NETGEAR®

User Manual

Insight Basic and Premium Mobile App and Cloud Portal

October 2018
202-11872-03

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

Support

Thank you for purchasing this NETGEAR product. You can visit https://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
202-11872-03	October 2018	Added the BR500 router to the section Supported Devices on page 18. Updated the section Lexicon of Insight Terms on page 19. Added the chapter Manage VPN Groups, VPN Users, and VPN Connections on page 146. Added the chapter Manage Individual Routers on page 151. Added sections to the chapter Monitor Insight Networks and Devices on page 197.
202-11872-02	July 2018	Restructured the manual, added sections for both new and existing features, and changed sections for existing features that were already documented in this manual.
202-11872-01	February 2018	First publication.

Contents

Chapter 1 Introduction to Insight Basic and Insight Premium

Overview....14
Network Location Provisioning Concepts....14
Insight Subscriptions....15
Insight Mobile App and Insight Cloud Portal....16
Insight Cloud Portal Dashboard....17
Insight and the Local Browser–Based Management Interface....17
Supported Devices....18
Lexicon of Insight Terms....19

Chapter 2 Get Started With Insight Basic or Insight Premium

Install the NETGEAR Insight Mobile App....24
Access the Insight Cloud Portal....24
Create an Insight Account....24
Create an Insight Account Using the Insight App....25
Create an Insight Account Using the Cloud Portal....26
Create an Insight Network Location....27
Create an Insight Network Location Using the Insight App....27
Create an Insight Network Location Using the Cloud Portal....28
Discover, Add, and Register Devices....29
Add a Device by Scanning Your Network With the Insight App....30
Add a Device by Scanning Its QR Code With the Insight App..30
Add a Device by Scanning Its Barcode With the Insight App...31
Add a Device by Entering Its Serial Number in the Insight App....31
Add a Device by Entering Its Serial Number Using the Cloud Portal....32
Access Your Network and Devices Remotely....32
Access Your Network and Devices Remotely Using the Insight App....33
Access Your Network and Devices Remotely Using the Cloud Portal....33
Interpret the Green, Red, Orange, and Gray Circles Next to a Device....34
View and Manage Insight Notifications....34

View, Share, or Delete Notifications Using the Insight App.....35
View, Share, or Delete Your Notifications in the Cloud Portal..36
Manage the Insight Notifications That You Receive Using the Insight App.....38
Manage the Insight Notifications That You Receive Using the Cloud Portal.....39
Set Up Two-Step Verification for Logging In to Insight.....40
Set Up Two-Step Verification for Logging In Using the Insight App.....40
Set Up Two-Step Verification for Logging In Using the Cloud Portal.....42

Chapter 3 Maintain Your Insight Managed Devices and Network Locations

Overview of Features That Apply to an Entire Network Location.45
Display and Update Device Firmware.....45
Display and Update Device Firmware Using the Insight App...45
Display and Update Device Firmware Using the Cloud Portal.46
Reboot a Device Remotely.....48
Reboot a Device From the Insight App.....48
Reboot a Device From the Cloud Portal.....48
Reload the Last Saved Configuration on an Insight Managed Device.....49
Reload the Configuration on a Device Using the Insight App..49
Reload the Configuration on an Insight Managed Switch Using the Cloud Portal.....50
Reset an Insight Managed Device to Factory Default Settings.....50
Reset a Device That You Manage in the Insight App to Factory Default Settings.....51
Reset an Insight Managed Access Point to Factory Default Settings Using the Cloud Portal.....52
Remove a Device From Your Insight Account.....53
Remove a Device From Your Insight Account Using the Insight App.....53
Remove a Device From Your Insight Account Using the Cloud Portal.....54
Display or Change the Device Admin Password for a Network Location.....55
Display or Change the Device Admin Password for a Network Location Using the Insight App.....55
Display or Change the Device Admin Password for a Network Location Using the Cloud Portal.....56
Change the Network Location Information.....56

Change the Network Location Information Using the Insight App....56
Change the Network Location Information Using the Cloud Portal....57
Manage 802.1x Network Access Authentication With RADIUS Servers....58
Set Up RADIUS Servers for a Network Location Using the Insight App....58
Set Up RADIUS Servers for a Network Location Using the Cloud Portal....59
Manage Static Routes for a Network Location....59
Add a Static Route for a Network Location Using the Insight App....60
Add a Static Route for a Network Location Using the Cloud Portal....61
Change the Default Route for a Network Location Using the Insight App....62
Change the Default Route for a Network Location Using the Cloud Portal....62
Manage the Firmware Policy and Schedule Device Firmware Updates for a Network Location....63
Schedule Device Firmware Updates Using the Insight App....64
Schedule Device Firmware Updates Using the Cloud Portal....66

Chapter 4 Manage VLANs and VLAN-Based Features for a Location

VLAN Concepts....69
Plan the VLANs in Your Insight Network....69
VLAN Membership and Tagging....70
Management VLAN Concepts....71
How a VLAN Works on an Insight Managed Switch....72
Create a Custom VLAN....72
Create a Custom VLAN Using the Insight App....72
Create a Custom VLAN Using the Cloud Portal....76
Create a VoIP VLAN....79
Create a Voice VLAN Using the Insight App....80
Create a Voice VLAN Using the Cloud Portal....83
Configure the Default Auto-Video VLAN....87
Configure the Default Auto-Video VLAN Using the Insight App....87
Configure the Default Auto-Video VLAN Using the Cloud Portal....90
Configure VLAN-Based Quality of Service on a Switch....93
Configure VLAN-Based Quality of Service on a Switch Using the Insight App....94

Configure VLAN-Based Quality of Service on a Switch Using the Cloud Portal....94
Configure Port VLAN IDs for Switch Ports....95
Configure the Port VLAN ID Using the Insight App....96
Configure the Port VLAN ID for One or More Ports on the Same Switch Using the Cloud Portal....96
Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal....98

Chapter 5 Manage the Wired Network for a Location

Overview of Features That Apply to a Wired Network, Switches, and Switch Ports....100
Configure Groups of Ports on Different Switches in the Same Network....101
Enable or Disable a Group of Ports on Different Switches Using the Cloud Portal....101
Set the Storm Rate Limit for Incoming Traffic for a Group of Ports on Different Switches Using the Cloud Portal....102
Set the Bandwidth Limit for Outgoing Traffic for a Group of Ports on Different Switches Using the Cloud Portal....103
Set the Duplex Mode for a Group of Ports on Different Switches Using the Cloud Portal....104
Set the Maximum Ethernet Frame Size for a Group of Ports on Different Switches Using the Cloud Portal....105
Set the Speed for a Group of Ports on Different Switches Using the Cloud Portal....105
Set Up Link Aggregation Between Two Network Devices....106
Set Up Link Aggregation Between Two Devices Using the Insight App....107
Set Up Link Aggregation Between Two Devices Using the Cloud Portal....108
Configure Spanning Tree....110
Configure Spanning Tree Using the Insight App....110
Configure Spanning Tree Using the Cloud Portal....111
Create a PoE Schedule....112
Create a PoE Schedule Using the Insight App....112
Create a PoE Schedule Using the Cloud Portal....113

Chapter 6 Manage the WiFi Network and SSIDs for a Location

Overview of Features That Apply to a WiFi Network, SSIDs, and Access Points....116
Add an SSID to a Location....116
Add an SSID to a Location Using the Insight App....117
Add an SSID to a Location Using the Cloud Portal....119

Manage the Settings and Security for an Existing SSID at a Location....121
Manage the Settings and Security for an Existing SSID Using the Insight App....121
Manage the Settings and Security for an Existing SSID Using the Cloud Portal....123
Set Up a MAC ACL for an Existing SSID....125
Set Up a MAC ACL for an Existing SSID Using the Insight App.126
Set Up a MAC ACL for an Existing SSID Using the Cloud Portal....128
Create a Captive Portal for an Existing SSID....130
Create a Captive Portal for an Existing SSID Using the Insight App....130
Create a Captive Portal for an Existing SSID Using the Cloud Portal....132
Configure Rate Limits for an Existing SSID....134
Configure Rate Limits for an Existing SSID Using the Insight App....134
Configure Rate Limits for an Existing SSID Using the Cloud Portal....135
Set Up URL Filtering for All WiFi Clients at a Location....136
Set Up URL Filtering for All WiFi Clients Using the Insight App.136
Set Up URL Filtering for All WiFi Clients Using the Cloud Portal....137
Configure Automatic Radio Resource Management and Optimize the Radios at a Location....138
Configure Automatic Radio Resource Management and Optimize the Radios Using the Insight App....138
Configure Automatic Radio Resource Management and Optimize the Radios Using the Cloud Portal....139
Configure Fast Roaming for a WiFi Network....140
Configure Fast Roaming for a WiFi Network Using the Insight App....141
Configure Fast Roaming for a WiFi Network Using the Cloud Portal....141
Register and Configure Facebook Wi-Fi for a WiFi Network....142
Register and Configure Facebook Wi-Fi for a WiFi Network Using the Insight App....142
Register and Configure Facebook Wi-Fi for a WiFi Network Using the Cloud Portal....144

Chapter 7 Manage VPN Groups, VPN Users, and VPN Connections

Manage VPN Groups for a Router....147
Create a VPN Group Using the Insight App....147

Create a VPN Group Using the Cloud Portal.....147
Manage VPN Users for a Router.....148
Invite Someone to a VPN Group Using the Insight App.....148
Invite Someone to a VPN Group Using the Cloud Portal.....148
Manage Devices in a VPN Group on a Router.....149
Add a Device to a VPN Group Using the Insight App.....149
Add a Device to a VPN Group Using the Cloud Portal.....150
Download and Install the NETGEAR Insight VPN Application....150

Chapter 8 Manage Individual Routers

Specify a Static WAN IP Address for a Router.....152
Change a Router's WAN IP Address Using the Insight App...152
Change a Router's WAN IP Address Using the Cloud Portal..152
Manage One or More DHCP Servers of a Router.....153
Change or Disable Your Router's DHCP Server Using the Insight App.....153
Change or Disable A Router's DHCP Server Using the Cloud Portal.....153
Manage the Router Settings.....154
Manage Individual Routers Using the Insight App.....154
Manage Individual Routers Using the Cloud Portal.....154

Chapter 9 Manage Individual Switches

Configure Switch Ports.....157
Enable or Disable One or More Ports.....157
Enable or Disable One or More Ports Using the Insight App.....158
Enable or Disable One or More Ports on the Same Switch Using the Cloud Portal.....158
Set the Storm Rate Limit for Incoming Traffic for One or More Ports.....159
Set the Storm Rate Limit for Incoming Traffic for One or More Ports Using the Insight App.....160
Set the Storm Rate Limit for Incoming Traffic for One or More Ports on the Same Switch Using the Cloud Portal.....160
Set the Bandwidth Limit for Outgoing Traffic for One or More Ports.....162
Set the Bandwidth Limit for Outgoing Traffic for One or More Ports Using the Insight App.....162
Set the Bandwidth Limit for Outgoing Traffic for One or More Ports on the Same Switch Using the Cloud Portal.....162
Set the Duplex Mode for One or More Ports.....164
Set the Duplex Mode for One or More Ports Using the Insight App.....164

Set the Duplex Mode for One or More Ports on the Same Switch Using the Cloud Portal....165
Set the Maximum Ethernet Frame Size for One or More Ports.166
Set the Maximum Ethernet Frame Size for One or More Ports Using the Insight App....166
Set the Maximum Ethernet Frame Size for One or More Ports on the Same Switch Using the Cloud Portal....167
Set the Speed for One or More Ports....168
Set the Speed for One or More Ports Using the Insight App....168
Set the Speed for One or More Ports on the Same Switch Using the Cloud Portal....169
Manage Power over Ethernet....170
Enable or Disable PoE for One or More PoE-Capable Ports..171
Enable or Disable PoE for One or More Ports on a Switch Using the Insight App....171
Enable or Disable PoE for One or More Ports on a Switch Using the Cloud Portal....171
Power-Cycle One or More PoE Ports on a Switch....173
Power-Cycle One or More PoE Ports on a Switch Using the Insight App....173
Power-Cycle One or More PoE Ports on a Switch Using the Cloud Portal....173
Manage Custom PoE Settings for One or More Ports on a Switch....174
Manage Custom PoE Settings for One or More Ports on a Switch Using the Insight App....176
Manage Custom PoE Settings for One or More Ports on a Switch Using the Cloud Portal....178
Assign a PoE Schedule to One or More Ports on a Switch.....180
Assign a PoE Schedule to One or More Ports on a Switch Using the Insight App....181
Assign a PoE Schedule to One or More Ports on a Switch Using the Cloud Portal....181
Specify a Static IP Address for a Switch....182
Specify a Static IP Address for a Switch Using the Insight App.183
Specify a Static IP Address for a Switch Using the Cloud Portal....183

Chapter 10 Manage Individual Access Points

Manage the Channels and Output Power for an Access Point Manually....186
Manage the Channels and Output Power for an Access Point Manually Using the Insight App....186

Manage the Channels and Output Power for an Access Point Manually Using the Cloud Portal....187
Specify a Static IP Address for an Access Point....188
Specify a Static IP Address for an Access Point Using the Insight App....188
Specify a Static IP Address for an Access Point Using the Cloud Portal....189

Chapter 11 Manage Individual ReadyNAS Storage Systems

ReadyNAS Storage System Requirements for Insight....192
Ethernet Ports eth0 and eth1 on a ReadyNAS Storage System..192
Specify a Static IP Address for a ReadyNAS Storage System....193
Specify a Static IP Address for a ReadyNAS Storage System Using the Insight App....193
Specify a Static IP Address for a ReadyNAS Storage System Using the Cloud Portal....194
Enable Secure Diagnostics Mode on a ReadyNAS Storage System....195
Enable Secure Diagnostics Mode on a ReadyNAS Storage System Using the Insight App....195
Enable Secure Diagnostics Mode on a ReadyNAS Storage System Using the Cloud Portal....195

Chapter 12 Monitor Insight Networks and Devices

Overview of the Monitoring Options for a Network Location in the Cloud Portal....198
Customize Widgets in the Cloud Portal....200
Monitor All Network Locations Using the Cloud Portal....200
Display All Devices at All Network Locations Using the Cloud Portal....201
Monitor All Devices at a Single Network Location Using the Cloud Portal....202
Monitor a Single Network Location Using the Cloud Portal....203
Monitor the Wired Network at a Location Using the Cloud Portal.204
Monitor the WiFi Network and SSIDs at a Location Using the Cloud Portal....205
Monitor the Storage Network at a Location Using the Cloud Portal....206
Monitor an Individual Switch and Individual Ports Using the Cloud Portal....207
Monitor an Individual Access Point and Its Clients Using the Cloud Portal....208
Monitor an Individual ReadyNAS Storage System Using the Cloud Portal....209

Monitor the Clients at a Network Location Using the Cloud Portal....210
Monitor the Clients at a Network Location Using the Insight App.211
Monitor the Clients Connected to a Router Using the Cloud Portal....211
Monitor the Clients Connected to a Router Using the Insight App....212
Monitor VPN Groups in the Cloud Portal....212
Monitor the VPN Groups on a Router Using the Insight App....213
Monitor VPN Users With the Cloud Portal....213

Chapter 13 Perform Diagnostics and Troubleshooting

Use the Device Diagnostic Options in Insight....215
Configure Port Mirroring on a Switch....215
Configure Port Mirroring on a Switch Using the Insight App....215
Configure Port Mirroring on a Switch Using the Cloud Portal....216
Perform a Cable Test on a Switch....216
Perform a Cable Test on a Switch Using the Insight App...217
Perform a Cable Test on a Switch Using the Cloud Portal..217
Share Diagnostic Information From a Device....218
Share Diagnostic Information From a Device Using the Insight App....218
Share Diagnostic Information From a Device Using the Cloud Portal....219
Reload the Last Saved Cloud Configuration on a Device....219
Reload the Last Saved Cloud Configuration on a Device Using the Insight App....220
Reload the Last Saved Cloud Configuration on a Switch Using the Cloud Portal....220
Register New Products That Are Not Manageable in Insight....221
Register a Product Using the Insight App....221
Register a Product Using the Cloud Portal....222
Troubleshoot Connectivity Problems Between Your Device and Insight....222
Check to See If the Insight App Can Recognize Your Device....223
Reboot Your Device Using the Insight App....224
Remove Your Device From the Network and Re-add It Using the Insight App....224
Reset a Device to Factory Default Settings Using the Insight App.225
Send Diagnostic Files From the Insight App to a NETGEAR Community Moderator....226
View Your Product Support Information Using the Insight App.227

Open a Technical Support Case For a Product Using the Insight App.....228

1

Introduction to Insight Basic and Insight Premium

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
- Network Location Provisioning Concepts
- Insight Subscriptions
- Insight Mobile App and Insight Cloud Portal
- Insight Cloud Portal Dashboard
- Insight and the Local Browser–Based Management Interface
- Supported Devices
- Lexicon of Insight Terms

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 applications

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 Subscriptions

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 subscriptions: Insight Basic and Insight Premium. Both subscriptions 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)

The subscriptions 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 subscriptions.
  - 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.

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 Subscriptions on page 15), 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.
  - Four different ways to add a device to a network location, including scanning your network, scanning the device QR code, scanning the device barcode, and entering the device serial number.
  - Secure remote access.
  - Instant alerts for critical events.
  - Access to logs and traffic history.
  - Self-help and click-to-connect support portal.

- **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.
  - 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 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.

Note the following about changing the management mode:

- **Access points**. If you configure an access point through the local browser interface and then enable the Insight management mode, or the other way around, the settings are reset to their factory default settings with some exceptions:
  - **Change to local browser interface mode**. The Insight management mode becomes disabled and all settings except for the access point IP address and access point name are reset to their factory default settings.
  - **Change to Insight management mode**. The local browser interface does not become disabled but all settings except for the access point IP address and access point name are reset to their factory default settings. Access point settings that are Insight-manageable are masked out in the local browser interface. However, you can use the local browser interface to change access point settings that are not Insight-manageable.

- **Switches**. If you configure a switch through the local browser interface and then enable the Insight management mode, or the other way around, the settings are *not* reset to their factory default settings:
  - **Change to local browser interface mode**. The Insight management mode becomes disabled and the current Insight-manageable switch settings are saved to the cloud server. Any changes that you make using the local browser interface (including changing the switch password) are not saved to the cloud server.
  - **Change to Insight management mode**. If you added the switch to an Insight network location before, all Insight-manageable switch settings are returned to the last configuration saved on the cloud server, including the switch password (that is, the password is reset to the Insight network location password). However, switch settings that are not Insight-manageable and that you changed using the local browser interface are not reset.

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.

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, including models GC110, GC110P, GC510P, GC510PP, GC728X, GC728XP, GC752X, and GC752XP	X	X	X	X	X
Insight Managed Access Points, including models WAC505 and WAC510	X	X	X	X	X
Insight Managed Routers, including model BR500		X	X	X	X

Table 1. Insight supported devices (Continued)

Product Line or Devices	Available Actions				
	Set Up	Manage	Monitor	Discover	Register
ReadyNAS 300, 400, 500, 600, 700, 2000, 3000, and 4000 series storage systems		X	X	X	X
Orbi Pro WiFi systems, including model SRK60			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
WAC 100 and 700 series access points				X	X
Unmanaged switches					X

Note: If a device can be managed in Insight, then it counts towards your total devices on your Insight subscription. 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.

Lexicon of Insight Terms

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

- **Account holder**. The individual or small business owner (SBO) that initiates and owns the Insight account and the NETGEAR devices that are used in an Insight managed network.
- **Client**. An Ethernet (wired) or WiFi client of a network at a location.
- **Client-to-gateway VPN connection**. Virtual private network (VPN) access in which a remote VPN user accesses a protected network. The device of the remote user is the VPN client, and the router is the VPN gateway. This type of VPN connection is also referred to as a remote VPN connection.
- **Device**. See Managed device.
- **Device credit**. The unit that lets you add a single Insight managed device to a network location. A purchase confirmation key defines the number of available device credits

and the expiration date of those device credits. NETGEAR does not require you to spend device credits for non-Insight managed devices, even though Insight can discover, register, and, in some cases, even perform basic monitoring of such devices.

- **Device entitlement**. The NETGEAR support and warranty entitlements for a device.
- **Insight**. NETGEAR Insight is the cloud-based network and device management platform.
- **Insight Basic**. A free Insight account that lets you manage and monitor a maximum of two Insight devices using the NETGEAR Insight mobile app only. Insight Basic excludes premium features such as Smart WiFi roaming and PoE scheduling.
- **Insight Premium**. An Insight account that requires a subscription fee for each managed Insight device and that grants access to both the NETGEAR Insight mobile app and the Insight Cloud Portal. Insight Premium includes premium features such as Smart WiFi roaming and PoE scheduling.
- **Insight Cloud Portal**. The Insight Cloud Portal (or abbreviated as the Cloud Portal), is the website that provides access to the Insight cloud-based management platform. The Cloud Portal is available to Insight Premium subscribers.
- **Insight mobile app**. The NETGEAR Insight mobile app (or abbreviated as the Insight app or the mobile app) is the application for Android and iOS smartphones. The Insight app provides access to the Insight cloud-based management platform. The Insight app is available to all subscribers, including Insight Basic subscribers.
- **Insight payment**. Credit card payment to NETGEAR for an online or in-app purchase of device credits.
- **Insight Pro**. Insight Pro is the cloud-based management, multi-tenant management platform for managed service providers (MSPs), value-added resellers (VARs), and other types of businesses.
- **Insight VPN application**. An application that a VPN user must install on a computer or smartphone so that the user can initiate a VPN connection from that computer or smartphone to a VPN device at the Insight network location.
- **LAG**. Link aggregation group, which is two or more Ethernet links grouped into a single logical link between two network devices, allowing for an increase in throughput, fault tolerance, or both. 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.
- **Managed device**. A device such as a router, switch, access point, or ReadyNAS storage system that is managed by Insight and that requires one device credit.
- **Network location**. Also referred to as a network or a location. A network location is a subaccount of a single Insight account and is the physical site where the NETGEAR devices reside. Therefore, a network location includes a wired network, WiFi network

with SSIDs, storage network, or a combination of these three components. An Insight account can support multiple network locations.

- **PoE**. Power over Ethernet, which allows a device that is PoE-capable to receive power over the Ethernet cable from a switch that is also PoE-capable.
- **Provisioning**. The process of installing and configuring devices and the associated wired network, WiFi network, and storage system for one particular network location.
- **PVID**. A port VLAN ID, which is the VLAN ID that is assigned to the port. 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.
- **RADIUS**. Remote Authentication Dial-In User Service, which is a protocol that allows authentication and accounting for WPA2 Enterprise WiFi security and MAC access control lists (ACLs), both of which are supported on Insight Managed access points.
- **Remote client VPN connection**. See Client-to-gateway VPN connection and see VPN user.
- **Site-to-site VPN connection**. VPN access with two routers, each at a different site, which lets you connect two local LANs and separate networks together as if they were physically connected and colocated.
- **SSID**. Service set identifier, which is the WiFi network name. When you add a new SSID to a network location, you are not only creating a WiFi network name but are actually defining the settings for a new virtual access point (VAP). An SSID that you create on one access point at a location is deployed on all access points at that location.
- **Storage network**. A storage network that consist of at least one ReadyNAS storage device at one network location.
- **Subscription**. An Insight Premium account requires a subscription that defines the number of available device credits and the expiration date of those device credits. You can add device credits and extend the expiration date of device credits.
- **Uplink**. For a switch, the Ethernet connection to the router or modem that provides the Internet connection. For an access point or ReadyNAS storage system, to the Ethernet connection to the wired network.
- **VLAN**. A virtual LAN (VLAN), which is a local area network (LAN) 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.
- **VPN connection**. A VPN connection, which is an encrypted, secure tunnel between a remote VPN client and a VPN device at a site or between two VPN devices at different sites.

- **VPN client**. A computer or smartphone on which the Insight VPN application is installed, allowing the client to connect to a VPN device at the Insight network location. See also VPN user.
- **VPN device**. A VPN device such as a NETGEAR Insight Instant VPN router BR500.
- **VPN group**. A collection of VPN routers that can all communicate with each other. A group with up to three VPN routers allows for a complete meshed network between three locations. A VPN group with a single VPN router supports 10 remote users. Each additional VPN router supports another 10 remote users.
- **VPN user**. A remote user who is added to an Insight network location and who installed the Insight VPN application on a computer or smartphone. A VPN user can initiate a VPN connection from that computer or smartphone to a VPN device at the Insight network location.
- **Wired network**. An Ethernet network that consists of at least one switch at one network location with distinct features such as VLANs, spanning tree, and PoE schedules that apply to the entire wired network. (Other switch features apply to individual switches only or to individual switch ports only.)
- **Wireless network**. A collection of SSIDs at one network location with distinct features such as URL filtering, Auto RRM, Fast Roaming, and Facebook Wi-Fi that apply to the entire WiFi network. (Other WiFi features apply to individual SSIDs only or to individual access points only.) An SSID that you create on one access point at a location is deployed on all access points at that location.

2

Get Started With Insight Basic or Insight Premium

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:

- Install the NETGEAR Insight Mobile App
- Access the Insight Cloud Portal
- Create an Insight Account
- Create an Insight Network Location
- Discover, Add, and Register Devices
- Access Your Network and Devices Remotely
- Interpret the Green, Red, Orange, and Gray Circles Next to a Device
- View and Manage Insight Notifications
- Set Up Two-Step Verification for Logging In to Insight

Install the NETGEAR Insight Mobile App

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

To install the Insight mobile 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 26.
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 27
- Discover, Add, and Register Devices on page 29

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.
7. Click the **NETGEAR Sign-Up** button.
   A confirmation page displays. A verification email is sent to the email address that you used to set up your Insight account. 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 27
    - Discover, Add, and Register Devices on page 29

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 29.

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. At the top right of the page, click the **+** (Add Network) button.
   The Setup a New Network Location pop-up window opens.
4. In the **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. Enter the zip code for your location.
8. Select the country and time zone for your new network location.
9. To upload an image for your new network location, click the **Choose a file** button, locate the image, and upload it.
10. 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 29.

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 25 or Create an Insight Account Using the Cloud Portal on page 26.
2. Create an Insight network location.
   For more information, see Create an Insight Network Location Using the Insight App on page 27 or Create an Insight Network Location Using the Cloud Portal on page 28.

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
- Add a Device by Scanning Its QR Code With the Insight App
- Add a Device by Scanning Its Barcode With the Insight App
- Add a Device by Entering Its Serial Number in the Insight App
- Add a Device by Entering Its Serial Number Using 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 the **Go** button.

   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 18) 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 29).

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 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, Share, or Delete Notifications Using the Insight App

To view, share, or delete notifications using the Insight app:

1. Launch the Insight app.
2. Tap **Notifications** in the lower right corner of the page.
3. To filter notifications by device, severity, or time received, do the following:
   a. Tap **...** in the upper right corner of the page and tap **Filter**.
   b. Tap each category of notifications (**Device**, **Severity**, and **Time**) to view or hide notifications in that category.
   c. In each category, clear the check box for the type of notifications that you do not want to view.
   d. Tap **Apply**.
4. To share all notifications by email, do the following:
   a. Tap **...** in the upper right corner of the page and tap **Share**.
   b. Enter an email address.
   c. To enter more email addresses, tap **+**.
   d. Tap **Send**.
5. To delete notifications, do the following:
   - To delete a single notification, do the following:
     a. Tap and hold the notification and move it to the left.
     b. Tap the red **trash can** icon.
   - To delete all notifications, do the following:
     a. Tap **...** in the upper right corner of the page and tap **Delete All**.
     b. Confirm your decision by tapping **Delete All** again.

View, Share, 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 **bell** (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. To filter notifications, do the following:
   a. Click the **Filter** icon.
      A pop-up window opens.
   b. 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.
   c. Click the **Apply** button.
      The notifications are filtered.
5. To share notifications by email, do the following:
   - To share a single notification, do the following:
     a. Point to the notification.
     b. Click the **mail tray** icon that displays on the right.
        The Share Notifications pop-up window opens.
     c. Enter an email address.
     d. To enter more email addresses, click the **+** button.
     e. Click the **Send** button.
        The notification is sent.
   - To share several notifications, do the following:
     a. Click the **check box and pencil** icon.
     b. Select the check boxes for the notifications that you want to share.
     c. Click the **Share** button.

The Share Notifications pop-up window opens.

d. Enter an email address.

e. To enter more email addresses, click the **+** button.

f. Click the **Send** button.
The selected notifications are sent.

- To share all notifications, do the following:
  a. Click the **check box and pencil** icon.
  b. Select the check box in the table heading.
  c. Click the **Share** button.
  The Share Notifications pop-up window opens.
  d. Enter an email address.
  e. To enter more email addresses, click the **+** button.
  f. Click the **Send** button.
  All notifications are sent.

6. To delete notifications, do the following:
   - To delete a single notification, do the following:
     a. Point to the notification.
     b. Click the red **x** that displays on the right.
     The notification is deleted.
   - To delete several notifications, do the following:
     a. Click the **check box and pencil** icon.
     b. Select the check boxes for the notifications that you want to delete.
     c. Click the **Delete** button.
     The selected notifications are deleted.
   - To delete all notifications, do the following:
     a. Click the **check box and pencil** icon.
     b. Select the check box in the table heading.
     c. Click the **Delete** button.
     All notifications are deleted.

Manage the Insight Notifications That You Receive Using the Insight App

You can manage the push and email notifications that you receive.

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 the Insight Notifications That You Receive 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 menu opens.
3. Select **Account Management**.
   The Manage Notifications page displays.

   By default, the push notification settings display and the push notifications are enabled (the **Push Notifications** button displays green).
4. To edit smartphone or tablet push notification settings, do the following:
   a. To turn off all 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.
5. 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 all 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.

Set Up Two-Step Verification for Logging In to Insight

With two-step verification, you log in to the Insight app or Cloud Portal with an extra verification step. That is, you not only must enter your password, you must also enter a login verification code that you receive as an SMS message on the phone number that you must specify as the primary number, or as an email message at your account email address. For easier verification without the requirement to enter a login verification code after initial verification, you can set up push notifications to a trusted device.

Note the following security measures:

- **Primary number**. If you set up a primary phone number, you receive an SMS text message with a login verification code when you or someone else tries to log in to your account from another phone number. A one-time password (OTP) is sent to the primary phone number so that you can approve the login attempt, for example, by forwarding the OTP to the other phone number.
- **Trusted device**. A trusted device is a device that is already verified by Insight. If you set up a trusted device, you receive a push notification if you or someone else tries to log in to your account from a nontrusted device so that you can approve the login attempt.

You can set up two-step verification for logging in to Insight using the following methods:

- Set Up Two-Step Verification for Logging In Using the Insight App on page 40
- Set Up Two-Step Verification for Logging In Using the Cloud Portal on page 42

Set Up Two-Step Verification for Logging In Using the Insight App

Note: As another secure method of logging in, on devices that support touch ID, you can log in using the touch ID option of the Insight app so that you do not need to enter a user name and password. This option is displayed only on devices that support touch ID. To use touch ID login, you must first configure the fingerprint settings on your device.

When you set up two-step verification for logging in using the Insight app, the verification process applies to both the Insight app and the Cloud Portal.

To set up two-step verification for logging in 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 Profile > Login Settings > Two-Step Verification**.
4. Tap the **Enable** button so that the button displays purple.
   The Select verification method page displays. You can use both push notifications and SMS text messages, but you need to set up one method at a time.
   By default, the **Push Notifications** check box is selected.
5. To use push notifications, do the following
   a. Tap **CONTINUE**.
   b. To approve the device that you are using as a trusted device for push notifications, tap **APPROVE**.
   c. Name your device and tap **GOT IT**.
   Your device is added as a trusted device for push notifications. When you log into the Insight app or the Cloud Portal from the trusted device, you do not need to enter a security code because the verification process for the trusted device occurs in the background.
   d. To also add SMS text message verification, tap **ADD SMS VERIFICATION**, and follow the Step 6.c and Step 6.d.
6. To use SMS text message verification, do the following:
   a. Select the **SMS Text Message** check box.
   b. Tap **CONTINUE**.
   c. Select a country, enter a phone number, and tap **ADD PHONE NUMBER**.
   Insight sends an SMS text message with a one-time security pair code to the phone number. The Add SMS Verification page displays.
   d. Enter the security pair code that you received and tap **NEXT**.
   The phone number is verified and added to the page as the primary number for login verification. Now, each time that you log into the Insight app or the Cloud Portal, an SMS text message with a login verification code is sent to the phone number and you must enter the code during the login process.
   If the device that you use to log into the Insight app is the same device on which you received the code, the first time that you log in *after* you entered the code, you can add your device as a trusted device so that Insight automatically verifies your identity when you log in.

Note: During the Insight app login process, you either can let Insight send a login verification code to the primary phone number or you can tap **TRY ANOTHER VERIFICATION METHOD** and let Insight send a login verification code to your account email address.

7. To add another phone number, click the **ADD SMS VERIFCATION** button and repeat Step 6.c and Step 6.d.
8. To return to the Account Management page, click the left arrow button at the upper left of the page three times.

Set Up Two-Step Verification for Logging In Using the Cloud Portal

When you set up two-step verification for logging in using the Cloud Portal, the verification process applies to both the Cloud Portal and the Insight app.

To set up two-step verification for logging in 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 menu opens.
3. Select **Update Profile**.
   Your profile page displays.
4. Select **Login Settings > Two-Step Verification**.
   The Two-Step Verification page displays.
5. Click the **Enable** button.
   The Add SMS Verification page displays.
6. Select a country, enter a phone number (which must be capable of receiving SMS messages), and click the **ADD PHONE NUMBER** button.
   Insight sends a one-time security pair code to the phone number. The Add SMS Verification page displays.
7. Enter the security pair code that you received and click the **NEXT** button.
   The phone number is verified and added to the page as the primary number for login verification. Now, each time that you log into the Cloud Portal, a login verification code is sent to the phone number and you must enter the code during the login process.

Note: During the Cloud Portal login process, you either can let Insight send a login verification code to the phone number or you can click the **Try Another Verification Method** link and let Insight send a login verification code to your account email address.

8. To add another phone number, click the **ADD SMS VERIFCATION** button and repeat Step 6 and Step 7.
9. To return to the dashboard, click the left arrow button at the upper left of the page three times.

3

Maintain Your Insight Managed Devices and Network Locations

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

The chapter includes the following sections:

- Overview of Features That Apply to an Entire Network Location
- Display and Update Device Firmware
- Reboot a Device Remotely
- Reload the Last Saved Configuration on an Insight Managed Device
- Reset an Insight Managed Device to Factory Default Settings
- Remove a Device From Your Insight Account
- Display or Change the Device Admin Password for a Network Location
- Change the Network Location Information
- Manage 802.1x Network Access Authentication With RADIUS Servers
- Manage Static Routes for a Network Location
- Manage the Firmware Policy and Schedule Device Firmware Updates for a Network Location

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Overview of Features That Apply to an Entire Network Location

The following features apply to the *entire* network at a location, that is, to the wired network, WiFi network, and storage network and all associated devices at a single network location:

- VLANs, including VLAN IP filtering and VLAN MAC authentication (see Manage VLANs and VLAN-Based Features for a Location on page 68)
- Device admin password (see Display or Change the Device Admin Password for a Network Location on page 55)
- RADIUS servers (see Manage 802.1x Network Access Authentication With RADIUS Servers on page 58)
- Syslog configuration.
- LED settings.
- Static routes (see Manage Static Routes for a Network Location on page 59)
- Firmware policy (see Manage the Firmware Policy and Schedule Device Firmware Updates for a Network Location on page 63)

Display and 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.

You can also schedule automatic firmware updates for a network location (see Manage the Firmware Policy and Schedule Device Firmware Updates for a Network Location on page 63).

Display and 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. Do one of the following:

   - **Update the firmware for a single device for which an update is available**. To the right of the device for which you want to update the firmware, tap **Update**.
   - **Update the firmware for all devices for which updates are available**. At the top right of the page, tap **UPDATE ALL**.

   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.

Display and 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 or on all devices simultaneously. You cannot manually download a firmware version to the Cloud Portal and upload it to a device.

To update the firmware for one or all devices for which firmware updates are available 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 at the network location, 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.

   For information about scheduling firmware updates, see Schedule Device Firmware Updates Using the Cloud Portal on page 66.

4. Do one of the following:

   - **Update the firmware for a single device for which an update is available**. To the right of the device for which you want to update the firmware, click the **Update** icon.
   - **Update the firmware for all devices for which updates are available**. In the heading of the Updates Available table, click the **Update All Devices** link.

   The Update firmware pop-up window opens.

5. Read the warning, and click the **Yes, update the 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 or devices 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 or devices with the updated firmware versions.

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 52).

Note: For devices that are capable of being managed by Insight but that are no longer managed by Insight, any configuration changes that you saved through the local browser interface that occurred after the last saved configuration in the cloud are lost. Use the local browser interface to reapply these settings.

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 54.

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 29.

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 54).

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 30.

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 32.

   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 show 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.

Change the Network Location Information

You can change the information for an existing network location, such as the name, address, time zone, wireless region, and location image (logo). For information about changing the password, see Display or Change the Device Admin Password for a Network Location on page 55.

Change the Network Location Information Using the Insight App

You can change the information for an existing Insight network location using the Insight app.

To change the information for an Insight 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. Change the name of the location, address, time zone, wireless region, location image (logo), or a combination of these.
   For information about changing the password, see Display or Change the Device Admin Password for a Network Location on page 55.
6. Tap **Save**.

Change the Network Location Information Using the Cloud Portal

You can change the information for an existing Insight network location using the Cloud Portal.

To change the information for 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. 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. Change the name of the location, address, time zone, wireless region, location image (logo), or a combination of these.
   For information about changing the password, see Display or Change the Device Admin Password for a Network Location on page 55.
5. 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 set up a RADIUS server.
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 show 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 Static Routes for a Network Location

You can configure static routes for situations in which you use multiple routers and switches or multiple IP subnets for a network location.

As an example of when you need to set up a static route, consider the following case:

- The primary Internet access for a network location is through an ADSL modem to an ISP.

- An ISDN router at the network location must be able to connect to a company IP address. This router's address at the network location 192.168.1.100.
- The company's network address is 134.177.0.0.

When you first set up the router at the network location, two implicit static routes were created. A default route was created with the ISP as the gateway and a second static route was created to the local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, the router forwards the connection request to the ISP. In turn, the ISP forwards the connection request to the company, and the request is likely to be denied by the company's firewall.

In this case, you must define a static route, instructing the router that the 134.177.0.0 network is accessed through the ISDN router at 192.168.1.100. Here is an example:

- Through the destination IP address and IP subnet mask, specify that this static route applies to all 134.177.x.x addresses.
- Through the gateway IP address, specify that all traffic for these addresses is forwarded to the ISDN router at 192.168.1.100.
- A metric value of 1 works fine because the ISDN router is on the LAN.

Add a Static Route for a Network Location Using the Insight App

To add a static route 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 add a static route.
4. Tap **Edit Network**.
   The Edit Network page displays.
5. Tap **Routing** and then tap **Static Route**.
6. Tap the switch on which you want to specify the static route.
7. Tap **+** in the upper right corner of the page.
8. Enter the IP address, IP subnet mask, and nexthop IP address for the new route.
   Use standard IP address notation (four octets, each separated by a dot).
9. If you want to make the new route the default route, tap the **Default Route** button so that the button displays green.

Caution: Make sure that the new route is valid before you save it as the default route. A faulty default route causes connectivity problems in your network.

10. Tap **Save**.

Add a Static Route for a Network Location Using the Cloud Portal

To add a static route 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 show All Locations, click the network menu and select **See all locations**.
3. For the network location for which you want to add a static route, click the **...** button and select **Edit location** from the pop-up menu.
   The Network Location Settings page displays.
4. Select **Routing**.
   The routing VLANs display.
5. Click the **+** to the right of Static Route.
   The section expands.
6. Select the switch on which you want to specify the static route and click the **Next** button.
7. Click the **+ Add new** button.
8. Enter the IP address, IP subnet mask, and nexthop IP address for the new route.
   Use standard IP address notation (four octets, each separated by a dot).
9. If you want to make the new route the default route, click the **Default Route** button so that the button displays green.
   A warning pop-up window opens and informs you that the current default route will be deleted and replaced by the new default route.

   Caution: Make sure that the new route is valid before you save it as the default route. A faulty default route causes connectivity problems in your network.

10. Click the **Yes** button.
11. Click the **Save** button.

Your settings are saved.

Change the Default Route for a Network Location Using the Insight App

To change the default route 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 add a static route.
4. Tap **Edit Network**.
   The Edit Network page displays.
5. Tap **Routing** and then tap **Static Route**.
6. Tap the switch on which you want to change the default route.
7. Tap the route that you want to make the new default route.
8. Tap the **Default Route** button so that the button displays green.

   Caution: Make sure that the route is valid before you make it the default route. A faulty default route causes connectivity problems in your network.

9. Tap **Save**.

Change the Default Route for a Network Location Using the Cloud Portal

To change the default route 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 show All Locations, click the network menu and select **See all locations**.
3. For the network location for which you want to add a static route, click the **...** button and select **Edit location** from the pop-up menu.
   The Network Location Settings page displays.
4. Select **Routing**.

The routing VLANs display.

5. Click the **+** to the right of Static Route.
   The section expands.
6. Select the switch on which you want to specify the static route and click the **Next** button.
7. Point to the route that you want to make the new default route and click the **pencil** icon at the right of the page.
   The page that displays shows details about the route.
8. Click the **Default Route** button so that the button displays green.
   A warning pop-up window opens and informs you that the current default route will be deleted and replaced by the new default route.

   Caution: Make sure that the route is valid before you make it the default route. A faulty default route causes connectivity problems in your network.

9. Click the **Yes** button.
10. Click the **Save** button.
    Your settings are saved.

Manage the Firmware Policy and Schedule Device Firmware Updates for a Network Location

You can set the firmware policy for a network location by enabling automatic firmware updates for devices at the network location. You must schedule a period (the update window) during which updates are allowed to occur (for example, during a period when clients are minimally affected). As an option, you can specify a recurrence interval that can be in effect during the update window only.

Schedule Device Firmware Updates Using the Insight App

To schedule firmware updates for all devices at 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 your network.
4. Tap **Edit Network**.
   The Edit Network page displays.
5. Tap **Firmware Policy**.
   The **Auto Upgrade** button displays. By default, the button displays gray because automatic updates are disabled.
6. Tap the **Auto Update** button so that the button displays green.
   The update and recurrence fields display.
7. Next to Start, tap **Pick date & time** and do the following:
   a. Using the controls on the page, specify the start date and time of the update window during which automatic firmware updates are allowed.
   b. Tap **Done**.
8. Next to End, tap **Pick date & time** and do the following:
   a. Using the controls on the page, specify the end date and time of the update window during which automatic firmware updates are allowed.
   b. Tap **Done**.

   By default, recurrence is disabled. If you want to use recurrence, specify an update window that stretches over a longer period. The recurrence occurs only during the update window and only if firmware updates are available.
9. To allow recurrence, do the following:
   a. Tap the **Repeats** menu.
   b. Swipe up or down to select a frequency.

c. Tap **Done**.

d. Depending on the selected frequency, refine your selection by doing the following:

- **Daily**. If you selected **Daily**, updates are allowed daily during the update window. No other refinement is required.
- **Weekly**. If you selected **Weekly**, tap one or more buttons for the days of the week during which updates are allowed.
- **Monthly**. If you selected **Monthly**, select when the updates are allowed. The selection depends on the day on which you schedule and configure the firmware updates. For example, if today is June 18, you can select **Monthly on day 18** or **Monthly on third Monday**. However, if today, is June 19, you can select **Monthly on day 19** or **Monthly on third Tuesday**.

If firmware is available, updates occur during the time that you specified in Step 7 and Step 8.

10. Specify if recurrence ends by tapping one of the following radio buttons:

- **Never**. The recurrence does not end.
- **On**. Select a particular day on which recurrence must end. Do the following:
  a. Tap the date to open a calendar.
  b. Tap the day on which recurrence must end.
  c. Tap **Done**.
- **On recurrence**. Enter the number of recurrences after which recurrence must end. Do the following:
  a. Tap the number (by default, 1 for one recurrence).
  b. Select the number of recurrences.

When the update window that you specified in Step 7 and Step 8 expires, recurrence also ends.

11. Tap **Save**.

Schedule Device Firmware Updates Using the Cloud Portal

To schedule firmware updates for all devices at 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 **Firmware**.
   The Scheduled upgrade section displays at the top of the page.
4. Click the **Enable** button so that the button displays green.
   The date and time links and the **Repeats** menu display.
5. Using the date and time links, specify the update window during which automatic firmware updates are allowed.
   You must specify the start date and time and the end date and time.
   By default, recurrence is disabled. If you want to use recurrence, specify an update window that stretches over a longer period. The recurrence occurs only during the update window and only if firmware updates are available.
6. To allow recurrence, select a frequency from the **Repeats** menu:
   - **Daily**. Updates are allowed daily during the update window.
   - **Weekly**. Click one or more buttons for the days of the week during which updates are allowed.
   - **Monthly**. If you selected **Monthly**, select when the updates are allowed. The selection depends on the day on which you schedule and configure the firmware updates. For example, if today is June 18, you can select **Monthly on day 18** or **Monthly on third Monday**. However, if today, is June 19, you can select **Monthly on day 19** or **Monthly on third Tuesday**.

   If firmware is available, updates occur during the time that you specified in Step 5.
7. Specify if recurrence ends by selecting one of the following radio buttons:
   - **Never**. The recurrence does not end.
   - **On**. Click the date and select a particular day on which recurrence must end.
   - **On recurrence**. Enter the number of recurrences after which recurrence must end.

When the update window that you specified in Step 5expires, recurrence also ends.

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

4

Manage VLANs and VLAN-Based Features for a Location

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
- Plan the VLANs in Your Insight Network
- VLAN Membership and Tagging
- Management VLAN Concepts
- How a VLAN Works on an Insight Managed Switch
- Create a Custom VLAN
- Create a VoIP VLAN
- Configure the Default Auto-Video VLAN
- Configure VLAN-Based Quality of Service on a Switch
- Configure Port VLAN IDs for Switch Ports

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

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 95).

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 96.

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 96 or Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal on page 98.

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 95).

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 96.

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 96 or Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal on page 98.

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 95).

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 96.

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 96 or Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal on page 98.

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.

5

Manage the Wired Network for a Location

This chapter describes how you can manage features that are specific to Insight Managed wired networks at a location. A wired network and VLAN that you create for one location can be used by multiple devices at that location.

For information about VLANs, see Manage VLANs and VLAN-Based Features for a Location on page 68.

For imformation about features that are specific to a single switch at a location, see Manage Individual Switches on page 156.

The chapter includes the following sections:

- Overview of Features That Apply to a Wired Network, Switches, and Switch Ports
- Configure Groups of Ports on Different Switches in the Same Network
- Set Up Link Aggregation Between Two Network Devices
- Configure Spanning Tree
- Create a PoE Schedule

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Overview of Features That Apply to a Wired Network, Switches, and Switch Ports

In this manual, a wired network consists of a collection of routers and switches at one network location. The following list describes which features you can configure for which components:

- **Wired network**. The following features (which are described in this chapter) apply to the entire wired network at a network location:
  - Spanning tree and spanning tree mode (see Configure Spanning Tree on page 110)
  - PoE schedules (see Create a PoE Schedule on page 112)

  Note: Although you configure a VLAN on a switch, the VLAN applies to an entire network location because you can apply the VLAN also to an SSID of the WiFi network at the same location. For more information, see Manage VLANs and VLAN-Based Features for a Location on page 68.

  Note: A link aggregation group (LAG) applies to two network devices at a network (see Set Up Link Aggregation Between Two Network Devices on page 106).

- **Switch**. The following features apply to individual switches at a network location (see Manage Individual Switches on page 156):
  - IP settings (see Specify a Static IP Address for a Switch on page 182)
  - Port mirroring (see Configure Port Mirroring on a Switch on page 215)
  - Cable test (see Perform a Cable Test on a Switch on page 216)

- **Switch port**. The following features apply to individual switch ports (see Manage Individual Switches on page 156):
  - Enable or disable a port (see Enable or Disable One or More Ports on page 157)
  - PoE (see Manage Power over Ethernet on page 170)
  - Rate limits (see Set the Bandwidth Limit for Outgoing Traffic for One or More Ports Using the Insight App on page 162 and Set the Storm Rate Limit for Incoming Traffic for One or More Ports on page 159)
  - Default VLAN (PVID) (see Configure Port VLAN IDs for Switch Ports on page 95)
  - Duplex mode (see Set the Duplex Mode for One or More Ports on page 164)

- Maximum frame size (see Set the Maximum Ethernet Frame Size for One or More Ports on page 166)
- Port speed (see Set the Speed for One or More Ports on page 168)

Note: You can also simultaneously configure multiple switch ports in a network (see Configure Groups of Ports on Different Switches in the Same Network on page 101 and Configure the Port VLAN ID for a Group of Ports on Different Switches Using the Cloud Portal on page 98)

Configure Groups of Ports on Different Switches in the Same Network

You can simultaneously configure groups of ports on different switches in the same network.

For information about configuring individual switches, see Manage Individual Switches on page 156.

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 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 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 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 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 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.

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.

Configure Spanning Tree

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of switches and bridges in a network. STP also provides one path between end stations on a network, avoiding and eliminating loops and preventing network congestion. Insight supports STP and Rapid STP (RSTP).

RSTP can recognize full-duplex connectivity and ports that are connected to end stations, allowing for rapid transitioning of such ports to the forwarding state.

By default, both STP and RSTP are disabled. You can enable either STP or RSTP. You cannot configure any specific STP or RSTP settings.

You can configure spanning tree using the following methods:

- Configure Spanning Tree Using the Insight App on page 110
- Configure Spanning Tree Using the Cloud Portal on page 111

Configure Spanning Tree Using the Insight App

To configure Spanning Tree 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 configure Spanning Tree.
5. Tap **Spanning Tree (STP)**.
6. If the Spanning Tree settings do not display, tap the **Enable** button.
7. To select the Spanning Tree mode, do the following:
   a. Tap **Spanning Tree Mode**.
   b. Swipe up or down to select **STP** or **RSTP**.
   c. Tap **Done**.
8. For each switch for which you want to configure Spanning Tree, in the graphic of the switch, tap the ports, LAGs, or both to enable Spanning Tree for them.
   For each switch, tap **Select All** to select all ports on that switch. (After you tap **Select All**, the name changes to Deselect All.) Tap **Deselect All** for a switch to clear all selected ports on that switch.
9. Tap **Save**.
   Your settings are saved.

Configure Spanning Tree Using the Cloud Portal

To configure Spanning Tree 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 **Spanning Tree**.
   The Spanning Tree page displays.
6. Click the **Enable** button so that the button displays green.
   The Spanning Tree settings display.

7. From the **Spanning Tree Mode** menu, select **STP** or **RSTP**.
8. For each switch for which you want to configure Spanning Tree, in the graphic of the switch, select the ports, LAGs, or both to enable Spanning Tree for them.

   For each switch, click the **Select All** button to select all ports on that switch. (After you click the **Select All** button, the name of the button changes to Deselect All.) Click the **Deselect All** button for a switch to clear all selected ports on that switch.
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 181.
   - 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 181.
   - 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.

6

Manage the WiFi Network and SSIDs for a Location

This chapter describes how you can manage features that are specific to an Insight Managed WiFi network and its SSIDs (WiFi network names).

In this manual, a WiFi network is a collection of SSIDs at one network location. Some features apply to a WiFi network (all SSIDs at the network location), other features apply to individual SSIDs (see Overview of Features That Apply to a WiFi Network, SSIDs, and Access Points on page 116). An SSID that you create on one access point at a location is deployed on all access points at that location.

For information about features that are specific to a single access point at a location, see Manage Individual Access Points on page 185.

The chapter includes the following sections:

- Overview of Features That Apply to a WiFi Network, SSIDs, and Access Points
- Add an SSID to a Location
- Manage the Settings and Security for an Existing SSID at a Location
- Set Up a MAC ACL for an Existing SSID
- Create a Captive Portal for an Existing SSID
- Configure Rate Limits for an Existing SSID
- Set Up URL Filtering for All WiFi Clients at a Location
- Configure Automatic Radio Resource Management and Optimize the Radios at a Location
- Configure Fast Roaming for a WiFi Network
- Register and Configure Facebook Wi-Fi for a WiFi Network

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Overview of Features That Apply to a WiFi Network, SSIDs, and Access Points

In this manual, we refer to a WiFi network as a collection of SSIDs at one network location. The following list describes which features you can configure for which components:

- **WiFi network**. The following features (which are described in this chapter) apply to the entire WiFi network, that is, to the collective SSIDs at a network location:
  - URL filtering (see Set Up URL Filtering for All WiFi Clients at a Location on page 136)
  - Auto RRM (see Configure Automatic Radio Resource Management and Optimize the Radios at a Location on page 138)
  - Fast roaming (see Configure Fast Roaming for a WiFi Network on page 140)
  - Facebook Wi-Fi (see Register and Configure Facebook Wi-Fi for a WiFi Network on page 142)

- **SSID**. The following features (which are described in this chapter) apply to individual SSIDs at a network location:
  - MAC ACL (see Set Up a MAC ACL for an Existing SSID on page 125)
  - Captive portal (see Create a Captive Portal for an Existing SSID on page 130)
  - Rate limits (see Configure Rate Limits for an Existing SSID on page 134)

- **Access point**. The following features apply to individual access points at a network location (see Manage Individual Access Points on page 185):
  - IP settings (see Specify a Static IP Address for an Access Point on page 188)
  - Radio and channels (see Manage the Channels and Output Power for an Access Point Manually on page 186)

Add an SSID to a Location

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

Important: An SSID that you create on one access point at a network location is deployed on and broadcast by *all* access points at the network location. That is, even though you create the SSID on a single access point, the SSID is not specific to that single access point.

Add an SSID to a Location Using the Insight App

To add a new WiFi network (SSID) to a 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.
4. Tap **WiFi**.
5. Tap **Add New WiFi (SSID)**.
6. In the **SSID** field, enter the name for the SSID.

   Enter a name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

7. 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.

8. 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.

9. If you want to enable band steering, tap the **Band Steering** button so that the button displays green.

   If you enable band steering, the access points identify the WiFi devices that are dual-band capable and steer those devices to the 5 GHz band rather than the 2.4 GHz band of the VAP. Generally, more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience.

   By default, band steering is disabled and the **Band Steering** button displays white.

10. 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 58).

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.

11. If you select **WPA2-PSK** or **WPA/WPA2-PSK** security, tap **Password** and enter a password.

    Enter a password with a minimum length of 8 characters and a maximum length of 63 characters.

12. If you want to enable client isolation, in the ADVANCED SETTINGS section, tap the **Client Isolation** button so that the button displays green.

    If you enable client isolation, the access points block communication between WiFi clients that are associated with the same SSID or different SSIDs on the access points. This option can be useful for an open network, for example, for a hotspot at a public place.

    By default, client isolation is disabled and the **Client Isolation** button displays gray.

    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 for a Location on page 68) 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.

13. 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**.

14. Tap **Save**.

    Your settings are saved.

    The new SSID is created and broadcast by all access points at the location.

Add an SSID to a Location Using the Cloud Portal

To add a new WiFi network (SSID) to a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. At the top right of the page, click the **+** (**Add SSID**) button.
   The Add New SSID pop-up window opens.
6. In the **SSID** field, enter the name for the SSID.
   Enter a name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).
7. If you want to disable broadcasting, click the **Broadcast SSID** button so that the button displays gray.
   If you disable broadcast of the SSID, only users who know the name of your WiFi network can connect to it.
   By default, broadcasting is enabled and the **Broadcast SSID** button displays green.
8. If you want the SSID to broadcast on a single radio band only, select the radio band from the **Band** menu.
   By default, the SSID is broadcast on both radio bands.
9. If you want to enable band steering, click the **Band Steering** button so that the button displays green.
   If you enable band steering, the access points identify the WiFi devices that are dual-band capable and steer those devices to the 5 GHz band rather than the 2.4 GHz band of the VAP. Generally, more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience.
   By default, band steering is disabled and the **Band Steering** button displays gray.

10. If you want to use security other than the default WPA2-PSK security, select another type of security from the **Security** menu.

    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 Cloud Portal on page 59).

    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.

11. If you select **WPA2-PSK** or **WPA/WPA2-PSK** security, enter a password in the **Password** field.

    Enter a password with a minimum length of 8 characters and a maximum length of 63 characters.

12. If you want to enable client isolation, in the Advanced Settings section, click the **Client Isolation** button so that the button displays green.

    If you enable client isolation, the access points block communication between WiFi clients that are associated with the same SSID or different SSIDs on the access points. This option can be useful for an open network, for example, for a hotspot at a public place.

    By default, client isolation is disabled and the **Client Isolation** button displays gray.

    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 for a Location on page 68) 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.

13. To assign a VLAN other than the Management VLAN to the SSID, in the Advanced Settings section, select the VLAN from the **VLAN** menu.
14. Do one of the following:

    - Click the **Save** button. Your settings are saved. The new SSID is created and broadcast by all access points at the location.
    - Click the **Save and Configure** button. Your settings are saved, the new SSID is created and broadcast by all access points at the location, and the Settings page for the SSID displays. From the Settings page, you can access the MAC ACL page, Captive Portal page, and Rate Limit page to further configure the SSID.

Manage the Settings and Security for an Existing SSID at a Location

You can change the settings and security for an existing WiFi network (SSID) at a location. These settings include the following:

- Whether or not the SSID is enabled
- The name of the SSID
- Whether or not the SSID is broadcast
- The band or bands on which the SSID is enabled
- Whether band steering is enabled.
- The type of WiFi security, if any, and associated encryption
- Whether client isolation is enabled
- The VLAN on which the SSID enabled

Manage the Settings and Security for an Existing SSID Using the Insight App

To manage the settings and security for an existing SSID at a 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.
4. Tap **WiFi**.
5. Tap the SSID for which you want to manage the settings and security.
6. Enable or disable the SSID by tapping the **Enable** button.
   If the button displays green, the SSID is enabled. If the button displays gray, the SSID is disabled, in which case the settings for the SSID are not deleted but the SSID becomes inoperational.
7. To change the name for the SSID, in the **SSID** field, enter the new name for the SSID.

Enter a name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

8. Enable or disable broadcast of the SSID by tapping the **Broadcast SSID** button.

   If the button displays green, broadcast is enabled. If the button displays gray, broadcast is disabled, in which case only users who know the name of the SSID can connect to it.

9. If you want the SSID to broadcast on a single radio band, tap the radio band from the **Band** menu, or tap **Both** to enable the SSID to broadcast on both bands.
10. Enable or disable band steering by tapping the **Band Steering** button.

    If the button displays green, band steering is enabled. If the button displays gray, band steering is disabled.

    If you enable band steering, the access points identify the WiFi devices that are dual-band capable and steer those devices to the 5 GHz band rather than the 2.4 GHz band of the VAP. Generally, more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience.

11. Select the type of security from the **Security** menu:

    - **WPA2-PSK**. 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 mixed mode security. This type of security uses AES encryption.
    - **WPA/WPA2-PSK**. Mixed mode security allows both WPA and WPA2 WiFi clients to connect to the SSID. This type of security uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES.
    - **WPA2 ENTERPRISE**. 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 Cloud Portal on page 59).

    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.

12. If you select **WPA2-PSK** or **WPA/WPA2-PSK** security, tap **Password** and enter a password.

    Enter or change the password, which must consist of a minimum length of 8 characters and a maximum length of 63 characters.

13. Enable or disable client isolation by tapping the **Client Isolation** button in the ADVANCED SETTINGS section.

    If the button displays green, client isolation is enabled. If the button displays gray, client isolation is disabled.

    If you enable client isolation, the access points block communication between WiFi clients that are associated with the same SSID or different SSIDs on the access points. This option can be useful for an open network, for example, for a hotspot at a public place.

14. To assign another 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**.

    For information about setting up VLANs, see Manage VLANs and VLAN-Based Features for a Location on page 68.

15. Tap **Save**.
    Your settings are saved.

Manage the Settings and Security for an Existing SSID Using the Cloud Portal

To manage the settings and security for an existing SSID at a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. Point to the SSID and click the **pencil** icon at the right of the page.
   The Settings page for the SSID displays.

6. Enable or disable the SSID by clicking the **Enable SSID** button.

   If the button displays green, the SSID is enabled. If the button displays gray, the SSID is disabled, in which case the settings for the SSID are not deleted but the SSID becomes inoperational.

7. To change the name for the SSID, in the **SSID** field, enter the new name for the SSID.

   Enter a name with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

8. Enable or disable broadcast of the SSID by clicking the **Broadcast SSID** button.

   If the button displays green, broadcast is enabled. If the button displays gray, broadcast is disabled, in which case only users who know the name of the SSID can connect to it.

9. If you want the SSID to broadcast on a single radio band, select the radio band from the **Band** menu, or select **Both** to enable the SSID to broadcast on both bands.
10. Enable or disable band steering by clicking the **Band Steering** button.

    If the button displays green, band steering is enabled. If the button displays gray, band steering is disabled.

    If you enable band steering, the access points identify the WiFi devices that are dual-band capable and steer those devices to the 5 GHz band rather than the 2.4 GHz band of the VAP. Generally, more channels and bandwidth are available in the 5 GHz band, causing less interference and allowing for a better user experience.

11. Select the type of security from the **Security** menu:

    - **WPA2-PSK**. 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 mixed mode security. This type of security uses AES encryption.
    - **WPA/WPA2-PSK**. Mixed mode security allows both WPA and WPA2 WiFi clients to connect to the SSID. This type of security uses TKIP and AES encryption. Broadcast packets use TKIP. For unicast (that is, point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES.
    - **WPA2 ENTERPRISE**. 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 Cloud Portal on page 59).

    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.

12. If you select **WPA2-PSK** or **WPA/WPA2-PSK** security, enter a password in the **Password** field.

    Enter or change the password, which must consist of a minimum length of 8 characters and a maximum length of 63 characters.

13. Enable or disable client isolation by clicking the **Client Isolation** button in the Advanced Settings section.

    If the button displays green, client isolation is enabled. If the button displays gray, client isolation is disabled.

    If you enable client isolation, the access points block communication between WiFi clients that are associated with the same SSID or different SSIDs on the access points. This option can be useful for an open network, for example, for a hotspot at a public place.

14. To assign another VLAN to the SSID, in the Advanced Settings section, select the VLAN from the **VLAN** menu.

    For information about setting up VLANs, see Manage VLANs and VLAN-Based Features for a Location on page 68.

15. Click the **Save** button.

    Your settings are saved.

Set Up a MAC ACL for an Existing SSID

For added security, an SSID can support either a RADIUS access control list (ACL), for which you must configure a RADIUS server, or a local ACL that you must compose of individual WiFi devices.

If you set up an ACL with a policy that allows access and you enable the ACL, the ACL functions as follows:

- A WiFi device for which you placed the MAC address in the ACL is allowed access to the WiFi network.
- All other WiFi devices are denied access to the WiFi network.

If you set up an ACL with a policy that denies access and you enable the ACL, the ACL functions as follows:

- A WiFi device for which you placed the MAC address in the ACL is denied access to the WiFi network.
- All other WiFi devices are allowed access to the WiFi network.

Set Up a MAC ACL for an Existing SSID Using the Insight App

To set up a MAC ACL for an existing SSID at a 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.
4. Tap **WiFi**.
5. Tap the SSID for which you want to set up a MAC ACL.
6. Scroll down and tap **MAC Access Control**.

   Leave the MAC ACL disabled while you set up the ACL, that is, the **Enable MAC Access Control** button must display white (the default).

7. If you want to enable a RADIUS MAC ACL, from the **Type** menu, select **Radius ACL**, and enable the RADIUS MAC ACL by clicking the **Enable MAC Access Control** button so that the button displays green.

   Make sure that a RADIUS authentication server is set up for the network location (see Set Up RADIUS Servers for a Network Location Using the Insight App on page 58), otherwise you cannot enable the RADIUS MAC ACL.

   Note: After you enable a RADIUS MAC ACL, you can skip all of the following steps because they describe how you can set up a local MAC ACL.

8. From the **Type** menu, select **Local ACL**.
9. From the **Policy** menu, select one of the following modes:

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

     Note: If you set up a list with allowed WiFi devices and you use a WiFi device to access the Cloud Portal through the SSID for which you are setting up the MAC ACL, be sure that you add the MAC address of your WiFi device, or you will lose access to the SSID after you enable MAC authentication.

   - **Deny**. All WiFi devices are allowed to connect, except for WiFi devices for which you specify the MAC addresses and that are then denied access. To enable the local MAC ACL in this mode, you must add at least one WiFi denied device.

10. To add automatically detected WiFi devices, do the following:
    a. Tap **Add Devices** or, if you already added WiFi devices before, tap **Add More Devices**.
    b. Tap **Connected**, **Recent**, or **Blocked**.
    The MAC address and device name for currently connected, recently connected, or blocked WiFi devices display.
    c. Either tap the check boxes for individual MAC addresses to add those devices to the MAC ACL or tap the **MAC Address** check box to add all displayed WiFi devices to the MAC ACL.
    d. Tap **Allow** or **Deny**, depending on your selection in Step 9.
    The WiFi devices are added to the Allowed Devices or Denied Devices table, depending on your selection in Step 9.

11. To manually add a WiFi device, do the following:
    a. Tap **Add Devices** or, if you already added WiFi devices before, tap **Add More Devices**.
    b. Tap **Add Manually**.
    c. Enter a name in the **Device Name** field and a MAC address in the **MAC Address** fields.
    d. Tap **Allow** or **Deny**, depending on your selection in Step 9.
    The WiFi devices are added to the Allowed Devices or Denied Devices table, depending on your selection in Step 9.

12. To refine the table and remove one, several, or all WiFi devices from the table, do the following:
    a. Either tap the check boxes for individual MAC addresses to remove those devices from the MAC ACL or tap the **MAC Address** check box to remove all WiFi devices from the MAC ACL.
    b. Tap **Remove Device**.
    c. Tap **Yes** to confirm that you want to remove the WiFi device or devices from the MAC ACL.

13. To enable the local MAC ACL, tap the **Enable MAC Authentication** button so that the button displays green.
    WiFi device access is now restricted according to the MAC ACL that you set up.

Set Up a MAC ACL for an Existing SSID Using the Cloud Portal

To set up a MAC ACL for an existing SSID at a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. Point to the SSID and click the **pencil** icon at the right of the page.
   The Settings page for the SSID displays.
6. Select **MAC ACL**.
   The MAC ACL page displays.

   Leave the MAC ACL disabled while you set up the ACL, that is, the **Enable MAC Access Control** button must display gray (the default).
7. If you want to enable a RADIUS MAC ACL, from the **Type** menu, select **Radius ACL**, and enable the RADIUS MAC ACL by clicking the **Enable MAC Access Control** button so that the button displays green.

   Make sure that a RADIUS authentication server is set up for the network location (see Set Up RADIUS Servers for a Network Location Using the Cloud Portal on page 59), otherwise you cannot enable the RADIUS MAC ACL.

   Note: After you enable a RADIUS MAC ACL, you can skip all of the following steps because they describe how you can set up a local MAC ACL.
8. From the **Type** menu, select **Local ACL**.
9. From the **Policy** menu, select one of the following modes:
   - **Allow**. No WiFi devices are allowed to connect, except for WiFi devices for which you specify the MAC addresses and that are then allowed access. To enable the local MAC ACL in this mode, you must add at least one allowed WiFi device.

Note: If you set up a list with allowed WiFi devices and you use a WiFi device to access the Cloud Portal through the SSID for which you are setting up the MAC ACL, be sure that you add the MAC address of your WiFi device, or you will lose access to the SSID after you enable MAC authentication.

- **Deny**. All WiFi devices are allowed to connect, except for WiFi devices for which you specify the MAC addresses and that are then denied access. To enable the local MAC ACL in this mode, you must add at least one WiFi denied device.

10. To add automatically detected WiFi devices, do the following:
    a. Click the **Add Device** button.
    The Manual Access Management pop-up window opens.
    b. Click the **+** to the right of the Connected, Recent, or Blocked heading.
    The MAC address and device name for currently connected, recently connected, or blocked WiFi devices display.
    c. Either select the check boxes for individual MAC addresses to add those devices to the MAC ACL or select the **MAC Address** check box to add all displayed WiFi devices to the MAC ACL.
    d. Click the **Allow** button.
    The pop-up window closes and the WiFi devices are added to the Allowed Devices or Denied Devices table, depending on your selection in Step 9.

11. To manually add a WiFi device, do the following:
    a. Click the **Manual** button.
    The Manual Access Management pop-up window opens.
    b. Enter a name in the **Device Name** field and a MAC address in the **MAC Address** field.
    c. Click the **Add** button.
    The pop-up window closes and the WiFi device is added to the Allowed Devices or Denied Devices table, depending on your selection in Step 9.

12. To refine the table and remove one, several, or all WiFi devices from the table, do the following:
    a. Either select the check boxes for individual MAC addresses to remove those devices from the MAC ACL or select the **MAC Address** check box to remove all WiFi devices from the MAC ACL.
    b. Click the **Remove Device** button.
    The Delete Device pop-up window opens.
    c. Click the **Delete** button.

The WiFi device or devices are removed from the MAC ACL.

13. To enable the local MAC ACL, click the **Enable MAC Authentication** button so that the button displays green.

    WiFi device access is now restricted according to the MAC ACL that you set up.

Create a Captive Portal for an Existing SSID

A captive portal is a page that guests see when they attempt to connect to your SSID. 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 SSID.

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

If you want to provide customers WiFi access by letting them check in to a Facebook local business page, first register the WiFi network with Facebook Wi-Fi and (see Register and Configure Facebook Wi-Fi for a WiFi Network on page 142).

Create a Captive Portal for an Existing SSID Using the Insight App

To create a captive portal for an existing SSID 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.
4. Tap **WiFi**.
5. Tap the SSID for which you want to create a captive portal.
6. Scroll down to the ADVANCED SETTINGS section and tap **Captive Portal**.
7. Tap the **Enable Captive Portal** button so that the button displays green.

   The captive portal settings display.

8. If you want to use Facebook Wi-Fi as the authentication method, do the following:
   a. Tap **Facebook WiFi**.
   b. If you did not yet register with Facebook Wi-Fi for the network, tap **Configure now** and register with Facebook Wi-Fi.
      For more information about registering with Facebook Wi-Fi, see Register and Configure Facebook Wi-Fi for a WiFi Network Using the Insight App on page 142.
   c. After you configure Facebook Wi-Fi, skip the remaining steps in this procedure and go to Step 14.
      The remaining steps apply to a local captive portal only, not to Facebook Wi-Fi.

   By default, the authentication method is Local Captive Portal.

9. Tap **Display Message**, and do the following
   a. Enter a title.
   b. Enter a message for the WiFi users.
   c. 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 WiFi users view the captive portal.
      - Enter the EULA content that displays when WiFi users view the captive portal.
   d. Tap the arrow in the upper left to return to the other captive portal settings.

10. For URL redirection, do one of the following:
    - Tap the **Redirect URL** so that the button displays white 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.

11. Tap **Session Timeout** and swipe up or down to select a session time-out period from 30 minutes to 24 hours.
12. 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.

13. Tap **Preview** to see what the captive portal will look like to WiFi users who connect to the SSID.
14. After you are done editing the captive portal settings, tap **Save**.
Your settings are saved. The captive portal is enabled on the SSID. However, by tapping the **Captive Portal** button so that the button displays white, you can disable the captive portal without losing the settings.

Create a Captive Portal for an Existing SSID Using the Cloud Portal

To create a captive portal for an existing SSID using the Cloud Portal:

1. Access the Insight Cloud Portal.
All network locations display.
2. Select your network.
The Summary page displays.
3. Select **Wireless**.
The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
The WiFi page displays.
5. Point to the SSID and click the **pencil** icon at the right of the page.
The Settings page for the SSID displays.
6. Select **Captive Portal**.
The captive portal settings display.
7. Click the **Enable Captive Portal** button so that the button displays green.
The captive portal settings become editable.
8. If you want to use Facebook Wi-Fi as the authentication method, do the following:
   a. Select the **Facebook WiFi** radio button.
   The Facebook WiFi pop-up window opens
   b. If you did not yet register with Facebook Wi-Fi for the network, click the **Configure Now** button and register with Facebook Wi-Fi.

For more information about registering with Facebook Wi-Fi, see Register and Configure Facebook Wi-Fi for a WiFi Network Using the Cloud Portal on page 144.

c. After you configure Facebook Wi-Fi, skip the remaining steps in this procedure and go to Step 14.
The remaining steps apply to a local captive portal only, not to Facebook Wi-Fi.

By default, the **Local Captive Portal** radio button is selected and the captive portal uses the local authentication method.

9. For URL redirection, do one of the following:
   - Click the **Redirect URL** button so that the it displays gray and users are not redirected to a website after they view the captive portal.
   - In the **Redirect URL** field, enter the URL for the website that users must be redirected to after they view the captive portal.
10. From the **Session Timeout** menu, select a session time-out period from 30 minutes to 24 hours.
11. To upload an image for the captive portal, click the **Choose a file** button, locate the image, and upload it.
    By default, the captive portal displays the WiFi symbol.
12. In the Display Message section, do the following
    a. In the **Title** field, enter a title.
    b. In the **Message** field, enter a message for the WiFi users.
    c. For the EULA content, do one of the following:
       - Click the **Eula** button so that it displays gray and the EULA content does not display when WiFi users view the captive portal.
       - In the **Eula** field, enter the EULA content that displays when WiFi users view the captive portal.
13. Click the **Preview** button to see what the captive portal will look like to WiFi users who connect to the SSID.
14. Click the **Save** button.
    Your settings are saved.
15. To disable the captive portal, at the top of the page, click the **Enable Captive Portal** button so that the button displays gray.
    If you disable the captive portal, your settings are not lost. You can reenable it later.

Configure Rate Limits for an Existing SSID

If you notice WiFi speeds slowing because of heavy use on an SSID, you might want to set upload rate limits, download rate limits, or both. These limits apply only to the SSID that you configure the limits on.

The minimum bandwidth rate is 64 Kbps, the maximum bandwidth rate is 1024 Mbps. You can set one rate for the upload bandwidth and another rate for the download bandwidth.

Configure Rate Limits for an Existing SSID Using the Insight App

To configure rate limits for an existing SSID 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.
4. Tap **WiFi** .
5. Scroll down and tap **Rate Limit**.
6. Tap the **Enable** button so that the button displays green.
   The rate limit settings display.
7. From the **Upload Data Rate Unit** menu, select **Kbps** (kilobits per second) or **Mbps** (megabits per second).
8. Move the **Upload Rate Limit** slider to select a limit from 64 Kbps to 1,024 Mbps (no limit), depending on your selection in the previous step.
9. From the **Download Data Rate Unit** menu, select **Kbps** or **Mbps**.
10. Move the **Download Rate Limit** slider to select a limit from 64 Kbps to 1,024 Mbps (no limit), depending on your selection in the previous step.
11. Tap the arrow in the upper left to return to the main WiFi settings page.
12. Tap **Save**.
    Your settings are saved.

Configure Rate Limits for an Existing SSID Using the Cloud Portal

To configure rate limits for an existing SSID using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Access the Insight Cloud Portal.
   All network locations display.
4. Select your network.
   The Summary page displays.
5. Select **Wireless**.
   The Wireless page displays.
6. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
7. Point to the SSID and click the **pencil** icon at the right of the page.
   The Settings page for the SSID displays.
8. Select **Rate Limit**.
   The rate limit settings display.
9. Click the **Enable Settings** button so that it displays green.
   The rate limit settings become editable.
10. From the **Upload Data Rate Unit** menu, select **Kbps** (kilobits per second) or **Mbps** (megabits per second).
11. Move the **Upload Rate Limit** slider to select a limit from 64 Kbps to 1,024 Mbps (no limit), depending on your selection in the previous step.
12. From the **Download Data Rate Unit** menu, select **Kbps** or **Mbps**.
13. Move the **Download Rate Limit** slider to select a limit from 64 Kbps to 1,024 Mbps (no limit), depending on your selection in the previous step.
14. Click the **Save** button.
    Your settings are saved.

Set Up URL Filtering for All WiFi Clients at a Location

You can set up a blacklist by specifying URLs (web addresses) for which Internet access must be blocked. If enabled, the blacklist applies to all WiFi clients at a location.

Set Up URL Filtering for All WiFi Clients Using the Insight App

To set up URL filtering for all WiFi clients at a 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.
4. Tap **WiFi**.
5. Scroll down and tap **URL Filtering**.
6. Tap the **Blacklist** button so that the button displays green.
7. Tap **+** in the upper right corner of the screen.
8. In the **Add Domain** field, add a URL or domain name.

   When you block a URL, the domain and all URLs in the domain are blocked. For example, if you enter and add www.google.com, all web pages in the www.google.com domain are blocked, including, for example, www.google.com/finance. If you enter and add the word gamble, all web pages that include the word gamble are blocked.
9. To add more URLs or domain names, repeat the previous step.
10. If you want to compose the blacklist but not enable it, tap the **Blacklist** button again so that the button displays gray.

    The URLs and domain names that you added to the blacklist do not display but are not deleted. If you reenable the blacklist, the URLs and domain names display again.

Set Up URL Filtering for All WiFi Clients Using the Cloud Portal

To set up URL filtering for all WiFi clients at a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. Select **URL Filtering**.
   The URL Filtering page displays.
6. Click the **Blacklist** button so that the button displays green.
7. At the top right of the page, click the **+** button.
   The Add Domain pop-up window opens.
8. In the **Add Domain** field, add a URL or domain name.
   When you block a URL, the domain and all URLs in the domain are blocked. For example, if you enter and add www.google.com, all web pages in the www.google.com domain are blocked, including, for example, www.google.com/finance. If you enter and add the word gamble, all web pages that include the word gamble are blocked.
9. To add more URLs or domain names, repeat the previous step.
10. If you want to compose the blacklist but not enable it, click the **Blacklist** button again so that the button displays gray.
    The URLs and domain names that you added to the blacklist do not display but are not deleted. If you reenable the blacklist, the URLs and domain names display again.

Configure Automatic Radio Resource Management and Optimize the Radios at a Location

Radio Resource Management (RRM), which is based on IEEE 802.11k, lets the access points and their clients dynamically measure the available radio resources. In an 802.11k-enabled network, access points and clients can send neighbor reports, beacon reports, and link measurement reports to each other, allowing 802.11k-aware clients to automatically select the best access point for initial connection or for roaming.

Automatic RRM (Auto RRM) collects the radio statistics and information from each access point at a location during each monitoring interval for a period of 24 hours and computes the best channel and best transmit power for the access point. The received signal strength indicator (RSSI) value of the neighboring devices and the average RSSI value of the associated clients is used to calculate the transmit power. To calculate the channel, the number of neighbors (both known and unknown) that are detected by each access point is considered, and neighbors that are detected by the neighbors on each channel. Based on the number of neighbors, the hop count, and the channels that are supported by the radio mode, the best channel is computed for the device.

You can enable or disable the automatic channel selection and automatic output power selection for the 2.4 GHz radios, 5 GHz radios, or both types of radios on all access points at a location. By default, the Auto RRM is enabled for both types of radios and applies to all access point at a location. You can also manually optimize automatic channel selection and automatic output power selection on all access points at a location.

Note: For information about manually configuring the channels and output power for an *individual* access point, see Manage the Channels and Output Power for an Access Point Manually on page 186.

Configure Automatic Radio Resource Management and Optimize the Radios Using the Insight App

Note: For information about manually configuring the channels and output power for an *individual* access point using the Insight app, see Manage the Channels and Output Power for an Access Point Manually Using the Insight App on page 186.

To configure automatic radio resource management (Auto RRM) and optimize the radios at a 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.
4. Tap **WiFi**.
5. Scroll down and tap **Auto RRM**.
6. For each type of radio, enable or disable the following settings:
   - **Automatic channel selection**. Tap the **Auto Channel Selection** button to enable or disable automatic channel selection, which applies to the selected type of radio on all access points at the location.
   - **Automatic output power selection**. Tap the **Auto Tx Power Selection** button to enable or disable automatic output power selection, which applies to the selected type of radio on all access points at the location.

   If a button displays green, the option is enabled. If the button displays gray, the option is disabled. By default, both options are enabled.
7. To immediately optimize automatic channel selection and automatic output power selection on all access points at the location, tap the **Optimize Now** button.
   The radios are optimized according to the settings that you selected in Step 6.

Configure Automatic Radio Resource Management and Optimize the Radios Using the Cloud Portal

Note: For information about manually configuring the channels and output power for an *individual* access point using the Cloud Portal, see Manage the Channels and Output Power for an Access Point Manually Using the Cloud Portal on page 187.

To configure automatic radio resource management (Auto RRM) and optimize the radios at a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. Select **Auto RRM**.
   The Auto RRM page displays.
6. For each type of radio, enable or disable the following settings:
   - **Automatic channel selection**. Click the **Auto Channel Selection** button to enable or disable automatic channel selection, which applies to the selected type of radio on all access points at the location.
   - **Automatic output power selection**. Click the **Auto Tx Power Selection** button to enable or disable automatic output power selection, which applies to the selected type of radio on all access points at the location.

   If a button displays green, the option is enabled. If the button displays gray, the option is disabled. By default, both options are enabled.
7. To immediately optimize automatic channel selection and automatic output power selection on all access points at the location, click the **Optimize Now** button.
   The radios are optimized according to the settings that you selected in Step 6.

Configure Fast Roaming for a WiFi Network

Fast Roaming helps to improve the performance of mobile devices that are roaming in a WiFi network, including power consumption and portability.

Fast Roaming is based on Opportunistic Key Caching (OKC). Fast Roaming reduces the delay in the connection when clients roam from one access point to another access point that is configured in the same WiFi network at the same location. Another advantage of fast roaming is that clients do not need to reauthenticate captive portal access while roaming within the same WiFi network at the same location.

Configure Fast Roaming for a WiFi Network Using the Insight App

To configure Fast Roaming for a WiFi Network at a 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.
4. Tap **WiFi**.
5. Scroll down and tap **Fast Roaming**.
6. Tap the **Enable** button so that the button displays green.
   By default, Fast Roaming is disabled and the button displays white.

   The Mobility ID field displays the mobility ID for the devices in the WiFi network.

Configure Fast Roaming for a WiFi Network Using the Cloud Portal

To configure Fast Roaming for a WiFi Network at a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. Select **Fast Roaming**.
   The Fast Roaming page displays.
6. Click the **Enable** button so that the button displays green.
   By default, Fast Roaming is disabled and the button displays gray.

   The Mobility ID field displays the mobility ID for the devices in the WiFi network.

Register and Configure Facebook Wi-Fi for a WiFi Network

If you want to use Facebook Wi-Fi as the authentication mode for any captive portal that you set up for the network location, you must first register and configure Facebook Wi-Fi. Registration and configuration applies too the entire WiFi network at a location. That is, after you register and configure Facebook Wi-Fi, you can use it as the authentication method for any captive portal that you set up at a location.

During the Facebook Wi-Fi registration and configuration process, you can set up a new Facebook account or select an existing one.

Register and Configure Facebook Wi-Fi for a WiFi Network Using the Insight App

To register and configure Facebook Wi-Fi for a WiFi network at a 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.
4. Tap **WiFi**.
5. Scroll down and tap **Facebook WiFi**.
6. Tap the **Facebook WiFi** button so that the button displays green.
7. Tap **Register**.
8. Either log in using an existing Facebook business account or create a new Facebook business account.

   After you are logged in, the Facebook Wi-Fi Configuration page displays.
9. From the **Facebook Page** menu, select the Facebook local business page.
10. In the Bypass Mode section, select one of the following bypass mode options:

    - To allow customers to skip check-in, select the **Skip check-in link** radio button. If you enable this option, users can either check in to the selected Facebook business page or skip the check-in.
    - To require users to enter a WiFi code before they can gain WiFi access, select the **Require Wi-Fi code** radio button and type a WiFi code in the field that

displays. If you enable this option, users can either check in to the selected Facebook business page or skip the check-in by using the WiFi code.

11. From the **Session Length** menu, select the period after which users are automatically logged out.
12. To add terms of service to the Facebook check-in page, select the **Terms of Service** check box and type or copy the terms of service.
13. Tap **Save Settings**.

    The Facebook Wi-Fi settings are saved.

    You might need to decrease the size of the page to see the **Save Settings** button.

14. Tap **<** in the upper left corner of the page to return to the Facebook WiFi page in the Insight app.

    The page no longer displays the **Register** button but now displays the **Configure** button and the **Verify Page** button. The **Configure** button allows you to make changes to the settings that you selected or select and configure another Facebook local business page.

15. Tap **Verify Page**.

    If the pairing is successful, the name of the Facebook local business page that you selected displays in the **Page** field, along with the **Enable SSL** button.

16. To allow a secure HTTP (HTTPS) Facebook session *before* authentication at a captive portal occurs, click the **Enable SSL** button so that the button displays green.

    By default, the button displays white and the Facebook session before authentication at a captive portal is over HTTP.

17. Tap **Save**.

    You can now select Facebook Wi-Fi as the authentication method for a captive portal on an individual SSID (see Create a Captive Portal for an Existing SSID Using the Cloud Portal on page 132).

Register and Configure Facebook Wi-Fi for a WiFi Network Using the Cloud Portal

To register and configure Facebook Wi-Fi for a WiFi network at a 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 **Wireless**.
   The Wireless page displays.
4. At the top right of the page, click the **Settings** button.
   The WiFi page displays.
5. Select **Facebook WiFi**.
   The Facebook WiFi page displays.
6. To enable the capability to register and configure Facebook WiFi, click the **Facebook WiFi** button so that the button displays green.
7. Click the **Register** button.
   The Facebook login page displays.
8. Either log in using an existing Facebook business account or create a new Facebook business account.
   After you are logged in, the Facebook Wi-Fi Configuration page displays.
9. From the **Facebook Page** menu, select the Facebook local business page.
10. In the Bypass Mode section, select one of the following bypass mode options:
    - To allow customers to skip check-in, select the **Skip check-in link** radio button. If you enable this option, users can either check in to the selected Facebook business page or skip the check-in.
    - To require users to enter a WiFi code before they can gain WiFi access, select the **Require Wi-Fi code** radio button and type a WiFi code in the field that displays. If you enable this option, users can either check in to the selected Facebook business page or skip the check-in by using the WiFi code.
11. From the **Session Length** menu, select the period after which users are automatically logged out.

12. To add terms of service to the Facebook check-in page, select the **Terms of Service** check box and type or copy the terms of service.
13. Click the **Save Settings** button.

    The Facebook Wi-Fi settings are saved.
14. Return to the Facebook WiFi page in the Cloud Portal.

    The page no longer displays the **Register** button but now displays the **Configure** button and the **Verify Page** button. The **Configure** button allows you to make changes to the settings that you selected or select and configure another Facebook local business page.
15. Click the **Verify Page** button.

    If the pairing is successful, the name of the Facebook local business page that you selected displays in the **Page** field, along with the **Allow HTTPS** button.
16. To allow a secure HTTP (HTTPS) Facebook session *before* authentication at a captive portal occurs, click the **Allow HTTPS** button so that the button displays green.

    By default, the button displays white and the Facebook session before authentication at a captive portal is over HTTP.
17. Click the **Save** button.

    Your settings are saved.

    You can now select Facebook Wi-Fi as the authentication method for a captive portal on an individual SSID (see Create a Captive Portal for an Existing SSID Using the Cloud Portal on page 132).

7

Manage VPN Groups, VPN Users, and VPN Connections

This chapter describes how to manage VPN groups, VPN users, and VPN connections for Insight Managed routers.

The chapter includes the following sections:

- Manage VPN Groups for a Router
- Manage VPN Users for a Router
- Manage Devices in a VPN Group on a Router
- Download and Install the NETGEAR Insight VPN Application

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Manage VPN Groups for a Router

You can manage VPN groups for a router.

Create a VPN Group Using the Insight App

You can connect your router to a virtual private network (VPN) consisting of up to three routers across multiple locations. Each router allows up to ten users to join, for a total of thirty possible users. In Insight, this is called a VPN Group.

To create a VPN group in the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.

   The list of devices on your network displays.
3. Tap your router.
4. Tap **VPN Group**.
5. At the top, tap **+**.
6. When prompted, enter a name for your new VPN group and tap **Save**.

   Your new VPN group appears on the Routers page. Now, you can add a device to your group. To learn more about adding a device, see Add a Device to a VPN Group Using the Insight App on page 149.

Create a VPN Group Using the Cloud Portal

You can connect your router to a virtual private network (VPN) consisting of up to three routers across multiple locations. Each router allows up to ten users to join, for a total of thirty possible users. In Insight, this is called a VPN Group.

To create a VPN group in the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. At the top, select **Routers**.
4. Click **Create VPN Group**.

   If the router is connected to a VPN group already, at the top, click **+** instead.
5. When prompted, enter a name for your new VPN group and click **Save**.

Your new VPN group appears on the Routers page. Now, you can add a device to your group. To learn more about adding a device, see Add a Device to a VPN Group Using the Cloud Portal on page 150.

Manage VPN Users for a Router

After you set up a VPN group, you can manage the VPN users for a router.

Invite Someone to a VPN Group Using the Insight App

After you create a virtual private network (VPN) group, invite up to ten users per router to give them access.

For more information on how to create a VPN group, see Create a VPN Group Using the Insight App on page 147.

To invite a new user to your VPN group in the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.
3. In the top left, tap the menu icon.
4. Tap **VPN Users**.
   The list of users for this location displays.
5. In the top right, tap **+**.
6. Enter the email address of the person you want to invite and tap **Invite**.
   An invitation is mailed to them. They can follow the instructions in the email to gain access to the VPN.

   On the VPN Users screen, under each person's email address their access status, such as "Pending" or "Active," is displayed.

Invite Someone to a VPN Group Using the Cloud Portal

After you create a virtual private network (VPN) group, you can invite up to ten users per router to give them access.

For more information on how to create a VPN group, see Create a VPN Group Using the Cloud Portal on page 147.

To invite a new user to your VPN group in the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. Select **Routers.**
4. At the top right of the page, click the **Settings** button.
5. Select **VPN Users**.
6. On the right, click **+**.
7. Enter the email address of the person that you want to invite and click **Invite**.

   An invitation is mailed to them. They can follow the instructions in the email to gain access to the VPN.

   On the VPN Users page, next to each person's email address their access status, such as "Pending" or "Active," is displayed.

Manage Devices in a VPN Group on a Router

You add devices to a VPN group on a router.

Add a Device to a VPN Group Using the Insight App

After you create a virtual private network (VPN) group, you can add up to three routers to it. Up to ten users can connect to each router. Devices added to your VPN group create site-to-site VPN tunnels between locations.

For more information about creating a VPN topic, see Create a VPN Group Using the Insight App on page 147.

To add a device to a VPN group in the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.

   The list of devices on your network displays.
3. Tap your router.
4. Inside the circle for the VPN group that you want to add the router to, tap **Add Device**.
5. Select the router that you want to add.
6. Tap **Save**.

Add a Device to a VPN Group Using the Cloud Portal

After you create a virtual private network (VPN) group, you can add up to three routers to it. Up to ten users can connect to each router. Devices added to your VPN group create site-to-site VPN tunnels between locations.

For more information about creating a VPN group, see Create a VPN Group Using the Cloud Portal on page 147.

To add a device to a VPN group in the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. Select **Routers**.
4. Under the name of your VPN group, inside the circle, click **Add Device**.
5. Select the device or devices that you want to add and click **Save**.

Download and Install the NETGEAR Insight VPN Application

If you plan to connect your computer to a virtual private network (VPN) group without a direct Ethernet connection to the router, you must install the NETGEAR Insight VPN application.

Before you can get the NETGEAR Insight VPN application, you need an invitation to a VPN network. For more information about invitations to a VPN network:

- Invite Someone to a VPN Group Using the Cloud Portal on page 148
- Invite Someone to a VPN Group Using the Insight App on page 148

To download and install the NETGEAR Insight VPN application:

1. On your computer, open your invitation email to the VPN group.
2. Click the included link to download the VPN application.
   You can also download the VPN application from the BR500 product support site.
3. Open and run the installation file.
4. Run the VPN application.
5. Log in with your NETGEAR account and password.
   If you do not have a NETGEAR account, click **Create account**.

8

Manage Individual Routers

This chapter describes how you can manage features that are specific to Insight Managed routers. A VLAN that you create for a router in one location can be used by multiple devices at that location. Therefore, VLANs are specific to a wired network (see Manage VLANs and VLAN-Based Features for a Location on page 68 and Manage the Wired Network for a Location on page 99), not to a single router.

The chapter includes the following sections:

- Specify a Static WAN IP Address for a Router
- Manage One or More DHCP Servers of a Router
- Manage the Router Settings

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Specify a Static WAN IP Address for a Router

How the router receives it's WAN IP address depends on how you set up the router. By default, the DHCP client of an Insight Managed router is enabled and the router receives an IP address from an Internet service provider (ISP) or from a DHCP server (or router that functions as a DHCP server) at the network location in which the router is installed.

You can disable the DHCP client of a router and specify a static (fixed) IP address.

Change a Router's WAN IP Address Using the Insight App

You can set a specific IP address or change the WAN IP address assigned to your router's LAN instead of letting a DHCP server assign it automatically.

To change a router's IP address using the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.

   The list of devices on your network displays.
3. Tap the router that you want to change the IP address of.
4. Tap **WAN IP**.
5. Turn **Assign IP Address Automatically** off.
6. Enter a new IP address.
7. Tap **Save**.

Change a Router's WAN IP Address Using the Cloud Portal

You can set a specific IP address or change the IP address assigned to your router instead of letting a DHCP assign it automatically.

To change your router's IP address using the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. At the top, select **Routers**.
4. Double-click the router you want to change the IP address of.
5. Select **WAN IP**.
6. Turn **Assign IP Address Automatically** off.
7. Enter the new IP address and click **Save**.

Manage One or More DHCP Servers of a Router

You can manage the settings for one or more DHCP servers on a router.

Change or Disable Your Router's DHCP Server Using the Insight App

You can change your router's DHCP server IP address or turn it off entirely.

To change or turn off a router's DHCP server using the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.
   The list of devices on your network displays.
3. Tap your router.
4. Tap **DHCP Servers**.
   You see a list of DHCP servers.
5. Tap the server that you want to change.
6. Turn off **DHCP Server** or change the IP addresses below.
7. When you are finished, tap **Save**.

Change or Disable A Router's DHCP Server Using the Cloud Portal

You can change your router's DHCP server IP address or turn it off entirely.

To change or disable your router DHCP server using the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. At the top, select **Routers**.
4. Scroll down to the Devices pane and double-click the router you want to change.
5. Select **DHCP Servers**.
6. Next to the DHCP Server, click the Edit icon.

7. Edit your DCHP Server's IP addresses or turn it off entirely.
8. When you are done, click **Save**.

Manage the Router Settings

You can manage the settings for an individual router.

Manage Individual Routers Using the Insight App

You can see and edit details about any router on your Insight network in the NETGEAR Insight app. Open your router's status screen to check essential information or modify settings remotely.

To manage an individual router's settings using the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.

   The list of devices on your network displays.
3. To see more details and options for any device on the network, tap it.

   A screen of detailed information about the router displays, such as model, firmware version, IP address, and MAC address.
4. Tap a menu item to see more information or edit the settings, such as **Connected Clients**, **VPN Group**, **VLANs In Use**, **DHCP servers**, or **WAN IP**.

Manage Individual Routers Using the Cloud Portal

You can see and edit details about any Insight managed router on your network in the Insight Cloud Portal. The router page displays essential information and lets you modify settings remotely.

To manage an individual router's settings using the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. Select **Routers**.
4. Scroll down to the Devices pane and double-click the router that you want to manage.

   A list of detailed information about the router displays, including its ports, name, firmware version, IP address, and MAC address.

5. Click a menu item on the left to see more information or edit the settings, such as **WAN IP**, **VPN Groups**, **VPN Users**, or **VLANs in use**.

9

Manage Individual Switches

This chapter describes how you can manage features that are specific to Insight Managed switches. A wired network and VLAN that you create for one location can be used by multiple devices at that location. Therefore, such features are specific to a wired network (see Manage VLANs and VLAN-Based Features for a Location on page 68 and Manage the Wired Network for a Location on page 99), not to a single switch.

The chapter includes the following sections:

- Configure Switch Ports
- Manage Power over Ethernet
- Specify a Static IP Address for a Switch

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

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 170.
- 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 95.

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.

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 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 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 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 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.

Manage Power over Ethernet

PoE and PoE+ use Ethernet cables to supply power to PoE-capable devices on the network, such as WiFi access points, IP cameras, VoIP phones, and switches. An Insight Managed switch is compliant with the IEEE 802.3at standard (PoE+) and backward compatible with the IEEE 802.3af standard (PoE). The switch can pass power through to any powered device (PD) that supports these standards. PoE and PoE+ let you power such devices without the need for a separate power supply.

An Insight Managed switch supports a Plug-and-Play process by which it detects the type of device that is connected to one of its PoE+ ports and whether that device needs power and how much so that the switch can provide the correct power the device. During the Plug-and-Play process, the connected device can provide its Class response to the switch in many ways, depending on how the vendor programmed the device.

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 manage custom PoE settings 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 (see Create a PoE Schedule on page 112). You can set up multiple PoE schedules for a network location.

This section describes PoE in relation to individual switches and 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
- Manage Custom PoE Settings for One or More Ports on a Switch

- 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 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.

Manage Custom PoE Settings for One or More Ports on a Switch

By default, Insight Managed switches supply PoE power according to the default device class power requirements.

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

For most network configurations, the default settings work well. However, if you do not want to use the default settings, you can manage the following PoE settings to create a custom PoE configuration for one or more ports on a switch:

- **PoE standard**. The detection type is also referred to as the PoE port mode. You can select one of the following power modes:
  - **802.3af**. The port is powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if the port functions in IEEE 802.3af mode.
  - **Legacy**. The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
  - **Pre-802.3at**. The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high-power IEEE 802.3at mode. Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.
  - **802.3at**. The port is powered in the IEEE 802.3at mode. This is the default setting. In this mode, if the switch detects that the attached PD is not a Class 4 device, the PD does not receive power from the switch.

- **Detection type**. The detection type specifies how the port detects the attached PD. You can select one of the following types:
  - **IEEE 802**. The port performs a 4-point resistive detection. This is the default setting.
  - **Legacy**. The port performs legacy detection.
  - **4pt 802.3af + Legacy**. The port performs a 4-point resistive detection, and if required, continues with legacy detection.

- **Port priority**. The port priority determines which ports can still deliver power after the total power delivered by the switch exceeds its total power budget. (In such a situation, the switch might not be able to deliver power to all connected devices.) If

the same priority applies to two ports, the lower-numbered port receives higher priority. You can select one of the following priorities:

- **Low**. Low priority. This is the default setting.
- **Medium**. Medium priority.
- **High**. High priority.
- **Critical**. Critical priority.

- **Class**. The class defines the PoE power limit that is set on the port or ports. You can manage the following class settings:
  - Select the default class, which the switch detects automatically. This is the default setting.
  - Override the default class and manually set the PoE power limit in watts.
  - Select a specific class (0, 1, 2, 3, or 4).

Manage Custom PoE Settings for One or More Ports on a Switch Using the Insight App

To manage custom PoE settings for a single port or for a group of ports on the same 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 Management**.
8. Tap the **Enable PoE** button to enable or disable PoE.

9. To set a custom PoE standard (PoE port mode), do the following:
   a. Tap **PoE Standard**.
   b. Swipe up or down to select one of the following modes:
      - **802.3af**. The selected ports are powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if a port functions in IEEE 802.3af mode.
      - **Legacy**. The selected ports are powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
      - **Pre-802.3at**. The selected ports are initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high-power IEEE 802.3at mode. Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.
      - **802.3at**. The selected ports are powered in the IEEE 802.3at mode. This is the default setting. In this mode, if the switch detects that the attached PD is not a Class 4 device, the PD does not receive power from the switch.
   c. Tap **Done**.
10. To set a custom detection type, do the following:
   a. Tap **Detection Type**.
   b. Swipe up or down to select one of the following types:
      - **IEEE802**. The selected ports perform a 4-point resistive detection. This is the default setting.
      - **Legacy**. The selected ports perform legacy detection.
      - **4pt 802.3aft + legacy**. The selected ports perform a 4-point resistive detection, and if required, continues with legacy detection.
   c. Tap **Done**.
11. To set a custom priority, do the following:
   a. Tap **Priority**.
   b. Swipe up or down to select **Low** (the default), **Medium**, **High**, or **Critical**.
   c. Tap **Done**.
12. To enable or disable use of the automatically detected PoE class, tap the **Use detected Class** button.

By default, Insight automatically uses the detected PoE class for all PoE-capable ports. If the button displays green, the detected PoE class is used for all selected PoE-capable ports. If the button displays white, the detected PoE class is not used for all selected PoE-capable ports.

13. If you do not use the detected PoE class (that is, the **Use detected Class** button displays white), do the following:
    a. Tap **Power Limit Type**.
    b. Swipe up or down to select **Class0 - 15.4W**, **Class1 - 4W**, **Class2 - 7W**, **Class3 - 15.4W**, **Class4 - 30W**, or **User Defined**.
    c. Tap **Done**.

14. If you select **User Defined** in the previous step, tap **Power Limit (Watts)** and move the slider to specify the limit in watts that the selected ports can deliver.
    The minimum and maximum watts that are displayed and that you can set depend on the switch model and the detected powered device (PD) class. In most situations, the minimum is 3W and the maximum is 30W.

15. Tap the arrow at the top of the page to return to the previous page.
16. Tap **Save**.
    Your settings are saved.

Manage Custom PoE Settings for One or More Ports on a Switch Using the Cloud Portal

This procedure lets you manage custom PoE settings 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 manage custom PoE settings 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. To set a custom PoE standard (PoE port mode), from the **PoE Standard** menu, select one of the following modes:

   - **802.3af**. The selected ports are powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if a port functions in IEEE 802.3af mode.
   - **Legacy**. The selected ports are powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
   - **Pre-802.3at**. The selected ports are initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high-power IEEE 802.3at mode.

Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.

- **802.3at**. The selected ports are powered in the IEEE 802.3at mode. This is the default setting. In this mode, if the switch detects that the attached PD is not a Class 4 device, the PD does not receive power from the switch.

8. To set a custom detection type, from the **Detection Type** menu, select one of the following types:
   - **IEEE802**. The selected ports perform a 4-point resistive detection. This is the default setting.
   - **legacy**. The selected ports perform legacy detection.
   - **4pt 802.3aft + legacy**. The selected ports perform a 4-point resistive detection, and if required, continues with legacy detection.
9. To set a custom priority, from the **Priority** menu, select **Low** (the default), **Medium**, **High**, or **Critical**.
10. 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.
11. If you do not use the default class, do one of the following:
    - Set a specific class by selecting **Class0 - 15.4W**, **Class1 - 4W**, **Class2 - 7W**, **Class3 - 15.4W**, or **Class4 - 30W**.
    - Select **User Defined** and in the **Power Limit (Watts)** field, enter a number to specify the maximum watts that the selected ports can deliver.
      The minimum and maximum watts that are displayed and that you can set depend on the switch model and the detected powered device (PD) class. In most situations, the minimum is 3W and the maximum is 30W.
12. Click the **Save** button.

    Your settings are saved.

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 112), 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 112).
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 113).
8. Click the **Save** button.
   Your settings are saved.

Specify a Static IP Address for a Switch

By default, the DHCP client of an Insight Managed switch is enabled and the switch receives an IP address from a DHCP server (or router that functions as a DHCP server) at the network location in which the switch is installed.

You can disable the DHCP client and specify a static (fixed) IP address.

Specify a Static IP Address for a Switch Using the Insight App

To specify a static IP address for 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. Tap **IP**.
5. Tap the **Assign IP Address Automatically** button so that it displays white.
   The DHCP client of the switch is disabled and the IP address fields become available.
6. Specify the static IP address settings:
   - **IP Address**. An IP address in the range that is used by the LAN at the network location.
   - **Subnet Mask**. A subnet mask that is compatible with the LAN at the network location.
   - **Gateway Address**. The IP address of the gateway on the LAN at the network location.
   - **DNS Server**. The IP address of the primary Domain Name System (DNS) server.

   Caution: Make sure that you enter the correct information otherwise you might no longer be able to access the switch and might need to reset the switch to its factory default configuration.
7. Tap **Save**.
   Your settings are saved and the switch restarts with the new IP settings.

Specify a Static IP Address for a Switch Using the Cloud Portal

To specify a static IP address for a 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. Select **IP Settings**.
   The IP Settings page displays.
6. Click the **Assign IP Address Automatically** button so that the button displays gray.
   By default, the DHCP client of the switch is enabled and the button displays green.
7. Specify the static IP address settings:
   - **IP Address**. An IP address in the range that is used by the LAN at the network location.
   - **Subnet Mask**. A subnet mask that is compatible with the LAN at the network location.
   - **Gateway Address**. The IP address of the gateway on the LAN at the network location.
   - **DNS Server**. The IP address of the primary Domain Name System (DNS) server and the secondary DNS server.

   Caution: Make sure that you enter the correct information otherwise you might no longer be able to access the switch and might need to reset the switch to its factory default configuration.

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

10

Manage Individual Access Points

This chapter describes how you can manage features that are specific to a single access point. A WiFi network that you create on one access point at a location is deployed on all access points at that location. Most features that you can manage on a single access point are deployed on all access points at a location. Therefore, such features are specific to WiFi networks (see Manage the WiFi Network and SSIDs for a Location on page 115), not to a single access point.

The chapter includes the following sections:

- Manage the Channels and Output Power for an Access Point Manually
- Specify a Static IP Address for an Access Point

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Manage the Channels and Output Power for an Access Point Manually

The available WiFi channels and frequencies depend on the country that you select for the location in which the access point functions and the radio (2.4 GHz or 5 GHz). The default is Auto, which enables the radio to automatically select the most suitable channel.

You do not need to change the WiFi channel unless you experience interference (which is indicated by lost connections). If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. We recommend a channel spacing of four channels between adjacent APs (for example, use Channels 1 and 5, or 6 and 10).

By default, the output power of the access point is set at the maximum. If two or more access points are operating in the same area and on the same channel, interference can occur. In such a situation, you might want to decrease the output power for an access point. Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in the country that you select for the location in which the access point functions.

Manage the Channels and Output Power for an Access Point Manually Using the Insight App

To manage the channels and output power for an access point manually 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. Scroll down and tap **Radio and Channels**.
   The 2.4 GHz Radio Configuration and 5 GHz Radio Configuration sections display.
5. To set the channel for a radio, do the following in the
   a. Tap **Channel**.
   b. Swipe up or down to select a channel and frequency.
      The default setting is Auto.
   c. Tap **Done**.

6. To set the width for a channel (which you can do only if the channel setting is not Auto), do the following:
   a. Tap **Channel Width**.
   b. Swipe up or down to select a channel width.
      The default setting for the 2.4 GHz radio is Dynamic 20 / 40 MHz.
      The default setting for the 5 GHz radio is Dynamic 20 / 40 / 80 MHz.
7. To set the output power for a radio, do the following:
   a. Tap **Output Power**.
   b. Swipe up or down to select an output power strength.
      The default setting is Full.
   c. Tap **Done**.
8. Tap **Save**.
   Your settings are saved.

Manage the Channels and Output Power for an Access Point Manually Using the Cloud Portal

To manage the channels and output power for an access point manually using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wireless**.
   The Wireless page displays.
4. Scroll down to the Devices pane, point to the access point that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the access point displays.
5. Select **Radio and Channels**.
   The Radio and Channels page displays.
6. To set the channel for a radio, from the **Channel** menu, select a channel.
   The default setting is Auto.

7. To set the width for a channel (which you can do only if the channel setting is not Auto), from the **Channel Width** menu, select a select a channel width.
   The default setting for the 2.4 GHz radio is Dynamic 20 / 40 MHz.
   The default setting for the 5 GHz radio is Dynamic 20 / 40 / 80 MHz.
8. To set the output power for a radio, from the **Output Power** menu, select the output power strength.
   The default setting is Full.
9. Click the **Save** button.
   Your settings are saved.

Specify a Static IP Address for an Access Point

By default, the DHCP client of an Insight Managed access point is enabled and the access point receives an IP address from a DHCP server (or router that functions as a DHCP server) at the network location in which the access point is installed.

You can disable the DHCP client and specify a static (fixed) IP address.

Specify a Static IP Address for an Access Point Using the Insight App

To specify a static IP address for 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 **IP**.
5. Tap the **Assign IP Address Automatically** button so that it displays white.
   The DHCP client of the access point is disabled and the IP address fields become available.

6. Specify the static IP address settings:
   - **IP Address**. An IP address in the range that is used by the LAN at the network location.
   - **Subnet Mask**. A subnet mask that is compatible with the LAN at the network location.
   - **Gateway Address**. The IP address of the gateway on the LAN at the network location.
   - **DNS Server**. The IP address of the primary Domain Name System (DNS) server.

   Caution: Make sure that you enter the correct information otherwise you might no longer be able to reach the access point and might need to reset the access point to its factory default configuration.

7. Tap **Save**.
   Your settings are saved and the access point restarts with the new IP settings.

Specify a Static IP Address for an Access Point Using the Cloud Portal

To specify a static IP address for an access point using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wireless**.
   The Wireless page displays.
4. Scroll down to the Devices pane, point to the access point that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the access point displays.
5. Select **IP Settings**.
   The IP Settings page displays.
6. Click the **Assign IP Address Automatically** button so that the button displays gray.
   By default, the DHCP client of the access point is enabled and the button displays green.

7. Specify the static IP address settings:
   - **IP Address**. An IP address in the range that is used by the LAN at the network location.
   - **Subnet Mask**. A subnet mask that is compatible with the LAN at the network location.
   - **Gateway Address**. The IP address of the gateway on the LAN at the network location.
   - **DNS Server**. The IP address of the primary Domain Name System (DNS) server.

   Caution: Make sure that you enter the correct information otherwise you might no longer be able to reach the access point and might need to reset the access point to its factory default configuration.

8. Click the **Save** button.
   Your settings are saved and the access point restarts with the new IP settings.

11

Manage Individual ReadyNAS Storage Systems

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
- Specify a Static IP Address for a ReadyNAS Storage System
- Enable Secure Diagnostics Mode on a ReadyNAS Storage System

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

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 18.

Before you can add a ReadyNAS storage system to your Insight account, as described in Discover, Add, and Register Devices on page 29, 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 and the account that you used to log in to ReadyCLOUD is the same account that you use to log in to Insight.

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.

Specify a Static IP Address for a ReadyNAS Storage System

By default, the DHCP client of a ReadyNAS storage system is enabled and the system receives an IP address from a DHCP server (or router that functions as a DHCP server) at the network location in which the system is installed.

You can disable the DHCP client and specify a static (fixed) IP address.

Specify a Static IP Address for a ReadyNAS Storage System Using the Insight App

To specify a static IP address for 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 storage system that you want to configure.
4. Tap **IP**.
5. Tap the **Assign IP Address Automatically** button so that it displays white.
   The DHCP client of the ReadyNAS storage system is disabled and the IP address fields become available.
6. Specify the static IP address settings:
   - **IP Address**. An IP address in the range that is used by the LAN at the network location.
   - **Subnet Mask**. A subnet mask that is compatible with the LAN at the network location.
   - **Gateway Address**. The IP address of the gateway on the LAN at the network location.
   - **DNS Server**. The IP address of the primary Domain Name System (DNS) server.

   Caution: Make sure that you enter the correct information otherwise you might no longer be able to access the ReadyNAS storage system and might need to reset the system to its factory default configuration.
7. Tap **Save**.
   Your settings are saved and the ReadyNAS storage system restarts with the new IP settings.

Specify a Static IP Address for a ReadyNAS Storage System Using the Cloud Portal

To specify a static IP address for a ReadyNAS storage system using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Storage**.
   The Storage page displays.
4. Scroll down to the Devices pane, point to the ReadyNAS storage system that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the ReadyNAS storage system displays.
5. Select **IP Settings**.
   The IP Settings page displays.
6. Click the **Assign IP Address Automatically** button so that the button displays gray.
   By default, the DHCP client of the ReadyNAS storage system is enabled and the button displays green.
7. Specify the static IP address settings:
   - **IP Address**. An IP address in the range that is used by the LAN at the network location.
   - **Subnet Mask**. A subnet mask that is compatible with the LAN at the network location.
   - **Gateway Address**. The IP address of the gateway on the LAN at the network location.
   - **DNS Server**. The IP address of the primary Domain Name System (DNS) server.

   Caution: Make sure that you enter the correct information otherwise you might no longer be able to access the ReadyNAS storage system and might need to reset the ReadyNAS storage system to its factory default configuration.
8. Click the **Save** button.

Your settings are saved and the ReadyNAS storage system restarts with the new IP settings.

Enable Secure Diagnostics Mode on a ReadyNAS Storage System

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.

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

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.

Enable Secure Diagnostics Mode on a ReadyNAS Storage System Using the Cloud Portal

To enable Secure Diagnostics Mode on a ReadyNAS storage system using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.

3. Select **Storage**.
   The Storage page displays.
4. Scroll down to the Devices pane, point to the ReadyNAS storage system that you want to configure, and click the **pencil** icon at the right of the page.
   The Summary page for the ReadyNAS storage system displays.
5. Select **Diagnostic Mode**.
   The Diagnostics Mode page displays.
6. Click the **Secure Diagnostics Mode** button so that the button displays green.
   A pop-up warning displays.
7. Click the **OK** button.
   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.

12

Monitor Insight Networks and Devices

This chapter describes the options to monitor the Insight network location, individual devices, and clients.

The chapter includes the following sections:

- Overview of the Monitoring Options for a Network Location in the Cloud Portal
- Customize Widgets in the Cloud Portal
- Monitor All Network Locations Using the Cloud Portal
- Display All Devices at All Network Locations Using the Cloud Portal
- Monitor All Devices at a Single Network Location Using the Cloud Portal
- Monitor a Single Network Location Using the Cloud Portal
- Monitor the Wired Network at a Location Using the Cloud Portal
- Monitor the WiFi Network and SSIDs at a Location Using the Cloud Portal
- Monitor the Storage Network at a Location Using the Cloud Portal
- Monitor an Individual Switch and Individual Ports Using the Cloud Portal
- Monitor an Individual Access Point and Its Clients Using the Cloud Portal
- Monitor an Individual ReadyNAS Storage System Using the Cloud Portal
- Monitor the Clients at a Network Location Using the Cloud Portal
- Monitor the Clients at a Network Location Using the Insight App
- Monitor the Clients Connected to a Router Using the Cloud Portal
- Monitor the Clients Connected to a Router Using the Insight App
- Monitor VPN Groups in the Cloud Portal
- Monitor the VPN Groups on a Router Using the Insight App
- Monitor VPN Users With the Cloud Portal

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:

- **Summary**. 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.

- **Wireless**. 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 individual 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.

- **Wired**. 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 an individual switch, point to it and click the **pencil** icon at the right of the page.

- **Storage**. 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 an an individual ReadyNAS storage system, point to it and click the **pencil** icon at the right of the page.

- **Firmware**. 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.

- **Devices**. 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, type of device, MAC address, firmware version, IP address, and up time.

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

- **Clients**. 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 Widgets in the Cloud Portal

You can customize the Cloud Portal dashboard and pages. Depending on the Cloud Portal page, you can customize the following options:

- **Summary page for a network location**. To customize the widgets that display on the Summary page for a network location, click the **+ Add a Widget** button at the bottom of the page, select the widgets, and click the **Add** button. You can restore the default layout by clicking the **Restore Layout** button at the bottom of the page.
- **Wireless page and Wired page for a network location**. To customize the widgets that display on the Wireless page or Wired page for a network location, click the **...** (**Options**) button.
- **Tables in a widget**. To customize the columns that display in a table in a widget, click the **...** (**Options**) button *in* the widget.

Monitor All Network Locations Using the Cloud Portal

To display all network locations using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. If the network locations menu at the top of the page does not show All Locations, click the network locations menu and select **See All Locations**.

3. To search for a location, click the **Search** icon, enter the term that you want to search for, and click the **Search** button.
   If a match or matches are found, the page displays them.

4. To change the information that displays for each location on the page, click the **Options** icon, select the information that you want to display, and click the **Apply** button.
   The selected information displays for each location.

5. To switch between icon view (the default view) and list view, do one of the following:

   - **List view**. To show the locations in list view (that is, in a table), click the **Options** icon, click the **list view** icon, and click the **Apply** button.
     The locations display in a table.
   - **Icon view**. To show the locations as icons (the default view) with the logo and information listed in the icon, click the **Options** icon, click the **dotted square** icon, and click the **Apply** button.
     The locations display as icons.

Display All Devices at All Network Locations Using the Cloud Portal

To display all devices at all network locations using the Cloud Portal:

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

2. From the main menu at the top of the page, select **My Devices**.
   Headings for the network locations display.

3. Click **+** to the right of a network locations heading.
   The devices at the network location display.

4. To sort the table in a different order, click a table heading.

5. To filter devices, click the **Filter** icon, select the type or types of devices, and click the **Apply** button.
   Only the selected type or types of devices display on the page.

Monitor All Devices at a Single Network Location Using the Cloud Portal

To monitor all devices at a single network location using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select the network location.
   The Summary page for the network location displays.
3. Select **Devices** (that is, do *not* select My Devices from the main menu).
   The devices at the network location display.
4. To sort the table in a different order, click a table heading.
5. To filter devices, click the **Filter** icon, select the type or types of devices, and click the **Apply** button.
   Only the selected type or types of devices display on the page.
6. To search for a device, click the **Search** icon, enter the term that you want to search for, and click the **Search** button.
   If a match or matches are found, the page displays them.
7. To change the columns that display on the page, click the **Options** icon, select the columns that you want to display, and click the **Apply** button.
   The page display the selected columns.
8. To view details about a device, point to the device and click the **pencil** icon at the right of the page.
   The Summary page for the device displays.

Monitor a Single Network Location Using the Cloud Portal

To monitor a single network location using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
   By default, the Properties, System Health, Wireless Clients, Port Utilization, and Notifications widgets display.
   Optional widgets include Storage Utilization, Wireless Data Consumption, Switch Traffic Utilization (that is, the Wired Data Consumption widget), and PoE Power Utilization (that is, the PoE Power Usage widget).
3. To customize the data that displays in a widget or perform a task in a widget, do the following:
   - **Wireless Clients widget**. Select the radio band and the period over which data is displayed.
   - **Port Utilization widget**. Scroll horizontally through the port utilization for the switches at the network location.
   - **Notifications widget**. Share notifications by clicking the **mail tray** icon in the widget, entering one or more email addresses, and sending an email with notifications to the email addresses.
4. To customize the widgets and the page layout, do the following:
   - **Add optional widgets**. To add one or more optional widgets, click the **+ Add a widget** button at the bottom of the page, selects one or more widgets in the Widget pop-up window, and click the **Add** button.
   - **Rearrange widgets**. To rearrange a widget on the page, click the **dotted square** icon in the widget, and move the widget to another location on the page.
   - **Refresh data**. To refresh the data in a widget, click the **...** button in the widget, and from the pop-up menu, select **Refresh**.
   - **Remove a widget**. To remove a widget from the page, click the **...** button in the widget, and from the pop-up menu, select **Remove Widget**.

- **Restore the default widgets and layout**. To restore the default widgets and locations of the widgets on the page, click the **Restore Layout** button at the bottom of the page.

Monitor the Wired Network at a Location Using the Cloud Portal

To monitor the wired network at a 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.
   The page shows the Usage, PoE Power Usage, and Wired - Traffic, and Devices widgets.
4. To hide or show widgets on the page, click the **...** (Options) button, select or clear one or more widgets at the top of the page, and click the **Apply** button.
   By default, all available widgets display on the page.
5. To customize the data that displays in a widget or perform a task in a widget, do the following:
   - **PoE Power Usage**. Click the **Detailed View** button.
   - **Wired - Traffic**. Select the period over which data is displayed.
   - **Devices**. Click the **...** (Options) button, select or clear the buttons for columns that display in the table, and click the **Apply** button.
     You can also sort the table in a different order by clicking a table heading.

     Note: Using the Devices widget, you can also add, change, reboot, or delete a device. These tasks are described in detail in other sections in this manual.

Monitor the WiFi Network and SSIDs at a Location Using the Cloud Portal

To monitor the WiFi (wireless) network and SSIDs at a 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 **Wireless**.
   The Wireless page displays.
   The page shows the Usage : Clients, Usage : Traffic, Devices, and Client List widgets.
4. To hide or show widgets on the page, click the **...** (Options) button at the top of the page, select or clear one or more widgets, and click the **Apply** button.
   By default, all available widgets display on the page.
5. To customize the data that displays in a widget or perform a task in a widget, do the following:
   - **Usage : Clients**. Select the period over which data is displayed.
   - **Usage : Traffic**. Select the period over which data is displayed.
   - **Devices**. Click the **...** (Options) button, select or clear the buttons for columns that display in the table, and click the **Save** button.
     You can also sort the table in a different order by clicking a table heading.

     Note: Using the Devices widget, you can also add, change, reboot, or delete a device. These tasks are described in detail in other sections in this manual.

   - **Client List**. Click the **...** (Options) button, select or clear the buttons for columns that display in the table, and click the **Save** button.
     You can also sort the table in a different order by clicking a table heading.

6. To display information about the SSIDs at the WiFi network and about an individual SSID, do the following:
   a. At the top of the page, click the **Settings** button.
      The WiFi page display, showing the SSIDs that are set up in the WiFi network. Although you can change the configuration of the WiFi network from this page (see Manage the WiFi Network and SSIDs for a Location on page 115), this section of the manual describes the monitoring options for the WiFi network.
   b. To search for an SSID, click the **Search** icon and enter the term that you want to search for.
      If a match or matches are found, the page displays them.
   c. Click the **...** (Options) button, select or clear the buttons for columns that display in the table with SSIDs, and click the **Save** button.
   d. To view details about an SSID, point to the SSID and click the **pencil** icon at the right of the page.
      The Settings page for the SSID displays.
      Although you can change the configuration of the SSID from this page (see Manage the WiFi Network and SSIDs for a Location on page 115), this section of the manual describes the monitoring options for the SSID.

Monitor the Storage Network at a Location Using the Cloud Portal

To monitor the storage network at a 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 **Storage**.
   The Storage page displays.
   The page shows the Usage and Devices widgets.
4. If your network location includes more than one ReadyNAS storage device, select the device from the menu in the upper right of the Usage widget.
5. To change the information that is shown in the table, click the **...** (Options) button at the top right of the page, select or clear the buttons for columns that display in the table, and click the **Save** button.

6. To sort the table in a different order, click a table heading.

Monitor an Individual Switch and Individual Ports Using the Cloud Portal

To monitor an individual switch and individual ports 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 widget (also referred to as pane), point to the switch that you want to monitor, and click the **pencil** icon at the right of the page.
   The Summary page for the switch displays, showing port and device details.
   Although you can change the configuration of the switch from this page (see Manage Individual Switches on page 156), this section of the manual describes the monitoring options for the switch.
5. To display details about a switch feature, select an item from the menu on the left.
   The following menu items are specific to monitoring a switch:
   - **Connected Neighbors**. For each connected port, the page displays the neighbor name, neighbor IP address, neighbor MAC address, and VLAN ID for the port connection. To display details about a neighbor, see Step 7.
   - **Traffic**. Display the traffic usage over a period that you can select.
   - **Statistics**. Displays information about the temperature, CPU usage, transmitted (Tx) data, received (Rx) data, and fan status.
     To clear the counters, click the **Clear Counters** button.
   - **Notifications**. Displays the type of notification, details about the notification, and timestamp of the notification.
6. To share diagnostic information about the switch, click the **mail tray** (Share) icon at the top of the page, enter an email address, and send an email with the diagnostic information.

You can share diagnostic information by using the **mail tray** (Share) icon on the Summary, Connected Neighbors, Traffic, Statistics, or Notifications page for the switch.

7. To display details about an individual port and a connected neighbor, do the following:
   a. Click **Summary**.
   b. Click a port.
      The Overview and Neighbor Info panes display, showing details about the port and the connected neighbor.
   c. To share diagnostic information about the switch from the Summary page for the port, click the **mail tray** (Share) icon at the top of the page, enter an email address, and send an email with the information.

Monitor an Individual Access Point and Its Clients Using the Cloud Portal

To monitor an individual access point and its clients using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Wireless**.
   The Wireless page displays.
4. Scroll down to the Devices widget (also referred to as pane), point to the WiFi device that you want to monitor, and click the **pencil** icon at the right of the page.
   The Summary page for the WiFi device displays, showing the Channel Utilization and Client OS widgets and the Device Details pane.
   Although you can change the configuration of the WiFi device from this page (see Manage Individual Access Points on page 185), this section of the manual describes the monitoring options for the WiFi device.
5. To customize the data that displays in a widget, do the following:
   - **Channel Utilization**. Select the radio band and the period over which data is displayed.

- **Client OS**. Select the radio band.

6. To hide or show widgets on the page, click the **...** (Options) button, select or clear one or more widgets at the top of the page, and click the **Save** button.
   By default, both widgets display on the page.
7. To display details about a WiFi device feature, select an item from the menu on the left.
   The following menu items are specific to monitoring a WiFi device:
   - **Clients**. For each client, displays information about the type of device, access point name, SSID, operating system, MAC address, IP address, the number of transmitted (Tx) bytes, and the number of received (Rx) bytes, and RSSI.
     To sort the table in a different order, click a table heading.
   - **Statistics**. Displays information about the transmitted (Tx) data and received (Rx) data.
   - **Notifications**. Displays the type of notification, details about the notification, and timestamp of the notification.
8. To share diagnostic information about the access point, click the **mail tray** (Share) icon at the top of the page, enter an email address, and send an email with the diagnostic information.
   You can share diagnostic information by using the **mail tray** (Share) icon on the Summary, Statistics, or Notifications page for the access point.

Monitor an Individual ReadyNAS Storage System Using the Cloud Portal

To monitor an individual ReadyNAS storage system using the Cloud Portal:

1. Access the Insight Cloud Portal.
   All network locations display.
2. Select your network.
   The Summary page displays.
3. Select **Storage**.
   The Storage page displays.

4. Scroll down to the Devices widget (also referred to as pane), point to the ReadyNAS storage system that you want to monitor, and click the **pencil** icon at the right of the page.

   The Summary page for the ReadyNAS storage system displays, showing the Disk Overview and Device Details widgets.

   Although you can change the configuration of the ReadyNAS storage system from this page (see Manage Individual ReadyNAS Storage Systems on page 191), this section of the manual describes the monitoring options for the ReadyNAS storage system.

5. To see more information about the disk, click the **More** link in the Disk Overview widget.
6. To display details about a ReadyNAS storage system feature, select an item from the menu on the left.

   The following menu items are specific to monitoring a ReadyNAS storage system:

   - **Statistics**. Displays information about the disk temperature, CPU temperature, and fan speed.
   - **Notifications**. Displays the type of notification, details about the notification, and timestamp of the notification.

7. To share diagnostic information about the ReadyNAS storage system, click the **mail tray** (Share) icon at the top of the page, enter an email address, and send an email with the diagnostic information.

   You can share diagnostic information by using the **mail tray** (Share) icon on the Summary, Statistics, or Notifications page for the ReadyNAS storage system.

Monitor the Clients at a Network Location Using the Cloud Portal

To monitor the clients at 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 **Clients**.

The Clients page displays, showing for each client the type of device, access point name, SSID, operating system, MAC address, IP address, the number of transmitted (Tx) bytes, and the number of received (Rx) bytes, and RSSI.

4. To search for a client, click the **Search** icon, and enter the term that you want to search for.

   If a match or matches are found, the page displays them.

5. To change the information that is shown in the table, click the **...** (Options) button at the top right of the page, select or clear the buttons for columns that display in the table, and click the **Save** button.
6. To sort the table in a different order, click a table heading.

Monitor the Clients at a Network Location Using the Insight App

See how many clients are connected to your network location in the NETGEAR Insight app.

To monitor clients connected to a network location using the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. At the bottom, tap **Locations**.
3. If you set up more than one network in Insight, at the top of the page, select the network.

   The number of clients currently connected to the network appears next to the device image.

Monitor the Clients Connected to a Router Using the Cloud Portal

You can see which clients are connected to each individual router.

To monitor clients connected to your router using the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. Select **Routers**.

4. Scroll down to the Devices pane and double-click the router that you want to monitor.
5. Select **Connected Clients**.
   A list of all clients currently connected to the router displays.
6. To see more details about a client, next to its name, click **+**.

Monitor the Clients Connected to a Router Using the Insight App

You can see which clients are connected to each individual router.

To monitor clients connected to your router using the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network.
   The list of devices on your network displays.
3. Tap a router.
4. Tap **Connected Clients**.
   A list of all clients currently connected to the router displays.
5. To see more details about a client, next to its name, tap the down arrow.

Monitor VPN Groups in the Cloud Portal

You can check the status of your VPN groups in Insight.

To see the status of your VPN groups using the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. Select **Routers**.
4. At the top right, click the **Settings** button.
5. Select **VPN Groups**.
   A list of VPN groups on this router with the status of each connection in the group displays.

Monitor the VPN Groups on a Router Using the Insight App

You can monitor the connections of devices connected to your virtual private network (VPN) group.

To monitor your VPN group status using the NETGEAR Insight app:

1. Launch the NETGEAR Insight app.
2. If you set up more than one network in Insight, at the top of the page, select the network you want to monitor.
   The list of devices on your network displays.
3. Under the network name, tap a router.
4. Tap **VPN Group**.
   A list of the VPN groups on this router and the status of each connection in the group displays.

Monitor VPN Users With the Cloud Portal

You can check the status of individual virtual private network (VPN) users in Insight.

To see who's connected to your VPN using the Insight Cloud Portal:

1. Access the Insight Cloud Portal.
2. Select your network.
3. Select **Routers**.
4. At the top right, click the **Settings** button.
5. On the router page, select **VPN Users**.
   A list of the VPN users invited to this group and their status appears.

13

Perform Diagnostics and Troubleshooting

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:

- Use the Device Diagnostic Options in Insight
- Register New Products That Are Not Manageable in Insight
- Troubleshoot Connectivity Problems Between Your Device and Insight
- Check to See If the Insight App Can Recognize Your Device
- Reboot Your Device Using the Insight App
- Remove Your Device From the Network and Re-add It Using the Insight App
- Reset a Device to Factory Default Settings Using the Insight App
- Send Diagnostic Files From the Insight App to a NETGEAR Community Moderator
- View Your Product Support Information Using the Insight App
- Open a Technical Support Case For a Product Using the Insight App

Note: If you are an Insight Pro user, depending on your role, you might need to select your organization before you can select a network location. If applicable, the procedures in this chapter start with all network locations for an organization. If your Insight Pro role lets you select an organization, these procedures assume that you do so.

Use the Device Diagnostic Options in Insight

The diagnostics options that are available for an Insight managed device 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
- Perform a Cable Test on a Switch
- Share Diagnostic Information From a Device
- Reload the Last Saved Cloud Configuration on a Device

Configure Port Mirroring on a Switch

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.

Configure Port Mirroring on a Switch Using the Insight App 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.

Configure Port Mirroring on a Switch Using the Cloud Portal To configure port mirroring on a 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. Select **Port Mirroring**.
   The Port Mirroring page displays.
6. Click 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 clicking the ports.
8. Select the single destination port by clicking the port.
9. Click the **Apply** button.
   Your settings are saved.

Perform a Cable Test on a Switch

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.)

Perform a Cable Test on a Switch Using the Insight App 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: The cable test will disrupt connectivity to all devices on the selected port or ports for a few seconds. If you are performing a cable test on the port that connects the switch to the Internet, the switch will lose Internet connectivity and Insight will show the switch and devices that are connected to the switch as offline while the test is being performed.
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.

Perform a Cable Test on a Switch Using the Cloud Portal To perform a cable test on a 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. Select **Cable Test**.
   The Cable Test page displays.
6. Select one or more ports by clicking the ports.
7. Click the **Test Selected Ports** button.
   A warning displays: The cable test will disrupt connectivity to all devices on the selected port or ports for a few seconds. If you are performing a cable test on the port that connects the switch to the Internet, the switch will lose Internet connectivity and Insight will show the switch and devices that are connected to the switch as offline while the test is being performed.
8. Click the **Yes, Test the cable** button.
   The cable test starts. After a short period, the test results display.

Share Diagnostic Information From a Device

You can let the Insight 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.

Share Diagnostic Information From a Device Using the Insight App

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.

Share Diagnostic Information From a Device Using the Cloud Portal To share diagnostic information from 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 **Devices** (that is, do *not* select My Devices from the main menu).
   The page displays all devices at the network location.
4. Point to the device and click the **pencil** icon at the right of the page.
   The Summary page for the device displays.
5. Click the **mail tray** (Share) icon at the top of the page.
   The Share Diagnostics pop-up window opens
6. Enter an email address.
7. Click the **Send** button.
   Insight sends the email with diagnostics information and the pop-up window closes.

Reload the Last Saved Cloud Configuration on a Device

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.

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 52).

Note: For devices that are capable of being managed by Insight but that are no longer managed by Insight, any configuration changes that you saved through the local browser interface that occurred after the last saved configuration in the cloud are lost. Use the local browser interface to reapply these settings.

Reload the Last Saved Cloud Configuration on a Device Using the Insight App

To reload the last saved cloud configuration on 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 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.

Reload the Last Saved Cloud Configuration on a Switch Using the Cloud Portal

To reload the last saved cloud configuration on a 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 **Devices** (that is, do *not* select My Devices from the main menu).
   The page displays all devices at the network location.
4. Point to the device and click the **pencil** icon at the right of the page.
   The Summary page for the device displays.
5. Click the **Reload** icon at the top of the page.

The Reload Configuration pop-up window opens.

6. Click the **Yes, reload** button.
   A notification displays. The configuration is reloaded and the device is offline for a few minutes.

Register New Products That Are Not Manageable in Insight

Insight Managed Switches, Insight Managed Wireless Access Points, ReadyNAS OS 6 storage systems, and Orbi Pro WiFi Systems are automatically registered when you add them to a network location in Insight. For more information, see Discover, Add, and Register Devices on page 29.

You can register any product that is *not* manageable in Insight using the following methods:

- Register a Product Using the Insight App on page 221
- Register a Product Using the Cloud Portal on page 222

Register a Product Using the Insight App

Use this procedure only for a product that is *not* manageable in Insight.

To register a product using the Insight app:

1. Launch the Insight app.
2. Tap the menu button in the upper left corner of the screen.
3. Tap **Register Any NETGEAR Device**.
4. Do one of the following:
   - **Enter the serial number**. Enter the serial number of your device in the **Enter Serial Number** field and, to the right of the field, tap **GO**.
   - **Scan the barcode**. Do the following:
     a. Tap **Scan Barcode**.
     b. 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.
     c. To the right of the **Enter Serial Number** field, tap **GO**.

After the information is validated by the NETGEAR registration server, a confirmation displays.

Register a Product Using the Cloud Portal

Use this procedure only for a product that is *not* manageable in Insight.

To register a product 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 menu opens.
3. Select **Register Any Network Device**.
   The Register any NETGEAR Product pop-up window opens.
4. Enter the serial number of your device in the **Enter Serial Number**, and click the **Go** button.
   After the information is validated by the NETGEAR registration server, a confirmation displays.

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 system 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 223
2. Reboot Your Device Using the Insight App on page 224
3. Remove Your Device From the Network and Re-add It Using the Insight App on page 224
4. Reload the Last Saved Cloud Configuration on a Device Using the Insight App on page 220
5. Reset a Device to Factory Default Settings Using the Insight App on page 225

For more troubleshooting help, see the hardware installation guide (HIG) for your switch, access point, or ReadyNAS storage system. 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.

View Your Product Support Information Using the Insight App

Your can view product support information for your registered products, including entitlements, contracts, (support) cases, and return merchandise authorizations (RMAs).

To view your product support information using the Insight app:

1. Launch the Insight app.
   All organizations display.
2. Tap the menu button in the upper left corner of the screen.
3. Tap **Technical Support**.
4. Tap **Registered Products**.
   The registered products display.
5. Tap a product.
   Product information displays.

   In addition to tabs that let you select and view videos, articles, and community questions and responses, the following tabs provide specific support information:

   - **Entitlement**. Lists your hardware warranty information, chat support expiration date, phone support expiration date, and online support expiration date. For information about opening a chat, phone, or online support case, see Open a Technical Support Case For a Product Using the Insight App on page 228.
   - **Contracts**. List your support contracts, if any.
   - **Cases**. List the support cases that you opened, if any.
   - **RMA**. Lists the RMAs that you initiated and that were approved, if any.

6. To view all support cases that you opened, tap the **support case** icon in the upper right corner of the screen.
   The subject and status of each case displays.

Open a Technical Support Case For a Product Using the Insight App

You can open a support case for a registered product for which you are entitled support. You can use chat, online, or phone technical support.

To open a technical support case for a product using the Insight app:

1. Launch the Insight app.
   All organizations display.
2. Tap the menu button in the upper left corner of the screen.
3. Tap **Technical Support**.
4. Tap **Registered Products**.
   The registered products display.
5. Tap a product.
   Product information displays.
6. Open a support case using one of the following methods:
   - **Online**. To open an online case, do the following:
     a. Tap **Cases**.
     b. Tap **Create a Case**.
        A pop-up window opens.
     c. Enter the subject and the message, and tap **Send**.
        A confirmation displays and an email message is sent to the email address that is associated with your Insight account.
     d. Tap **Done**.
        The product information displays again.
   - **Chat**. To open a chat case, do the following:
     a. Tap **Entitlements**.
     b. Tap **Chat Support**.
        A chat window opens, providing you access to online support.

- **Phone**. To open a case over the phone, do the following:
  a. Tap **Entitlements**.
  b. Tap **Phone Support**.
     Phone numbers and support information display.
  c. Call a phone number to open a case.

7. To view all support cases that you opened, including the one you just opened, tap the **support case** icon in the upper right corner of the screen.
   The subject and status of each case displays.