for a group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. At the top right of the page, click the **Settings** button.
   The VLAN page displays.
5. Select **Group Port Config**.
   The Group Port Config page displays.
6. For each switch that you want to configure, in the graphic of the switch, select the ports that you want to configure.
   Selected ports display green.
7. Move the slider to specify the maximum Ethernet frame size from 1518 bytes to 9216 bytes.
   By default, the setting is 1518 bytes.
8. Click the **Save** button.
   Your settings are saved.

Set the Speed for One or More Ports

By default, the speed for all ports is set to Auto, enabling the ports to detect the speed of the connection between the port and the attached device. You can also manually set the port speed to 10, 100, or 1000 Mbps.

Note If you are familiar with switch port features, you can also simultaneously enable or disable ports and configure rate limits, the default VLAN, the duplex mode, and the frame size for multiple ports.

Set the Speed for One or More Ports Using the Insight App

To set the speed for one or more ports using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.

   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.

   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap **Port Speed**.
8. Swipe **Auto**, **10 Mbps**, **100 Mbps**, or **1000 Mbps** into the selection field.

   By default, the setting is Auto.
9. Tap **Save**.

   Your settings are saved.

Set the Speed for One or More Ports on the Same Switch Using the Cloud Portal

This procedure lets you set the speed for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To set the speed for one or more ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.
2. Select your network.

   The Summary page displays.
3. Select **Wired**.

   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.

   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:

   - **Select a single port**. Do the following:

a. In the graphic, click the port that you want to configure.
The Summary page for the port displays.

b. Select **Settings**.
The Settings page for the port displays.

- **Select a group of ports**. Do the following:

a. In the graphic, click any port.
The Summary page for the port displays.

b. Select **Settings**.
The Settings page for the port displays.

c. Click the **Batch port configuration** button.
A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.

d. Click the **Yes, Open Batch Config** button.
A graphic displays again.

e. In the graphic, select the ports that you want to configure.
Selected ports display green.

6. From the **Port Speed** menu, select **Auto**, **10 Mbps**, **100 Mbps**, or **1000 Mbps**.
By default, the setting is Auto.

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

Set the Speed for a Group of Ports on Different Switches Using the Cloud Portal

This procedure lets you set the speed for a group of ports on different switches in the same network using the Group Port Config tool in the Cloud Portal.

To set the speed for a group of ports on different switches in the same network using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.

2. Select your network.
The Summary page displays.

3. Select **Wired**.
The Wired page displays.

4. At the top right of the page, click the **Settings** button.
The VLAN page displays.

5. Select **Group Port Config**.

The Group Port Config page displays.

6. For each switch that you want to configure, in the graphic of the switch, select the ports that you want to configure.

   Selected ports display green.

7. From the **Port Speed** menu, select **Auto**, **10 Mbps**, **100 Mbps**, or **1000 Mbps**.

   By default, the setting is Auto.

8. Click the **Save** button.

   Your settings are saved.

Manage Power over Ethernet

You can use the Insight app or the Cloud Portal to enable or disable Power over Ethernet (PoE) for PoE-capable ports, power-cycle PoE ports, and set the power limit for PoE-capable ports. You can also set up a PoE schedule for a network location and assign the schedule to ports on one or more switches at the network location. You can set up multiple PoE schedules for a network location.

This section includes the following subsections:

- *Enable or Disable PoE for One or More PoE-Capable Ports*
- *Power-Cycle One or More PoE Ports on a Switch*
- *Manually Set the PoE Power Limit for One or More Ports on a Switch*
- *Create a PoE Schedule*
- *Assign a PoE Schedule to One or More Ports on a Switch*

Enable or Disable PoE for One or More PoE-Capable Ports

By default, PoE is enabled for all PoE-capable switch ports.

Enable or Disable PoE for One or More Ports on a Switch Using the Insight App

To enable or disable PoE for one or more ports on a switch using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.

   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.

5. Tap **OK**.

   The Port Config Wizard page displays.

6. Select the ports that you want to configure.

7. Tap the **Enable PoE** button to enable or disable PoE.

   By default, PoE is enabled for all PoE-capable ports. If the button displays green, PoE is enabled on all selected PoE-capable ports. If the button displays white, PoE is disabled on all selected PoE-capable ports.

8. Tap **Save**.

   Your settings are saved.

Enable or Disable PoE for One or More Ports on a Switch Using the Cloud Portal

This procedure lets you enable or disable PoE for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To enable or disable PoE for a single port or for a group of ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.

2. Select your network.

   The Summary page displays.

3. Select **Wired**.

   The Wired page displays.

4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.

   The Summary page for the switch displays.

5. Either select a single port or select a group of ports:

   - **Select a single port**. Do the following:

     a. In the graphic, click the port that you want to configure.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

   - **Select a group of ports**. Do the following:

     a. In the graphic, click any port.
     The Summary page for the port displays.

     b. Select **Settings**.
     The Settings page for the port displays.

     c. Click the **Batch port configuration** button.
     A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.

     d. Click the **Yes, Open Batch Config** button.

A graphic displays again.

e. In the graphic, select the ports that you want to configure.
Selected ports display green.

6. If the PoE settings do not display, to the right of the Power Management (PoE Ports only) heading, click **+**.
The PoE settings display.

7. Click the **Enable PoE** button to enable or disable PoE for the selected ports.
By default, PoE is enabled for all PoE-capable ports. If the button displays green, PoE is enabled for the selected ports. If the button displays gray, PoE is disabled for the selected ports.

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

Power-Cycle One or More PoE Ports on a Switch

Situations might occur in which you want to power-cycle PoE ports on a switch.

Power-Cycle One or More PoE Ports on a Switch Using the Insight App

To power-cycle one or more PoE ports on a switch using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **PoE**.
By default, Ports is selected.
5. Tap **Power Cycle Ports**.
6. Select the check boxes for individual ports, or select the **Select All** check box for all ports.
7. Tap the **Start Power Cycle**.
A pop-up window displays a notification.
8. Tap **OK**.
The pop-up window closes.

Power-Cycle One or More PoE Ports on a Switch Using the Cloud Portal

To power-cycle one or more PoE ports on a switch using using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.
2. Select your network.

The Summary page displays.

3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Select **PoE**.
   The PoE page displays.
6. Click the **Power Cycle Ports** button.
   A graphic of the switch displays.
7. Select the PoE ports that you want to power-cycle.
   Selected ports display green.
8. Click the **Start Power Cycle** button.
   Your settings are saved and the selected ports are power-cycled.

Manually Set the PoE Power Limit for One or More Ports on a Switch

By default, the Insight Managed switches supply PoE power according to the default device class power requirements. You can override the default class and manually set the PoE power limit for one or more ports.

The following table shows the device classes for PoE+ devices adhering to the IEEE 802.3at standard. The device classes for PoE devices adhering to the IEEE 802.3af standard are identical with the exception that Device Class 4 is not supported.

Table 2. PoE and PoE+ device class power allocation

Device Class	Standard	Range of Power Delivered to the Powered Device	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
0	PoE and PoE+	0.44W–12.95W	15.4W	16.2W
1	PoE and PoE+	0.44W–3.84W	4.0W	4.2W
2	PoE and PoE+	3.84W–6.49W	7.0W	7.4W

Table 2. PoE and PoE+ device class power allocation (Continued)

Device Class	Standard	Range of Power Delivered to the Powered Device	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
3	PoE and PoE+	6.49W–12.95W	15.4W	16.2W
4	PoE+ only	12.95W–25.5W	30.0W	31.6W

Manually Set the PoE Power Limit for One or More Ports on a Switch Using the Insight App

To manually set the PoE power limit for one or more ports on a switch using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.

   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.

   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap **Power Limit**.
8. Tap the **Enable PoE** button to enable or disable PoE.
9. Select the ports that you want to configure.
10. Tap the **Use Default Class** button to enable or disable use of the PoE default class.

    By default, the PoE default class is used for all PoE-capable ports. If the button displays green, the default PoE class is used for all selected PoE-capable ports. If the button displays white, the default PoE class is not used for all selected PoE-capable ports and the **Power Limit (Watts)** slider displays.
11. Move the **Power Limit (Watts)** slider to specify the limit in watts.

    The default setting depends on the switch model and the detected powered device (PD) class.
12. Tap the arrow at the top of the page to return to the previous page.
13. Tap **Save**.

    Your settings are saved.

Manually Set the PoE Power Limit for One or More Ports on a Switch Using the Cloud Portal

This procedure lets you manually set the PoE power limit for a single port or for a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To manually set the PoE power limit for a single port or for a group of ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:
   - **Select a single port**. Do the following:
     a. In the graphic, click the port that you want to configure.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
   - **Select a group of ports**. Do the following:
     a. In the graphic, click any port.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
     c. Click the **Batch port configuration** button.
        A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.
     d. Click the **Yes, Open Batch Config** button.
        A graphic displays again.
     e. In the graphic, select the ports that you want to configure.
        Selected ports display green.
6. If the PoE settings do not display, to the right of the Power Management (PoE Ports only) heading, click **+**.
   The PoE settings display.

7. Click the **Use Default Class** button to enable or disable use of the PoE default class for the selected ports.

   By default, the PoE default class is used for all PoE-capable ports. If the button displays green, the PoE default class is used for the selected ports. If the button displays gray, the PoE default class is not used for the selected ports, and the **Power Limit (Watts)** slider displays.

8. Move the **Power Limit (Watts)** slider to specify the limit in watts.

   The default setting depends on the switch model and the detected powered device (PD) class.

9. Click the **Save** button.

   Your settings are saved.

Create a PoE Schedule

By default, PoE-capable ports can deliver PoE power continuously. You can set up one or more PoE schedules that you can assign to PoE ports and that you can use, for example, during evenings and weekends.

When a PoE schedule is active, PoE power is *disabled* on the PoE ports to which you assign the schedule, that is, the ports do not deliver PoE power. When the PoE schedule is not active, PoE power is *enabled* on the PoE ports to which you assign the schedule, that is, the ports do deliver PoE power.

Create a PoE Schedule Using the Insight App

To create a PoE schedule for a network location using the Insight app:

1. Launch the Insight app.
2. In the menu at the bottom, tap **Networks**.
3. Tap **Wired Settings**.
4. If you set up more than one network in Insight, at the top of the page, select the network for which you want to set up a PoE schedule.
5. Tap **PoE Schedules**.
6. Tap **Create Schedule**.

   The Create PoE Schedule page displays.

7. Using the controls on the page, give the schedule a name, set the days and time, if applicable, set the recurrence, and set the start date and end date for the schedule.

   You are setting up a schedule for a period during which PoE power is *disabled*. That is, the ports to which you assign this schedule do not deliver PoE power while the schedule is active.

8. Do one of the following:

   - To save the schedule, tap **Save**.
     Your settings are saved. The PoE Schedules page displays, showing the new schedule. By default, the schedule is enabled, that is, the button next to the schedule displays green.
     For information about assigning the schedule to PoE ports, see *Assign a PoE Schedule to One or More Ports on a Switch Using the Insight App* on page 90.
   - To save the schedule and immediately assign it to PoE ports, tap **Save and Pick Ports**.

A pop-up window displays a notification that the schedule is created and that you can now assign it to ports.
Do the following:

a. Tap **OK**.
Graphics of the switches at the network location display.

b. Select the PoE ports to which you want to assign the new schedule.
Selected ports display green.

c. Tap **Apply to Ports**.
Your settings are saved. The PoE Schedules page displays, showing the new schedule. By default, the schedule is enabled, that is, the button next to the schedule displays green.

Create a PoE Schedule Using the Cloud Portal

To create a PoE schedule for a network location using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. At the top right of the page, click the **Settings** button.
   The VLAN page displays.
5. Select **PoE Schedules**.
   The PoE Schedules page displays.
6. At the top right of the page, click the **+** (**Add Schedule**) button.
   The Add PoE Schedule pop-up window opens.
7. Using the controls on the page, give the schedule a name, set the days and time, if applicable, set the recurrence, and set the start date and end date for the schedule.
   You are setting up a schedule for a period during which PoE power is *disabled*. That is, the ports to which you assign this schedule do not deliver PoE power while the schedule is active.
8. Do one of the following:

   - To save the schedule, click the **Save** button.
     Your settings are saved. The PoE Schedules page displays, showing the new schedule. By default, the schedule is enabled, that is, the button next to the schedule displays green.
     For information about assigning the schedule to PoE ports, see *Assign a PoE Schedule to One or More Ports on a Switch Using the Cloud Portal* on page 90.
   - To save the schedule and immediately assign it to PoE ports, click the **Save and Pick Ports** button.
     The Edit Ports pop-up window opens and shows graphics of the switches at the network location.

Do the following:

a. Select the PoE ports to which you want to assign the new schedule.
Selected ports display green.

b. Click the **Save** button.
Your settings are saved. The PoE Schedules page displays, showing the new schedule. By default, the schedule is enabled, that is, the button next to the schedule displays green.

Assign a PoE Schedule to One or More Ports on a Switch

If you previously set up a PoE schedule (see *Create a PoE Schedule* on page 88), you can assign it to one or more PoE-capable ports on a switch.

Assign a PoE Schedule to One or More Ports on a Switch Using the Insight App

To assign a PoE schedule to one or more ports on a switch using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch that you want to configure.
4. Scroll down and tap **CONFIG PORTS**.
   A warning pop-up window opens and informs you that the values that are shown on the Port Config Wizard page for the ports are the default values and not the currently configured values.
5. Tap **OK**.
   The Port Config Wizard page displays.
6. Select the ports that you want to configure.
7. Tap **Power Schedule**.
   Swipe up or down to select a PoE schedule that you previously created (see *Create a PoE Schedule Using the Insight App* on page 88).
8. Tap **Save**.
   Your settings are saved.

Assign a PoE Schedule to One or More Ports on a Switch Using the Cloud Portal

This procedure lets you assign a PoE schedule to a single port or to a group of ports on the same switch using the Batch port configuration tool in the Cloud Portal.

To assign a PoE schedule to a single port or to a group of ports on the same switch using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wired**.
   The Wired page displays.
4. Scroll down to the Devices pane, point to the switch that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays.
5. Either select a single port or select a group of ports:
   - **Select a single port**. Do the following:
     a. In the graphic, click the port that you want to configure.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
   - **Select a group of ports**. Do the following:
     a. In the graphic, click any port.
        The Summary page for the port displays.
     b. Select **Settings**.
        The Settings page for the port displays.
     c. Click the **Batch port configuration** button.
        A warning pop-up window opens and informs you that the values that are shown on the wizard page for the ports are the default values and not the currently configured values.
     d. Click the **Yes, Open Batch Config** button.
        A graphic displays again.
     e. In the graphic, select the ports that you want to configure.
        Selected ports display green.
6. If the PoE settings do not display, to the right of the Power Management (PoE Ports only) heading, click **+**.
   The PoE settings display.
7. From the **PoE Schedule** menu, select a PoE schedule that you previously created (see *Create a PoE Schedule Using the Cloud Portal* on page 89).
8. Click the **Save** button.
   Your settings are saved.

Set Up Link Aggregation Between Two Network Devices

Link aggregation lets you combine multiple Ethernet links into a single logical link between two network devices. The most common combinations involve connecting a switch to another switch, a server, a network attached storage (NAS) device, or a multiport WiFi access point. Network devices treat the link aggregation group (LAG) as a single link, which increases throughput, fault tolerance, or both between the two devices.

Insight Managed switches support both static LAGs and Link Aggregation Control Protocol (LACP) for dynamic LAGs. If a physical link in a dynamic LAG goes down, other physical links in the same dynamic LAG continue to dynamically and transparently pass traffic. NETGEAR Insight assigns all VLANs at the network location to the LAG.

When you set up a LAG between two devices, the following requirements apply:

- The devices must be capable of supporting LAGs. For a dynamic LAG, both devices must be capable of supporting LACP.
- You must configure the LAG on each device. However, if both switches are Insight Managed switches, you can set up the LAG on one switch and specify the partner switch.
- On each device, specify at least two ports as members of the LAG.
- After you configure the LAG, connect the member ports with Ethernet cables. (If you do it before, you might create a network loop.)

Set Up Link Aggregation Between Two Devices Using the Insight App

To set up link aggregation between two devices using the Insight app:

1. Launch the Insight app.
2. In the menu at the bottom, tap **Networks**.
3. Tap **Wired Settings**.
4. If you set up more than one network in Insight, at the top of the page, select the network in which you want to set up a LAG.
5. Tap **LAG**.
6. Tap **+** in the upper right corner of the page.
7. Depending on the type of devices that you are using for the LAG, select the devices by doing one of the following:

   - **LAG between two Insight Managed switches**. Select the check box for each of the Insight Managed switches for which you want to set up the LAG.
   - **LAG between one Insight Managed switch and another type of device that supports LAGs**. Select the check box for the Insight Managed switch.

8. Tap **Next**.
9. In the **LAG Name** field, enter a name for the LAG.

10. If you do not want to enable the LAG immediately, tap the **Enable** button so that the button displays white.

    By default, the button displays green, and the LAG is enabled.

11. If you are setting up a dynamic LAG on switches that both support IEEE 802.3ad Link Aggregation Control Protocol (LACP), tap the **Static LAG** button so that the button displays white.

    By default, the button displays green and the LAG is set up as a static LAG.

    Note Insight Managed switches support LACP so that you can set up a dynamic LAG between them.

12. Depending on the type of devices that you are using for the LAG, select the member ports by doing one of the following:

    - **LAG between two Insight Managed switches**. For each Insight Managed switch, select at least two ports as members of the LAG.
    - **LAG between one Insight Managed switch and another type of device that supports LAGs**. For the Insight Managed switch, select at least two ports as members of the LAG. For the other device, see *Step 14*.

13. Tap **Save**.

    Your settings are saved.

14. If you are setting up a LAG for an Insight Managed switch and another type of device, you must manually configure the LAG on other type of the device.

    Note If you set up a static LAG, be sure that the switch ports that you are making members of the static LAG are using the same port speed, duplex mode, and flow control settings as on the Insight Managed switch.

15. Use Ethernet cables to connect the member ports of the LAG on each device.

    Unless you configured the LAG to be disabled (see *Step 10*), the LAG becomes active immediately.

Set Up Link Aggregation Between Two Devices Using the Cloud Portal

To set up link aggregation between two devices using the Cloud Portal:

1. Access the Insight Cloud Portal.

   All network locations display.

2. Select your network.

   The Summary page displays.

3. Select **Wired**.

The Wired page displays.

4. At the top right of the page, click the **Settings** button.
   The VLAN page displays.
5. Select **LAG**.
   The LAG page displays.
6. At the top right of the page, click the **+** (**Add LAG**) button.
   The Create New LAG pop-up window opens.
7. Depending on the type of devices that you are using for the LAG, select the devices by doing one of the following:

   - **LAG between two Insight Managed switches**. Select each Insight Managed switch.
   - **LAG between one Insight Managed switch and another type of device that supports LAGs**. Select the Insight Managed switch.

8. Click the **Next** button.
9. In the **LAG Name** field, enter a name for the LAG.
10. If you do not want to enable the LAG immediately, click the Enable **OFF** button.
    By default, the Enable **ON** button is selected and the LAG is enabled.
11. If you are setting up a dynamic LAG on switches that both support IEEE 802.3ad Link Aggregation Control Protocol (LACP), click the Static LAG **OFF** button.
    By default, the Static LAG **ON** button is selected and the LAG is set up as a static LAG.

    Note Insight Managed switches support LACP so that you can set up a dynamic LAG between them.

12. Click the **Save and Continue** button.
13. Depending on the type of devices that you are using for the LAG, select the member ports by doing one of the following:

    - **LAG between two Insight Managed switches**. For each Insight Managed switch, select at least two ports as members of the LAG.
    - **LAG between one Insight Managed switch and another type of device that supports LAGs**. For the Insight Managed switch, select at least two ports as members of the LAG. For the other device, see *Step 15*.

14. Click the **Save** button.
    Your settings are saved and the LAG page displays again, showing the configured LAG.
15. If you are setting up a LAG for an Insight Managed switch and another type of device, you must manually configure the LAG on other type of the device.

Note If you set up a static LAG, be sure that the switch ports that you are making members of the static LAG are using the same port speed, duplex mode, and flow control settings as on the Insight Managed switch.

16. Use Ethernet cables to connect the members ports of the LAG on each device.

    Unless you configured the LAG to be disabled (see *Step 10*), the LAG becomes active immediately.

Manage WiFi Access Point Features

6

This chapter describes how you can manage features that are specific to Insight Managed WiFi access points.

The chapter includes the following sections:

- *Create a WiFi Network on an Access Point Using the Insight App*
- *Configure Rate Limits for an Existing WiFi Network Using the Insight App*
- *Create a Captive Portal for an Existing WiFi Network Using the Insight App*

Note Cloud Portal sections for this chapter will be added in an upcoming revision of this manual.

Create a WiFi Network on an Access Point Using the Insight App

A WiFi network name is referred to as an SSID, which stands for service set identifier. When you create a new SSID on an access point, you are actually defining the settings for a new virtual access point (VAP). Each Insight Managed access point can support multiple SSIDs.

> **Note** An SSID that you create on one access point at a network location is shared and broadcast by all access points at the network location.

To create a new WiFi network on an access point using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the access point that you want to configure.
4. Tap **WiFi Networks**.
5. Tap **Add New WiFi (SSID)**.
6. If you want to disable broadcasting, tap the **Broadcast SSID** button.

   If you disable broadcast of the SSID, only users who know the name of your WiFi network can connect to it.
7. If you want the SSID to broadcast on a single radio band only, tap **Band** and select the radio band.

   By default, the SSID is broadcast on both radio bands.
8. Unless you are familiar with the band steering concept, leave band steering disabled.

   By default, band steering is disabled and the **Band Steering** button displays white.
9. If you want to use security other than the default WPA2-PSK security, tap **Security** and select another type of security.

   WPA2-PSK provides a secure connection but some legacy WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select **WPA/WPA2-PSK** for mixed mode security.

   If you want to use WPA2 enterprise security, you must set up RADIUS servers for the network location (see *Set Up RADIUS Servers for a Network Location Using the Insight App* on page 37).

   > **Note** Although you can set up an open network without any security, we do not recommend this. However, an open network might be appropriate for a WiFi hotspot at a public location.
10. If you select **WPA2-PSK** or **WPA/WPA2-PSK** security, tap **Password** and enter a password.

Note By default, the SSID is assigned to the Management VLAN with VLAN ID 1. However, if you configured other VLANs (see *Manage VLANs and VLAN-Based Features* on page 39) and you use VLAN 1 for management purposes only, you must specify another VLAN for the SSID so that the network can process the WiFi traffic on the SSID.

11. To assign a VLAN other than the Management VLAN to the SSID, do the following in the ADVANCED SETTINGS section:
    a. Tap **VLAN**.
    b. Swipe up or down to select a VLAN.
    c. Tap **Done**.
12. Tap **Save**.
    Your settings are saved.

Configure Rate Limits for an Existing WiFi Network Using the Insight App

If you do not plan to share WiFi access with many users, you probably do not need to set rate limits. However, if you notice WiFi speeds slowing because of heavy use, you might want to set upload rate limits, download rate limits, or both.

To configure rate limits for an existing WiFi network using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the access point that you want to configure.
4. Tap **WiFi Networks**.
5. Tap the WiFi network for which you want to set rate limits.
6. Scroll down and tap **Rate Limit**.
7. Tap the **Enable** button so that the button displays green.
   The rate limit settings display.
8. From the **Upload Data Rate Unit** menu, select **Kbps** (kilobits per second) or **Mbps** (megabits per second).
9. Move the **Upload Rate Limit** slider to select a limit from 64 Kbps to 1,000 Mbps (no limit), depending on your selection in the previous step.
10. From the **Download Data Rate Unit** menu, select **Kbps** or **Mbps**.
11. Move the **Download Rate Limit** slider to select a limit from 64 Kbps to 1,000 Mbps (no limit), depending on your selection in the previous step.
12. Tap the arrow in the upper left to return to the main WiFi settings page.
13. Tap **Save**.

Your settings are saved.

Create a Captive Portal for an Existing WiFi Network Using the Insight App

A captive portal is a page that guests see when they attempt to connect to your WiFi network. Insight lets you choose an image, a short message, and an optional end user license agreement (EULA) to display on your captive portal. For example, you could use an image of your business and a message that tells your customers where to find the WiFi password. The password for the captive portal is the same password that you set up for the WiFi network.

You can also set a session time-out period and specify a URL to redirect users to after they enter the captive portal.

To create a captive portal for an existing WiFi network using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the access point that you want to configure.
4. Tap **WiFi Networks**.
5. Tap the WiFi network for which you want to create a captive portal.
6. Tap **Captive Portal**.
7. Tap the **Captive Portal** button so that the button displays green.

   The captive portal settings display.
8. Tap **Display Message**, enter a title, and enter a message.
9. For the EULA content, do one of the following:

   - Tap the **EULA** button so that it displays white and the EULA content does not display when users view the captive portal.
   - Enter the EULA content that displays when users view the captive portal.
10. Tap the arrow in the upper left to return to the other captive portal settings.
11. For URL redirection, do one of the following:

    - Tap the **Redirect URL** so that the button displays gray and users are not redirected to a website after they view the captive portal.
    - Enter the URL for the website that users must be redirected to after they view the captive portal.
12. Tap **Session Timeout** and swipe up or down to select a session time-out period from 30 minutes to 24 hours.
13. If you want to use the default WiFi symbol as a captive portal log, tap **Default**.

Otherwise, do the following to select a logo image to display on the captive portal:

a. Tap **Replace**.

   The Insight app accesses your photos, or you can take a photo. Depending on the settings on your smartphone, you might need to allow the Insight app access to your photos or camera.

b. Select an existing photo or take a new photo and select it.

   The Captive Portal Logo pop-up window displays the selected photo.

c. Tap **Save**.

   The captive portal settings display again.

14. Tap **Preview** to see what the captive portal will look like to guests on your WiFi network.
15. After you are done editing the captive portal settings, tap **Save**.

    Your settings are saved. The captive portal is enabled on the WiFi network. However, by tapping the **Captive Portal** button so that the button displays gray, you can disable the captive portal without losing the settings.

Manage ReadyNAS Storage System Features

7

This chapter describes how you can manage features that are specific to Insight Managed ReadyNAS storage systems.

The chapter includes the following sections:

- *ReadyNAS Storage System Requirements for Insight*
- *Ethernet Ports eth0 and eth1 on a ReadyNAS Storage System*
- *Enable Secure Diagnostics Mode on a ReadyNAS Storage System Using the Insight App*

Note Cloud Portal sections for this chapter will be added in an upcoming revision of this manual.

ReadyNAS Storage System Requirements for Insight

You can use Insight to discover and monitor most ReadyNAS OS 6 storage systems. You can also perform some management functions, such as updating firmware, for certain models. For more information, see *Supported Devices* on page 10.

Before you can add a ReadyNAS storage system to your Insight account, as described in *Discover, Add, and Register Devices* on page 18, you must be sure of the following:

- Your ReadyNAS storage system is running ReadyNAS OS version 6.8.0 or a later version.
- ReadyCLOUD is enabled on your ReadyNAS storage system.

Ethernet Ports eth0 and eth1 on a ReadyNAS Storage System

A ReadyNAS storage system provides at least one Ethernet port, but some ReadyNAS storage systems provide more Ethernet ports. A network adapter is associated with each Ethernet port and is indicated by the label eth. The ReadyNAS local browser interface and Insight always display the network adapters in the same order, regardless of which Ethernet ports (network adapters) are connected to other devices and which are not.

When you view your ReadyNAS storage system network adapters in the local browser interface, in the Insight app, or in the Cloud Portal, the network adapters are listed starting with eth0 for the network adapter of the first Ethernet port, then eth1, eth2, and so on. The numbering does not start over for 10-Gigabit Ethernet ports.

If the Ethernet port that corresponds to network adapter eth0 is not connected to another device, the IP address for that port is listed as 0.0.0.0. The same applies to other Ethernet ports. If you see an IP address for a port listed as 0.0.0.0, that port is not connected to a device.

Enable Secure Diagnostics Mode on a ReadyNAS Storage System Using the Insight App

Enabling Secure Diagnostics Mode lets NETGEAR Technical Support log in to your ReadyNAS storage system remotely to help you troubleshoot. Do not enable Secure Diagnostics Mode unless NETGEAR Technical Support directs you to enable it.

To enable Secure Diagnostics Mode on a ReadyNAS storage system using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the ReadyNAS system that you want to configure.
4. Tap **Diagnostics > Diagnostics Mode**.
5. Tap the **Secure Diagnostics Mode** button so that the button displays green.
   A pop-up warning displays.
6. Tap **OK** to close the warning.

Your settings are saved and a five-digit port number displays. To connect to your ReadyNAS storage system remotely, NETGEAR Technical Support needs this number.

Monitor Insight Networks and Devices 8

This chapter describes the options to monitor the Insight networks and devices using the Insight app and Cloud Portal.

The chapter includes the following sections:

- *Overview of the Monitoring Options for a Network Location in the Cloud Portal*
- *Customize the Cloud Portal Pages*

Note Insight app sections and Cloud Portal sections for this chapter will be added in an upcoming revision of this manual.

Overview of the Monitoring Options for a Network Location in the Cloud Portal

The Cloud Portal provides extensive options for monitoring your Insight networks and devices.

For each network location, the main menu at the top of the page provides the following options:

- The **Summary** tab provides access to the following monitoring widgets:
  - **Properties**. The widget displays the types and numbers of active devices, clients, storage volumes, and so on.
  - **System Health**. The widget displays the number of online and offline devices and the situations that require your attention.
  - **Wireless Clients**. The widget displays the number of WiFi clients for each access point, viewable per radio band and per predefined period.
  - **Port Utilization**. The widget displays the status and utilization of the ports for each switch.
  - **Notifications**. The widget displays the notifications for the network location.
  - **Optional widgets**. You can add the Storage Utilization, Wireless Data Consumption, Switch Traffic Utilization, and PoE Power Utilization widgets.
- The **Wireless** tab provides access to the following monitoring widgets (in addition to access to the settings for the access points):
  - **Usage : Clients**. For each access point, the widget displays the number of WiFi clients, viewable per radio band and per predefined period.
  - **Usage : Traffic**. For each access point, the widget displays the volume of WiFi traffic, viewable per radio band and per predefined period.
  - **Devices**. For each access point, the widget displays the status, serial number, number of clients, model, MAC address, firmware version, IP address, and the up time (the period since the device was last restarted).

    Note To display more details about an access point, point to it and click the **pencil** icon at the right of the page.

  - **Client List**. For each WiFi client, the widget displays the type of device, the access point it is connected to, the SSID it is connected to, and the operating system, MAC address, IP address, number of transmitted bytes, number of received bytes, RSSI strength (indicated by an icon), and radio band that the device uses.
- The **Wired** tab provides access to the following monitoring widgets (in addition to access to the settings for the switches):
  - **Usage**. For each switch, the widget displays the ports that are connected and using power, connected and not using power, disabled, in an error state, and available (free).
  - **PoE Power Usage**. For each switch, the widget displays the PoE power usage.

> **Note** To display more details, click the **Detailed View** button.

- **Wired - Traffic**. For each switch, the widget displays the volume of wired traffic, viewable per predefined period.
- **Devices**. For each switch, the widget displays the status, the serial number, the model, the MAC address, the firmware version, the IP address, and the uptime.

> **Note** To display more details about a switch, point to it and click the **pencil** icon at the right of the page.

- The **Storage** tab provides access to the following monitoring widgets:
  - **Usage**. For each ReadyNAS storage system, the widget displays the size of the data, snapshots, and free storage space.
  - **Devices**. For each ReadyNAS storage system, the widget displays the status, serial number, model, MAC address, firmware version, IP address, and up time.

> **Note** To display more details about a ReadyNAS storage system, point to it and click the **pencil** icon at the right of the page.

- The **Firmware** tab provides access to the following monitoring widgets:
  - **Updates Available**. The widget displays the devices for which firmware updates are available, the current firmware versions on the devices, and the latest firmware versions that are available for the devices.
  - **Up-To-Date**. The widget displays the devices for which the firmware is up to date, the current firmware version, and the date on which the firmware was updated.
  - **Offline**. The widget displays devices that are offline, if any are offline.
- The **Devices** tab displays a single widget with the devices at the network location. For each device, the widget displays the status, serial number, number of clients, model, MAC address, firmware version, IP address, and up time.

> **Note** To display more details about a device, point to it and click the **pencil** icon at the right of the page.

- The **Clients** tab displays a single widget with the WiFi clients at the network location. For each WiFi client, the widget displays the type of device, the device name, the access point the device is connected to, the SSID the device is connected to, and the operating system, MAC address, IP address, radio band that the device uses, number of transmitted bytes, number of received bytes, channel, associated time stamp, BSSID, and RSSI strength (indicated by an icon).

Customize the Cloud Portal Pages

You can customize the Cloud Portal pages,

Depending on the page, in a widget, you can customize the following options:

- By clicking the **…** (**Options**) button on one of the following pages, you can customize the widgets that display on the page:
  - Summary page for a network location
  - Wireless page for a network location
  - Wired page for a network location
- By clicking the **…** (**Options**) button *in* a widget, you can customize the columns that display in the table in the widget.

Perform Diagnostics and Troubleshooting

9

This chapter describes how to use the diagnostics options in the Insight app, how to troubleshoot connections between the Insight app and devices, and how to troubleshoot managed devices.

The chapter includes the following sections:

Note Cloud Portal sections for this chapter will be added in an upcoming revision of this manual.

Use the Device Diagnostic Options in the Insight App

The diagnostics options that are available for an Insight managed device in the Insight app depend on the type of device:

- **Insight Managed switches**. You can reload the last saved cloud configuration, share diagnostics information, configure port mirroring, and perform a cable test.
- **Insight Managed access points**. You can reload the last saved cloud configuration and share diagnostics information.
- **Insight Managed ReadyNAS storage systems**. You can share diagnostics information.

The following subsections describe the device diagnostics options:

Configure Port Mirroring on a Switch Using the Insight App

Port mirroring lets you mirror the incoming (ingress) and outgoing (egress) traffic of one or more ports (the source ports) to a single predefined destination port. Port mirroring is useful if you want to analyze network traffic. Typically, you would send the traffic that is mirrored on the destination port to a network analyzer device.

To configure port mirroring on a switch using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch for which you want to configure port mirroring.
4. Scroll down and tap **Diagnostics**.
   The diagnostics options that are supported for the selected device display.
5. Tap **Port Mirroring**.
   The Port Mirroring page displays.
6. Tap the **Port Mirroring** button so that the button displays green and port mirroring is enabled.
   By default, port mirroring is disabled.
7. Select one or more source ports by tapping the ports.
8. Select the single destination port by tapping the port.
9. Tap **Apply**.
   Your settings are saved.
10. Tap **OK**.
    The diagnostics options display again.

Perform a Cable Test on a Switch Using the Insight App

You can perform a cable test to easily find out the health status of network cables. If any problems exist, this feature helps to quickly locate the point where the cabling fails, allowing connectivity issues to be fixed much faster, potentially saving technicians hours of troubleshooting.

If an error is detected, the distance at which the fault is detected is stated in meters. (This is the distance from the port.)

To perform a cable test on a switch using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the switch for which you want to perform a cable test.
4. Scroll down and tap **Diagnostics**.
   The diagnostics options display.
5. Tap **Cable Test**.
   The Cable Test page displays.
6. Select one or more ports by tapping the ports.
7. Tap **Test Selected Ports**.
   A warning displays.
8. Tap **OK**.
   The cable test starts. After a short period, the test results display.
9. Tap the arrow at the top of the page twice to return to the page that displays the diagnostics options.

Share Diagnostic Information From a Device Using the Insight App

You can let the Insight app collect diagnostic information from a device and send the information in a `.zip` file to one or more email addresses. If you encounter difficulties with your device, Technical Support might request the `.zip` file.

The `.zip` file includes the `Tech Support` file and the `Insight Log` file. Both of these files are `.txt` files.

To share diagnostic information from a device using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the device for which you want to share diagnostic information.
4. Scroll down and tap **Diagnostics**.
   The diagnostics options that are supported for the selected device display.
5. Tap **Share Diagnostics**.
   The Share Diagnostics page displays.

6. Enter an email address.
7. To enter another email address, tap **+** and enter the address.
8. Tap **Send**.
   The diagnostic information is sent to the email addresses.
9. Tap the arrow at the top of the page to return to the page that displays the diagnostics options.

Reload the Last Saved Cloud Configuration on a Device Using the Insight App

If communication problems occur between Insight and a device, reloading the last saved cloud configuration could resolve those problems.

You can reload the last saved cloud configuration for a device from your cloud account. During this process, the device goes offline for several minutes while the configuration is erased, the last saved cloud configuration is reloaded, and the device is rebooted for the changes to take effect.

To reload the last saved cloud configuration on a device through the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the device for which you want reload the last saved cloud configuration.
4. Scroll down and tap **Diagnostics**.
   By default, Ports is selected. The diagnostics options that are supported for the selected device display.
5. Tap **Reload Configuration**.
   The Reload Configuration page displays.
6. Tap **Reload**.
   A notification displays. The configuration is reloaded and the device is offline for a few minutes.
7. Tap **OK**.
   The diagnostic options display again.

Troubleshoot Connectivity Problems Between Your Device and Insight

If connectivity problems occur and you cannot get a connection between your device and the Insight app, start with the following general troubleshooting steps:

1. Make sure that the device is powered on.
   This is relevant because, for example, a ReadyNAS storage device can be powered off through a schedule.
2. Make sure that the cable connections between your device and your network are good.
3. Make sure that your device is connected to the Internet and that the Internet connection is good.

4. Make sure that the LEDs on your device do not indicate a problem.
5. For devices that support a Cloud LED, make sure that the Cloud LED indicates that the device is connected to the cloud.
6. Make sure that the device is functioning in the Insight management mode (which it is by default) and not in the local browser interface mode.
7. Make sure that the device is running the latest device firmware.

If the previous steps do not resolve the problem, see the following sections in the order suggested:

1. *Check to See If the Insight App Can Recognize Your Device* on page 112
2. *Reboot Your Device Using the Insight App* on page 112
3. *Remove Your Device From the Network and Re-add It Using the Insight App* on page 113
4. *Reload the Last Saved Cloud Configuration on a Device Using the Insight App* on page 111
5. *Reset a Device to Factory Default Settings Using the Insight App* on page 114

For more troubleshooting help, see the hardware installation guide (HIG) for your switch or access point. You can download your product's HIG from your product's support page under Documentation.

Check to See If the Insight App Can Recognize Your Device

If the Insight app cannot communicate with your device, the Insight app might still recognize your device.

To check if the Insight app can recognize your device:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Find your device.
4. Determine the device status:

   - If your device does not display, the Insight app does not recognize your device.
   - If your device displays with a red icon, the Insight app recognizes your device but cannot communicate with it.
   - If your device displays with a green icon, the Insight app recognizes your device and can communicate with it.

Reboot Your Device Using the Insight App

You can resolve some communication problems between the Insight app and your device by rebooting your device.

To reboot your device using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.

3. Select the device that you want to reboot.
4. Scroll down to the bottom and tap **Reboot**.
   A warning displays.
5. Read the warning and tap **Continue**.
   A notification displays. The device reboots and is offline for a few minutes.
6. Tap **OK**.
   The device page displays again.

Remove Your Device From the Network and Re-add It Using the Insight App

You can resolve some communication problems between the Insight app and your device by removing your device from the network and re-adding it using the Insight app. (You do not physically remove the device form the network and re-add it.)

To remove your device from the network and re-add it using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the device that you want to remove.
4. Scroll down to the bottom and tap **Remove**.
   A warning displays.
5. Read the warning and tap **Remove**.
   The device is removed and the list of devices displays again. The device that you just removed is now listed as an unclaimed device.
6. Select the same device.
7. Tap **ADD DEVICE**.
8. Select the network location to which you want to add the device.
9. If you want to rename your device, in the **Device Name** field, enter a new name.
10. Tap **Next**.
    A warning displays.
11. Tap **Continue**.
    The device is added to the network.
12. Tap **Devices**.
    When the process of adding the device to the network is complete, the status of your device turns green in the Insight app and in the Cloud Portal. This process might take up to 20 minutes.

Reset a Device to Factory Default Settings Using the Insight App

If you cannot resolve communication problems between a device and Insight, reset the device to factory default settings to see if that resolves the problem.

To reset a device to factory default settings using the Insight app:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the device that you want to reset.
   To reset the device, you must first remove it from the network.
4. Scroll down to the bottom and tap **Remove**.
   A warning displays.
5. Read the warning and tap **Remove**.
   The device is removed and the list of devices displays again. The device that you just removed is now listed as an unclaimed device.
6. Locate the recessed reset or factory defaults button on device.
7. Insert a device such as a straightened paper clip into the opening.
8. Press the button for up to 30 seconds or until Power LED lights amber.
   The device resets to factory defaults settings and reboots.
9. After the reboot process is complete, select the same device in the Insight app.
10. Tap **ADD DEVICE**.
11. Select the network location to which you want to add the device.
12. If you want to rename your device, in the **Device Name** field, enter a new name.
13. Tap **Next**.
    A warning displays.
14. Tap **Continue**.
    The device is added to the network.
15. Tap **Devices**.
    When the process of adding the device to the network is complete, the status of your device turns green in the Insight app and in the Cloud Portal. This process might take up to 20 minutes.

Send Diagnostic Files From the Insight App to a NETGEAR Community Moderator

To help troubleshoot a problem, community moderators or NETGEAR employees might request diagnostic files from your Insight managed device. You can let the Insight app collect diagnostic information from an Insight managed device and send the information in a `.zip` file.

The `.zip` file includes the `Tech Support` file and the `Insight Log` file. Both of these files are `.txt` files.

Before you send the file, first create a thread on the *NETGEAR Community* or contribute to an existing thread that is relevant to your issue. Do not send files unless instructed to do so by a community moderator or a NETGEAR employee.

To send diagnostic files from the Insight app to a NETGEAR community moderator:

1. Launch the Insight app.
2. If the managed devices do not display, in the menu at the bottom, tap **Devices**.
3. Select the device for which you want to send diagnostic files.
4. Scroll down and tap **Diagnostics**.

   The diagnostics options that are supported for the selected device display.
5. Tap **Share Diagnostics**.

   The Share Diagnostics page displays.
6. Enter **L3_SME_CBU@netgear.com**.

   If the community moderator or NETGEAR employee gave you another email address, enter that email address instead.
7. Tap **Send**.

   The diagnostic information is sent to the email address.
8. Tap the arrow at the top of the page to return to the page that displays the diagnostics options.