NETGEAR®

User Manual

10G/Multi-Gigabit Dual WAN Pro Router with Insight Cloud Management

Model PR60X

August 2023
202-12670-01

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

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Do not use this device outdoors. The PoE source is intended for intra building connection only.

Applicable to 6 GHz devices only: Only use the device indoors. The operation of 6 GHz devices is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12670-01	August 2023	First publication.

Contents

Chapter 5 Manage the LAN and VLAN Settings

Chapter 6 Manage the Firewall and Security

Chapter 7 Monitor the Router and its Network

Chapter 8 Maintain the Router

Chapter 9 Manage IPSec VPN Tunnels

Chapter 10 Diagnostics and Troubleshooting

Appendix A Supplemental information

1

Introduction

This manual is for the NETGEAR 10G/Multi-Gigabit Dual WAN Pro Router with Insight Cloud Management Model PR60X.

Model PR60X is a router for small-to-medium sized businesses. This model provides features such as WAN redundancy, a basic firewall with the option to set up multiple traffic rules, IPSec site-to-site VPN, and VLAN capabilities with a DHCP server for each VLAN. Model PR60X is in this manual referred to as the router.

This manual describes the router's device user interface (UI). If you manage the router using the Insight Cloud Portal or Insight app, you can also use the device UI to manage the router. That is, these management methods are not mutually exclusive but complement each other. Changes to Insight are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to Insight.

This chapter contains the following sections:

Note: For more information about the topics that are covered in this manual, visit the support website at netgear.com/support/.

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. You can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this manual, you might need to update the firmware.

Additional documentation

The following documents are available at netgear.com/support/download/:

- Installation guide
- Hardware installation guide
- Datasheet

Router management in NETGEAR Insight is described in the NETGEAR knowledge base. See kb.netgear.com/000065768.

How to manage the router

For NETGEAR Insight Premium and Insight Pro subscribers, the router supports the NETGEAR Insight Cloud Portal and Insight app:

- **Insight Cloud Portal**: Lets you configure and manage the router through the portal of the Insight cloud-based management platform.
- **Insight app**: Lets you configure and manage the router from your iOS or Android mobile device and connects to the Insight cloud-based management platform.

You can also manage the router with the device UI. Management through the Insight cloud-based management platform and management through the device UI are not mutually exclusive but complement each other. Changes to Insight are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to Insight.

You can manage and monitor the router using the following methods:

- **Insight-only management**: You use only the Insight Cloud Portal or Insight app. However, if you wish, at any time, you can change to the hybrid management method.
- **Hybrid management**: Overall network management and monitoring is through the Insight Cloud Portal or Insight app and some configuration and management tasks are performed through the device UI.
- **Standalone management**: You use the router as a standalone device in your network and manage and monitor the router using the device UI only. However, if you wish, at any time, you can change to the hybrid management method. (You can also completely disable Insight if you only want to use the device UI.)

About the device UI and NETGEAR Insight

This user manual describes the router's device user interface (UI), and tasks that you can perform using the device UI.

For information about NETGEAR Insight subscriptions, visit netgear.com/business/services/insight/subscription and kb.netgear.com/000061848/.

This manual does not describe NETGEAR Insight procedures, which are documented in the NETGEAR knowledge base. For knowledge base articles about NETGEAR Insight, visit kb.netgear.com/000065768.

If you install the router as a NETGEAR Insight managed device and the Insight Mode is enabled, the settings for features that you can manage through the Insight Cloud portal and Insight app are automatically synchronized with the device UI, and the other way around. For more information, see How Insight and the device UI interact with each other on page 21.

2

Set Up and Access the Router

This chapter describes how you can connect the router to the Internet and how you can access and log in to the router, including basic setup information for Insight users and those who prefer to manage the router as a standalone device without Insight remote management.

The chapter contains the following sections:

Note: The procedures that are described in this chapter are for a network setup in which you do not use the Insight Cloud Portal or Insight app to pre-onboard the router. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, additional setup options are available to you. For knowledge base articles about NETGEAR Insight, visit kb.netgear.com/000065768.

Pre-onboard the router with Insight and plug-and-play

We recommend that NETGEAR Insight subscribers use Insight to onboard and configure the router. See kb.netgear.com/000065773.

Depending on the method that the ISP uses to assign an IP address, you can use the Insight Cloud Portal or Insight app to pre-onboard the router and then connect the router to the Internet at the local site. Insight configures the router, which then becomes operational so the basic setup is plug and play.

After onboarding, you can optionally change the default configuration settings through the Insight Cloud Portal or Insight app, or through the device UI.

Set up the router with an Internet connection

If you are not an Insight user and prefer to use the device UI to onboard the router, you can set up the router as either a primary or secondary router:

- **Primary router providing Internet access**. If the router is the only router in your network, connect the router directly to a modem, such as a DSL or cable modem that is connected to the Internet, and set up the Internet connection. See Set up the router to connect to a modem on page 14.
- **Secondary router connected to an existing LAN**. If another router provides the Internet connection, connect the router to the LAN of the other router and set up the Internet connection of the router. See Set up the router to connect to the LAN of an existing router on page 15.

Note: You can also set up the router offline by manually configuring the router before you install it in your network either as a primary or secondary router. For more information, see Set up the router offline using a directly connected computer on page 17.

Example of a router setup with a connection to a modem

The following example figure shows the router connected to a modem that is connected to the Internet:

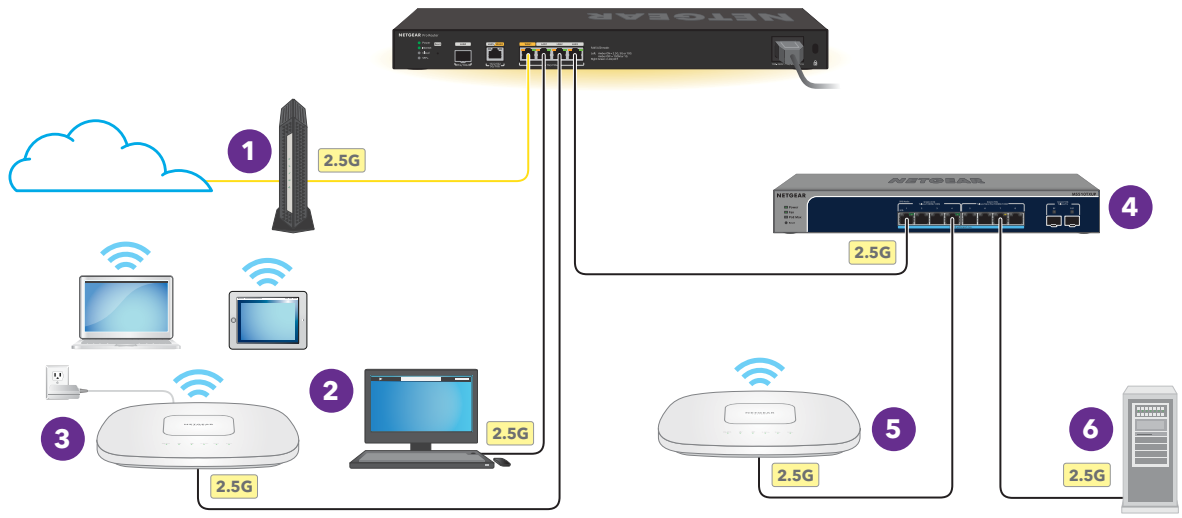

Figure 1. Example connections for a router setup with a connection to a modem

In this example, the following applies:

1. The WAN1 port of the router is connected to the modem, which is connected to the Internet.
2. Depending on the security settings, the wired desktop computer that is connected to the LAN1 port of the router can have access to the Internet.
3. The access point at the left side of the figure is connected to the LAN2 port of the router. Depending on the WiFi networks that are configured on the access point, the access point can provide Internet access to the mobile devices that are connected to it. The access point requires a power adapter because the router does not provide PoE.
4. A PoE switch is connected to the LAN3 port of the router.
5. The access point at the right side of the figure is connected to the PoE switch. Depending on the WiFi networks that are configured on the access point, the access point can provide Internet access to the mobile devices that are connected to the it. The access point does not require a power adapter because the switch provides PoE.
6. Depending on the security settings, the server that is connected to the switch can be accessible by users on the network.

Set up the router to connect to a modem

If the router is the only router in your network, connect the WAN1 port on the router directly to a modem, such as a DSL or cable modem that is connected to the Internet, and set up the Internet connection. After you physically connect the router, you can let the automated setup process configure your router automatically.

Before you start, locate your Internet service provider (ISP) configuration information. For DSL service, you might need the following information to set up the Internet connection for your router:

- The ISP configuration information for your DSL account.
- The ISP login name and password.
- Fixed or static IP address setting (special deployment by the ISP; this setting is rare).

The automated setup process runs on a computer with a web browser. Installation and basic setup takes about 15 minutes to complete.

To connect the router to a modem and use the automated setup process to automatically get an Internet connection:

1. Unplug the modem's power, leaving the modem connected to the wall jack for your Internet service.

   If the modem uses a battery backup, remove the battery.

2. Using an Ethernet cable, connect the modem to the yellow WAN1 port on the router.
3. Plug in and turn on the modem.

   If the modem uses a battery backup, put the battery back in before you turn on the modem.

4. Power on the router and check that the Power LED is lit.

   The Power LED lights solid amber for about one minute. When the router is ready, the Power LED lights solid green.

5. Connect your computer with an Ethernet cable to any of the router's LAN ports.

   Make sure that your computer is configured to obtain an IP address automatically using DHCP. This is the default configuration for most computers.

   The computer receives an IP address from the router.

   Note: If you configure a WiFi access point and connect it directly to a LAN port on the router, you can also use a WiFi connection to set up the router. The router itself does not provide WiFi capability or Power over Ethernet (PoE), so, in such a setup, you must use a power supply or PoE switch to power the access point.

6. Launch a web browser and enter **https://www.routerlogin.net** in the address field.
   You can also enter **https://192.168.1.1**, which is the default IP address of the router.

   Your browser might display a security warning because of the self-signed certificate on the router, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
   The automated setup process starts.

   When the router connects to the Internet, the Internet LED lights solid green.

7. Follow the prompts in the automated setup process to connect to the Internet.
   The automated setup process searches your Internet connection for servers and protocols to determine your Internet configuration.

8. You are also prompted to do the following:
   a. Set an admin password for local login.
   b. Select the time zone where the router operates.
   c. Update the router's firmware if a new firmware version is available.
      Follow the prompts to update the router's firmware. After you update the firmware, the router restarts.

   When the router connects to the Internet, the Internet LED lights solid green.

9. If the router does not connect to the Internet, do the following:
   a. Make sure that the Ethernet cable connection is secure at the router's yellow WAN1 port (do *not* use a LAN port for this connection) and at an Ethernet port on the modem.
   b. Review your settings. Make sure that you selected the correct options and typed everything correctly.
   c. Contact your ISP to verify that you are using the correct configuration information.

   If problems persist, register your product and contact NETGEAR technical support.

Set up the router to connect to the LAN of an existing router

If another router provides the Internet connection, connect the router to the LAN of the existing router and set up the Internet connection for the router.

After you physically connect the router, you can let the automated setup process configure your router automatically. By default, the DHCP client of the router is enabled so that the router receives an IP address from the other router in your network.

The automated setup process runs on a computer with a web browser. Installation and basic setup takes about 15 minutes to complete.

To connect the router to the LAN of an existing router and use the installation assistant to automatically get an Internet connection:

1. Using an Ethernet cable, connect the yellow WAN1 port on the router to a LAN port on a switch or hub that is connected to the LAN of the other router.

   You can also connect the Ethernet cable directly to a LAN port on the other router.

2. Power on the router and check that the Power LED is lit.

   The Power LED lights solid amber for about one minute. When the router is ready, the Power LED lights solid green.

3. Connect your computer with an Ethernet cable to any of the router's LAN ports.

   Make sure that your computer is configured to obtain an IP address automatically using DHCP. This is the default configuration for most computers.

   The computer receives an IP address from the router.

   Note: If you configure a WiFi access point and connect it directly to a LAN port on the router, you can also use a WiFi connection to set up the router. The router itself does not provide WiFi capability or Power over Ethernet (PoE), so, in such a setup, you must use a power supply or PoE switch to power the access point.

4. Launch a web browser and enter **https://www.routerlogin.net** in the address field.

   You can also enter **https://192.168.1.1**, which is the default IP address of the router.

   Your browser might display a security warning because of the self-signed certificate on the router, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980.
   The automated setup process starts.

   When the router connects to the Internet, the Internet LED lights solid green.

5. Follow the prompts in the automated setup process to connect to the Internet.

   The automated setup process searches your Internet connection for servers and protocols to determine your Internet configuration.

6. You are also prompted to do the following:
   a. Set an admin password for local login.
   b. Select the time zone where the router operates.
   c. Update the router's firmware if a new firmware version is available.
      Follow the prompts to update the router's firmware. After you update the firmware, the router restarts.

   When the router connects to the Internet, the Internet LED lights solid green.

7. If the router does not connect to the Internet, do the following:
   a. Make sure that the Ethernet cable connection is secure at the router's yellow WAN1 port (do *not* use a LAN port for this connection) and at an Ethernet port on the modem.
   b. Review your settings. Make sure that you selected the correct options and typed everything correctly.
   c. Contact your ISP to verify that you are using the correct configuration information.

   If problems persist, register your product and contact NETGEAR technical support.

Set up the router offline using a directly connected computer

You can set up the router offline (that is, disconnected from your network and the Internet), connect a computer through an Ethernet cable to a router LAN port, and connect to the router over its default IP address. After you complete the configuration, you can bring the router online, that is, connect it to your network and the Internet.

Note: We recommend that you only follow this procedure if you are comfortable with manually configuring the Internet settings.

To connect to the router offline using a computer that is connected to a router LAN port:

1. Use an Ethernet cable to connect your computer to a router LAN port on the router.
   You can use any LAN port. Do not use the yellow WAN1 port.
2. Power on the router and check that the Power LED is lit.
   The Power LED lights solid amber for about one minute. When the router is ready, the Power LED lights solid green.

   The computer receives an IP address from the router.
3. Launch a web browser and enter **https://www.routerlogin.net** in the address field.
   You can also enter **https://192.168.1.1**, which is the default IP address of the router.

   Your browser might display a security warning because of the self-signed certificate on the router, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see https://kb.netgear.com/000062980.
   The automated setup process starts. Because the router is not connected to the Internet, the autodetection fails (this is expected behavior).
4. Select the **No. Manually enter settings** radio button, and click the **Next** button.

A pop-up window displays.

5. Click the **OK** button.
6. You are prompted to do the following:
   a. Set an admin password for local login.
   b. Select the time zone where the router operates.
7. After the automated setup process finishes, if the login page does not display, enter **https://www.routerlogin.net** in the address field.

   You can also enter **https://192.168.1.1**, which is the default IP address of the router.

   Your browser might display a security warning because of the self-signed certificate on the router, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980. The login window displays.
8. Enter the router user name and password.

   The user name is **admin**. The password is the one that you set in Step 6. The user name and password are case-sensitive.

   The Dashboard displays.
9. Select **WAN > Internet/WAN > WAN1**.

   The Internet/WAN Setup page displays.
10. Select **IPv4**.

    The page displays the WAN options for the primary interface.
11. Configure the Internet settings.

    For more information, see Manage the Internet Settings for the WAN1 port on page 29.
12. Bring the router online by connecting it to your network and the Internet.
13. If the router does not connect to the Internet, do the following:
    a. Make sure that the Ethernet cable connection is secure at the router's yellow WAN1 port (do *not* use a LAN port for this connection) and at an Ethernet port on the modem or the switch or hub that is connected to the LAN of the other router.
    b. Review your settings. Make sure that you selected the correct options and typed everything correctly.
    c. If you use a modem, contact your ISP to verify that you are using the correct configuration information.

If problems persist, register your product and contact NETGEAR technical support.

Decide on the router management method

The router provides management options (which are *not* mutually exclusive) that let you add the router to your network and configure, monitor, and control the router:

- **NETGEAR Insight Cloud Portal**: As an Insight Premium or Pro user, you can use the NETGEAR Insight Cloud Portal to set up (pre-onboard) the router with in an Insight network. (Whether you can use pre-onboarding depends on the method that the ISP uses to assign an IP address.) After the router is connected to the Internet, you can perform advanced remote management, remotely monitor the router, remotely analyze the router and network usage, receive push notifications from the router, and, if necessary, remotely troubleshoot the router and the network. The time zone and device password for the router are set to those of the Insight network location.
  For more information, see Add the router to NETGEAR Insight using the Cloud Portal on page 23.
- **NETGEAR Insight mobile app**: You can use the NETGEAR Insight mobile app to set up (pre-onboard) the router in an Insight network. (Whether you can use pre-onboarding depends on the method that the ISP uses to assign an IP address.) After the router is connected to the Internet, you can manage and monitor the router remotely from your mobile device, and receive push notifications from the router. The time zone and device password for the router are set to those of the Insight network location.
  For more information, see Add the router to NETGEAR Insight using the Insight app on page 25.
- **Device UI**: If you do not use the pre-onboarding options that are available though the Insight Cloud Portal and Insight app, you must access the device UI to set up the WAN (Internet) connection and other settings of the router. You can then continue to use the device UI to configure, monitor, and control the router as a standalone router, or you can use the hybrid management method in which you use the Insight Cloud Portal or Insight app and the device UI.
  Management through the Insight cloud-based management platform and management through the device UI are not mutually exclusive but complement each other. Changes to Insight are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to Insight.

  Note: NETGEAR Insight remote management offers additional features and add-on services that are not available if you only use the device UI.

The router comes with Insight included. You can choose an Insight Premium or Insight Pro account. For more information, visit the following pages:

- netgear.com/business/services/insight/subscription/
- kb.netgear.com/000061848

Insight remote management

As a NETGEAR Insight Premium or Pro user, you can use NETGEAR Insight to pre-onboard the router. (Whether you can use pre-onboarding depends on the method that the ISP uses to assign an IP address.) After the router is connected to the Internet, you can remotely manage the router with the Insight Cloud portal or the Insight mobile app.

The following example figure shows the router connected to a modem that is connected to both the Internet and the (purple) Netgear cloud:

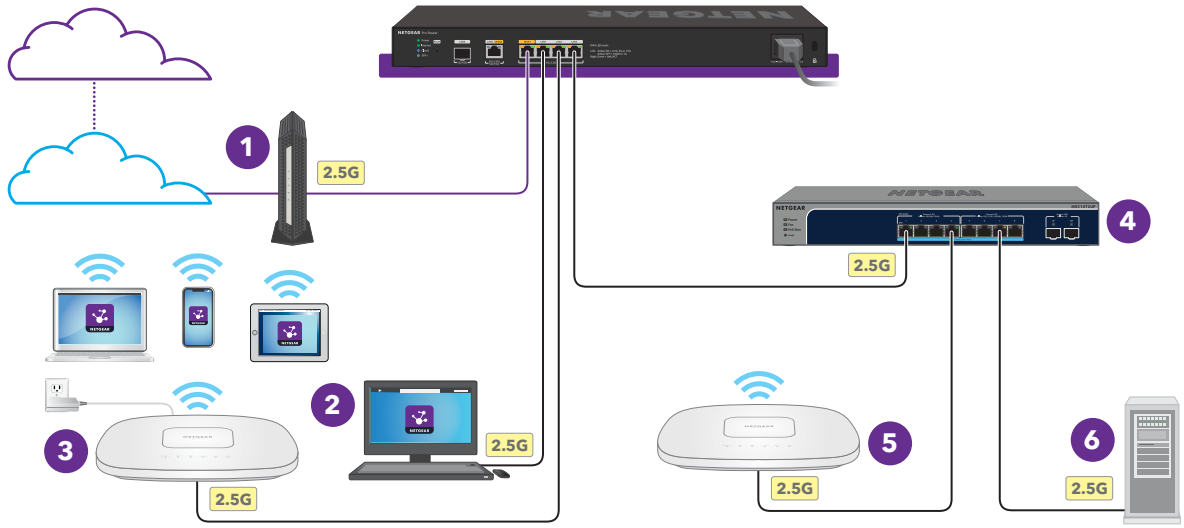

Figure 2. Example connections for a router setup with Insight remote management through the Cloud Portal or Insight app

In this example, the following applies:

1. The WAN1 port of the router is connected to the modem, which is connected to the Internet.
2. Depending on the security settings, the wired desktop computer that is connected to the LAN1 port of the router can have access to the Internet and access to the Insight Cloud Portal.
3. The access point at the left side of the figure is connected to the LAN2 port of the router. Depending on the WiFi networks that are configured on the access point,

the access point can provide Internet access to the mobile devices that are connected to it. The mobile devices cam have access to the Insight Cloud Portal or have the Insight app installed. The access point requires a power adapter because the router does not provide PoE.

4. A PoE switch is connected to the LAN3 port of the router.
5. The access point at the right side of the figure is connected to the PoE switch. Depending on the WiFi networks that are configured on the access point, the access point can provide Internet access to the mobile devices that are connected to the it. The mobile devices can have access to the Insight Cloud Portal or have the Insight app installed. The access point does not require a power adapter because the switch provides PoE.
6. Depending on the security settings, the server that is connected to the switch can be accessible by users on the network.

How Insight and the device UI interact with each other

If you manage the router using the Insight Cloud Portal or Insight app, you can *also* still use the device UI to manage the router. That is, these management methods are not mutually exclusive but complement each other. Changes to Insight are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to Insight.

Insight and the device UI interact with each other in the following ways:

- **Insight Mode enabled**: By default, Insight Mode is enabled in the device UI. When enabled, the Insight Mode can display one of the following states:
  - **Connected**: You added the router to an Insight network location. You can use either Insight or the device UI to manage the router. The device UI and Insight are synchronized with each other.
    When you add the router to an Insight network location, any preexisting device UI configuration is overwritten by the configuration on the Insight cloud.
    For information about how Insight affects the router admin password, see Credentials for the device UI on page 22.
  - **Not Registered**: You did not add the router to an Insight network location. The is the default setting for a standalone setup. Use the device UI to manage the router.

    Note: When the Insight Mode is Not Registered, Insight background services on the router remain in contact with the Insight cloud-based management platform.

  - **Disconnected**: You added the router to an Insight network location but the router does not yet have a connection to the Insight cloud (usually the Disconnected state changes quickly to Connected), or the router no longer has communication with the Insight cloud.
    If the router lost its connection to the Insight cloud, the router cannot synchronize with Insight. Any changes that you make in Insight are no longer synchronized with the device UI. Although you still can use the device UI to manage the router, any changes that you make in the device UI are no longer synchronized with Insight either. We recommend that you do not use the device UI in the Disconnected state because the absence of synchronization could cause unexpected behavior after the communication with the Insight cloud is restored.

- **Insight Mode disabled**: You disabled the Insight Mode. No Insight background services run on the router and the router stops all contact with the Insight cloud-based management platform. The results depend on whether you added the router to an Insight network location:
  - **You want to use only the device UI**: The Insight Mode is disabled and the router was not added to an Insight network location, so no Insight configuration exists for the router. Use the device UI to manage the router.
    If you later decide that you want to use the Insight Cloud Portal or Insight app, you can enable the Insight Mode.
  - **You already added the router to an Insight network location**: The router does not synchronize with Insight. Any changes that you make in Insight are not synchronized with the device UI. Any changes that you make in the device UI are not synchronized with Insight either. We do not recommend this configuration because the absence of synchronization could cause unexpected behavior if you reenable Insight Mode.

    Note: If you want to stop using Insight to manage the router, we recommend that you first remove the router from the Insight network location. The Insight Mode in the device UI returns to Not Registered.

For information about changing the Insight Mode, see Change the Insight management mode on page 26.

Credentials for the device UI

The information in this section applies to accessing the device UI. The way that you access the device UI depends on whether you onboard the router without using NETGEAR Insight, or if you onboarded it to NETGEAR Insight.

To access the device UI, use one of the following credentials:

- **You are using the device UI only: Use the router admin password**.
  You can access the device UI with your router admin password.
  The first time that you access the device UI, enter the default router admin password (**password**), after which you are required to customize the password for greater security. Subsequent times that you log in to the device UI, use your customized router admin password.
- **You are using both NETGEAR Insight and the device UI: Use the Insight network location password**.
  NETGEAR Insight can affect how you access the router device UI. If you keep the Insight mode in the device UI enabled (the default setting), *after* you add the router to an Insight network location, the Insight network location password replaces the router admin password for the device UI. To access the device UI, you must then enter the Insight network location password.
  Even if you then disable the Insight mode in the device UI, you must continue to use the Insight network location password to access the device UI. However, you can change the password in the device UI (see Change the admin user account password on page 131).
  For information about how the Insight network password functions and for knowledge base articles about NETGEAR Insight, visit kb.netgear.com/000065768.

The following table lists the essential credential options for access to the device UI.

Table 1. Credentials for access to the device UI

Management mode in the device UI	Added to an Insight network	Credentials
Insight Mode enabled (the default setting)	No	Device admin password
	Yes	Insight network password
Insight Mode disabled	No	Device admin password
	Yes[1]	Insight network password

1. This situation occurs if you disable the Insight mode after you already added the router to an Insight network location.

Add the router to NETGEAR Insight using the Cloud Portal

For Insight Pro users, one of the advantages of using the Insight Cloud Portal is that you can onboard multiple devices by entering the serial numbers and MAC addresses of the devices, or by uploading a device list as a CSV file.

Note: To onboard a single device, use the Insight app to scan the barcode or QR code. For more information see Add the router to NETGEAR Insight using the Insight app on page 25.

Your NETGEAR account is also your Insight account. Your NETGEAR account credentials let you log in as an Insight Premium user or Insight Pro user.

If you do not already have an Insight account, you can create an account now. For information about creating an Insight Premium account or upgrading to an Insight Pro account, visit netgear.com/000044343.

After the router is connected to the Internet, the router can communicate with the Insight cloud and you can add the router to an Insight managed network using the Insight Cloud Portal.

To add the router to NETGEAR Insight using the Cloud Portal:

1. On a computer or tablet, visit https://insight.netgear.com.
2. Enter the email address and password for your NETGEAR account and click the **NETGEAR Sign In** button.
3. Only if you are an Insight Pro user, select the organization to which you want to add the router.
4. Add a new network location where you want to add the router, or select an existing network location.
5. Click the **+ (Add Device)** button.

   Note: If you are an Insight Pro user, you can either add a single device or you can add multiple Insight managed devices by uploading a device list as a CSV file.

6. In the Add New Device pop-up page, enter the router's serial number and MAC address, and then click **Go**.

   The serial number and MAC address are printed on the router label and displayed on the Dashboard in the device UI.

7. After Insight verifies that the router is a valid product, you can optionally change the device name of the router, and then click **Next**.

   When the router is successfully added to the portal, a page displays a confirmation that setup is in progress.

   Note: If the router is online but Insight does not detect the router, a firewall at the physical location where the router is located might be preventing communication with the Insight cloud. In that situation, add port and DNS entries for outbound access to the firewall. For more information, see kb.netgear.com/000062467.

The router automatically updates to the latest Insight firmware and Insight location configuration. This might take up to 10 minutes, during which time the router will restart.

The router is now an Insight managed device that is connected to the Insight cloud-based management platform. The Cloud LED lights solid blue.

You can now use the Insight Cloud portal or Insight app to configure and manage the router.

Add the router to NETGEAR Insight using the Insight app

Your NETGEAR account is also your Insight account. Your NETGEAR account credentials let you log in as an Insight Premium user, or if you upgrade to an Insight Pro account, as an Insight Pro user.

If you do not already have an Insight account, you can create an account now. For information about creating an Insight Premium account or upgrading to an Insight Pro account, visit kb.netgear.com/000044343.

After the router is connected to the Internet, the router can communicate with the Insight cloud and you can add the router to an Insight managed network using the Insight app.

To add the router to NETGEAR Insight using the Insight app:

1. Connect your mobile device to the same network to which the router is connected.
2. Open the NETGEAR Insight app.
3. Enter the email address and password for your account and tap **LOG IN**.
4. Add a new network location where you want to add the router by tapping the **Next** button, and then tapping **OK**.

   You can also select an existing network location.

   The device admin password that you entered for the new network location replaces the existing admin password on all devices that you add to the network location.

   In most situations, Insight detects the router automatically, which can take several minutes.

5. To add the router to your network location, tap the **+** icon in the top bar, and do one of the following:

   - Tap the **SCAN BARCODE OR QR CODE** button, and then scan the router's code.
   - Tap the **Enter Serial Number** link, and then manually enter the router's serial number and MAC address.

   The serial number and MAC address are printed on the router label and displayed on the Dashboard in the device UI.

6. If prompted, name the router and tap the **Next** button.

   The router automatically updates to the latest Insight firmware and Insight location configuration. This might take up to 10 minutes, during which time the router will restart.

   The router is now an Insight-managed device that is connected to the Insight cloud-based management platform. The Cloud LED lights solid blue.

   You can now use the Insight app or Insight Cloud portal to configure and manage the router.

Change the Insight management mode

By default, the Insight management mode of the router is enabled so that you can add the router to an Insight network location and manage the router with the Insight Cloud Portal and the Insight app. You can also still use the device UI to manage the router. For more information, see How Insight and the device UI interact with each other on page 21.

You can disable the Insight management mode so that you can manage the router *only* from the device UI.

To change the Insight management mode:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. In the System Information pane, click the **Insight Mode** toggle to enable or disable the Insight mode:
   - **The toggle is blue and positioned to the right**: The Insight mode is enabled. This is the default setting.
   - **The toggle is gray and positioned to the left**: The Insight mode is disabled.

   A confirmation pop-up window displays.
5. Click the **Yes** button.
   Your settings are saved. The Insight mode is changed.

Log in to the device UI

After you set up the router and the router is connected to the Internet, you can view and change the router settings by connecting to the device UI.

Note: The first time that you access the router, the automated setup process starts. For more information, see Set up the router to connect to a modem on page 14 or Set up the router to connect to the LAN of an existing router on page 15. After you set up the router, the automated setup process no longer starts.

To log in to the device UI:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
   You can also connect your computer to a LAN port on the router.

   Note: If you configure a WiFi access point and connect it directly to a LAN port on the router, you can also use a WiFi connection to set up the router. The router itself does not provide WiFi capability or Power over Ethernet (PoE), so, in such a setup, you must use a power supply or PoE switch to power the access point.

2. In the address field of your browser, enter **https://www.routerlogin.net**.
   You can also enter **https://www.routerlogin.net** or **https://192.168.1.1**.

   Your browser might display a security warning because of the self-signed certificate on the router, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980//.

   The login page displays.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

3

Manage the Internet Settings for the WAN1 port

This chapter describes how you can view or manually change the Internet settings for the WAN1 port.

When you first set up and access the router with a web browser, the automated setup process detects the Internet connection. After you set up the router, you can view or manually change the Internet settings for the WAN1 port.

For information about setting up a dual WAN configuration with the WAN2 port in addition to the WAN1 port, see Set Up and Configure a Dual WAN Connection on page 37.

This chapter contains the following sections:

Note: The procedures that are described in this chapter are for a setup in which the router is installed as a standalone device in your network. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

Manually configure a dynamic Internet connection for the WAN1 port

You can manually configure an Internet connection with dynamic IP address settings for the WAN1 port. Use this setup if your ISP assigns the WAN IP address dynamically, or another router in your existing network does.

Before you start the configuration procedure, be sure that you have the dynamic IP address information that your ISP gave you.

To manually configure an Internet connection with dynamic IP address settings for the WAN1 port:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **WAN > Internet/WAN > WAN1**.
   The Internet/WAN Setup page displays.
5. Select **IPv4**.
   The page displays the options for the WAN1 port.
6. From the **Connection Type** menu, select **DHCP**.
   The page adjusts.

7. If your ISP requires you to use a specific device name, click the **Edit** button and change the router device name. Then, go back to the page for the WAN options for the WAN1 port.
8. If your ISP requires you to use a domain name, enter it in the **Domain Name** field.

   Note: The fields in the Internet IP Address section are masked because the information is automatically assigned by the DHCP server of the ISP or the other router in your network.

9. Select a radio button to specify how your domain name servers (DNS) are configured:
   - **Get Dynamically from ISP**: Your ISP assigns the DNS server IP addresses dynamically. This is the default setting.
   - **Use these DNS Servers**: Type the static IP addresses of the DNS 1 server, and if available, of the DNS 2 and DNS 3 servers.
10. If your ISP requires you to use a vendor class identifier (VCI) string, type it in the **Vendor Class Identifier String (Option 60)** field.
11. If your ISP requires you to use a client identifier (client ID) string, type it in the **Client Identifier String (Option 61)** field.
12. To configure advanced settings for the WAN1 port, select **Advanced**, and configure the following settings:
    - **Router MAC Address**: Select a radio button:
      - **Use Default MAC Address**: Use the default router MAC address that displays on the Dashboard page and the router label. This is the default setting.
      - **Use Computer MAC Address**: If the router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
      - **Use This MAC Address**: Type the MAC address in the **MAC Address** field.
    - **WAN VLAN Tag**: Depending on the requirements of your ISP, click the toggle to enable or disable the use of a WAN VLAG tag:
      - **The toggle is blue and positioned to the right**: Your ISP requires you to use a WAN VLAN for the DHCP connection. Type the VLAN ID in the **WAN VLAN Tag** field.
      - **The toggle is gray and positioned to the left**: No WAN VLAN ID is required. This is the default setting.

- **MTU**: Select a radio button:
  - **Auto**: Your ISP assign the MTU size automatically. In most situations, the default size is 1500 bytes.
  - **Manual**: If your ISP requires you to use a specific MTU size, select the **Manual** button and type the size in the **MTU Size** field.

13. Click the **Apply** button.
    Your settings are saved.
    It might take a few minutes before the WAN1 port is connected to your ISP.

Manually configure a static Internet connection for the WAN1 port

You can manually configure an Internet connection with static (fixed) IP address settings for the WAN1 port.

Before you start the configuration procedure, be sure that you have the static IP address information that your ISP gave you.

To manually configure an Internet connection with static IP address settings for the WAN1 port:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **WAN > Internet/WAN > WAN1**.
   The Internet/WAN Setup page displays.
5. Select **IPv4**.
   The page displays the options for the WAN1 port.
6. From the **Connection Type** menu, select **Static**.
   The page adjusts.
7. In the **IP Address**, **Subnet Mask**, and **Gateway** fields, type the static IP address, subnet mask, and gateway IP address that you r ISP gave you.
   The gateway is the ISP gateway to which your router connects.
8. In the **DNS 1** field, type the static IP addresses of the DNS 1 server, and if available, in the **DNS 2** and **DNS 3** fields type the IP addresses of the DNS 2 and DNS 3 servers.
   Your ISP gave you the IP addresses of the DNS servers.
9. To configure advanced settings for the WAN1 port, select **Advanced**, and configure the following settings:
   - **Router MAC Address**: Select a radio button:
     - **Use Default MAC Address**: Use the default router MAC address that displays on the Dashboard page and the router label. This is the default setting.
     - **Use Computer MAC Address**: If the router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
     - **Use This MAC Address**: Type the MAC address in the **MAC Address** field.
   - **WAN VLAN Tag**: Depending on the requirements of your ISP, click the toggle to enable or disable the use of a WAN VLAG tag:
     - **The toggle is blue and positioned to the right**: Your ISP requires you to use a WAN VLAN for the static connection. Type the VLAN ID in the **WAN VLAN Tag** field.
     - **The toggle is gray and positioned to the left**: No WAN VLAN ID is required. This is the default setting.

- **MTU**: Select a radio button:
  - **Auto**: Your ISP assign the MTU size automatically. In most situations, the default size is 1500 bytes.
  - **Manual**: If your ISP requires you to use a specific MTU size, select the **Manual** button and type the size in the **MTU Size** field.

10. Click the **Apply** button.
    Your settings are saved.
    It might take a few minutes before the WAN1 port is connected to your ISP.

Manually configure a PPPoE Internet connection for the WAN1 port

You can manually configure a PPPoE Internet connection for the WAN1 port.

Before you start, be sure that you have the PPPoE information that your ISP gave you.

To manually configure a PPPoE Internet connection for the WAN1 port:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.
   The Dashboard displays.
4. Select **WAN > Internet/WAN > WAN1**.

The Internet/WAN Setup page displays.

5. Select **IPv4**.
   The page displays the options for the WAN1 port.
6. From the **Connection Type** menu, select **PPPoE**.
7. Configure the following settings:
   - **Username**: Type the user name that your ISP gave you. The user name is often an email address.
   - **Password**: Type the password that you use to log in to your PPPoE service.
   - **Service Name (Optional)**: If your ISP requires a service name, type it in the field.
8. **Connection Mode**: Select the **Always On** (the default setting) or **Manually Connect** radio button.
   Connecting manually means that you do not have an Internet connection unless you manually connect to your ISP.
9. Select a radio button to specify how your IP address is configured:
   - **Get Dynamically from ISP**: Your ISP assigns the IP address dynamically. This is the default setting.
   - **Use Static IP address**: Your ISP assigns a static (fixed) IP address, which you must type in the **IP Address** field.
10. Select a radio button to specify how your domain name servers (DNS) are configured:
    - **Get Dynamically from ISP**: Your ISP assigns the DNS server IP addresses dynamically. This is the default setting.
    - **Use these DNS Servers**: Type the static IP addresses of the DNS 1 server, and if available, of the DNS 2 and DNS 3 servers.
11. To configure advanced settings for the WAN1 port, select **Advanced**, and configure the following settings:
    - **Router MAC Address**: Select a radio button:
      - **Use Default MAC Address**: Use the default router MAC address that displays on the Dashboard page and the router label. This is the default setting.
      - **Use Computer MAC Address**: If the router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
      - **Use This MAC Address**: Type the MAC address in the **MAC Address** field.

- **WAN VLAN Tag**: Depending on the requirements of your ISP, click the toggle to enable or disable the use of a WAN VLAG tag:
  - **The toggle is blue and positioned to the right**: Your ISP requires you to use a WAN VLAN for the PPPoE connection. Type the VLAN ID in the **WAN VLAN Tag** field.
  - **The toggle is gray and positioned to the left**: No WAN VLAN ID is required. This is the default setting.
- **MTU**: Select a radio button:
  - **Auto**: Your ISP assign the MTU size automatically. In most situations, the default size is 1500 bytes.
  - **Manual**: If your ISP requires you to use a specific MTU size, select the **Manual** button and type the size in the **MTU Size** field.

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

    It might take a few minutes before the WAN1 port is connected to your ISP.

4

Set Up and Configure a Dual WAN Connection

This chapter describes how you can set up a dual WAN connection with failover in which one WAN port functions as the primary interface and the other WAN port functions as a secondary interface.

This chapter contains the following sections:

Note: The procedures that are described in this chapter explain how to manage configuration options through the device UI. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

About Dual WAN and WAN failover

Dual WAN is a configuration in which two WAN ports are connected to the Internet. WAN failover means that if one WAN port goes down, the other WAN port can take over. Only *one* WAN connection is up at any time.

One WAN port functions as the primary interface, and the other WAN port functions as the secondary or backup interface. If the primary interface goes down (for example, your ISP has an outage), the router can automatically switch (that is, *failover*) to the secondary WAN interface. When the primary WAN interface comes back up again, the router can automatically switch back from the secondary WAN interface to the primary WAN interface.

The router can support two WAN ports:

- **WAN1 port**: The default WAN port for the router is the WAN1 port.
- **LAN5 WAN2 port**: The LAN5 WAN2 port functions by default as a LAN port, but you can configure the port as the WAN2 port. If you set the LAN5 WAN2 port to function as a WAN port, the port no longer functions as a LAN port. That is, the port either functions as the LAN5 port (the default setting) or as the WAN2 port, but not as both simultaneously.

Ideally, each WAN port is connected to a different ISP. For example, you could connect the WAN1 port over a cable modem to one ISP and connect the WAN2 port over a mobile router with a 5G connection to another ISP.

In a dual WAN configuration, by default the WAN1 port is set as the primary interface and the WAN2 port is set as the secondary interface. However, you can change the settings so that the WAN2 port functions as the primary interface and the WAN1 port as the secondary interface.

These are the high-level steps to set up a dual WAN configuration with failover:

1. Be sure that you have two WAN connections, one for each WAN interface. The WAN1 port supports a speed of up to 2.5 Gbps. The WAN2 port supports a speed of up to 10 Gbps.
2. Configure dual WAN by changing the function of the LAN5 WAN2 port to a WAN port and configure the WAN2 port. Depending on the type of Internet connection for your WAN2 port, see one of the following sections:
    - **Dynamic connection**: Configure dual WAN with a dynamic Internet connection for the WAN2 port on page 39
    - **Static connection**: Configure dual WAN with a static Internet connection for the WAN2 port on page 42

- **PPPoE connection**: Configure dual WAN with a PPPoE Internet connection for the WAN2 port on page 45

3. Configure dual WAN failover and the type of failover detection (see Configure dual WAN failover detection on page 48).

Configure dual WAN with a dynamic Internet connection for the WAN2 port

By default, the LAN5 WAN2 port functions as a LAN port. You can change the function of the port to a WAN port (the WAN2 port) and set up a dynamic ISP connection for the WAN2 port.

Before you start, be sure that you have the dynamic IP address information that your ISP gave you. This information is different from the information for the WAN1 port.

To configure dual WAN with a dynamic Internet connection for the WAN2 port:

1. Prepare the modem or mobile router that you want to use for the WAN2 port connection:
   - **Modem**: Unplug the modem's power, leaving the modem connected to the wall jack for your Internet service.
     If the modem uses a battery backup, remove the battery.
   - **Mobile router**: Unplug the mobile router's power.
     If the mobile router uses a battery backup, remove the battery.
2. Using an Ethernet cable, connect the modem or mobile router to the WAN2 port on the router.
   The port is labeled LAN5 WAN2.
3. Plug in and turn on the modem or mobile router.
   If the modem or mobile router uses a battery backup, put the battery back in before you turn on the modem or mobile router.
4. If the router is not yet powered on, power on the router and check that the LEDs are lit.
   When you power on the router, the Power LED lights solid amber for about one minute. When the router is ready, the Power LED lights solid green.
5. Launch a web browser from a computer or mobile device that is connected to the router network.
6. In the address field of your browser, enter **https://www.routerlogin.net**.

The login page displays.

Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

7. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
8. Select **WAN > Internet/WAN > WAN2**.

   The Internet/WAN Setup page displays. The page displays the option to convert the LAN5 port to the WAN2 port.
9. Click the toggle to convert the LAN5 port to the WAN2 port:
   - **The toggle is blue and positioned to the right**: The port functions as the WAN2 port. The page adjusts to display menu options.
   - **The toggle is gray and positioned to the left**: The port functions as the LAN5 port. This is the default setting.
10. Select **IPv4**.

    The page displays the options for the WAN2 port.
11. From the **Connection Type** menu, select **DHCP**.

    The page adjusts.
12. If your ISP requires you to use a specific device name, click the **Edit** button and change the router device name. Then, go back to the page for the options of the WAN2 port.
13. If your ISP requires you to use a domain name, enter it in the **Domain Name** field.

Note: The fields in the Internet IP Address section are masked because the information is automatically assigned by the DHCP server of the ISP or the other router in your network.

14. Select a radio button to specify how your domain name servers (DNS) are configured:
    - **Get Dynamically from ISP**: Your ISP assigns the DNS server IP addresses dynamically. This is the default setting.
    - **Use these DNS Servers**: Type the static IP addresses of the DNS 1 server, and if available, of the DNS 2 and DNS 3 servers.
15. If your ISP requires you to use a vendor class identifier (VCI) string, type it in the **Vendor Class Identifier String (Option 60)** field.
16. If your ISP requires you to use a client identifier (client ID) string, type it in the **Client Identifier String (Option 61)** field.
17. To configure advanced settings for the WAN2 port, select **Advanced**, and configure the following settings:
    - **Router MAC Address**: Select a radio button:
      - **Use Default MAC Address**: Use the default router MAC address that displays on the Dashboard page and the router label. This is the default setting.
      - **Use Computer MAC Address**: If the router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
      - **Use This MAC Address**: Type the MAC address in the **MAC Address** field.
    - **WAN VLAN Tag**: Depending on the requirements of your ISP, click the toggle to enable or disable the use of a WAN VLAG tag:
      - **The toggle is blue and positioned to the right**: Your ISP requires you to use a WAN VLAN for the DHCP connection. Type the VLAN ID in the **WAN VLAN Tag** field.
      - **The toggle is gray and positioned to the left**: No WAN VLAN ID is required. This is the default setting.
    - **MTU**: Select a radio button:
      - **Auto**: Your ISP assign the MTU size automatically. In most situations, the default size is 1500 bytes.
      - **Manual**: If your ISP requires you to use a specific MTU size, select the **Manual** button and type the size in the **MTU Size** field.
18. Click the **Apply** button.

    Your settings are saved.

    It might take a few minutes before the WAN2 port is connected to your ISP.

19. To display the status of the dual WAN configuration, see Display the status of the dual-WAN interfaces on page 50.

Configure dual WAN with a static Internet connection for the WAN2 port

By default, the LAN5 WAN2 port functions as a LAN port. You can change the function of the port to a WAN port (the WAN2 port) and set up a static ISP connection for the WAN2 port.

Before you start, be sure that you have the static IP address information that your ISP gave you. This information is different from the information for the WAN1 port.

To configure dual WAN with an ISP connection that uses a static IP address for the WAN2 port:

1. Prepare the modem or mobile router that you want to use for the WAN2 port connection:
   - **Modem**: Unplug the modem's power, leaving the modem connected to the wall jack for your Internet service.
     If the modem uses a battery backup, remove the battery.
   - **Mobile router**: Unplug the mobile router's power.
     If the mobile router uses a battery backup, remove the battery.
2. Using an Ethernet cable, connect the modem or mobile router to the WAN2 port on the router.
   The port is labeled LAN5 WAN2.
3. Plug in and turn on the modem or mobile router.
   If the modem or mobile router uses a battery backup, put the battery back in before you turn on the modem or mobile router.
4. If the router is not yet powered on, power on the router and check that the LEDs are lit.
   When you power on the router, the Power LED lights solid amber for about one minute. When the router is ready, the Power LED lights solid green.
5. Launch a web browser from a computer or mobile device that is connected to the router network.
6. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

7. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
8. Select **WAN > Internet/WAN > WAN2**.

   The Internet/WAN Setup page displays. The page displays the option to convert the LAN5 port to the WAN2 port.
9. Click the toggle to convert the LAN5 port to the WAN2 port:
   - **The toggle is blue and positioned to the right**: The port functions as the WAN2 port. The page adjusts to display menu options.
   - **The toggle is gray and positioned to the left**: The port functions as the LAN5 port. This is the default setting.
10. Select **IPv4**.

    The page displays the options for the WAN2 port.
11. From the **Connection Type** menu, select **Static**.

    The page adjusts.
12. In the **IP Address**, **Subnet Mask**, and **Gateway** fields, type the static IP addresses, subnet mask, and gateway IP address that your ISP gave you.

    The gateway is the ISP gateway to which your router connects.
13. In the **DNS 1** field, type the static IP addresses of the DNS 1 server, and if available, in the **DNS 2** and **DNS 3** fields type the IP addresses of the DNS 2 and DNS 3 servers.

    Your ISP gave you the IP addresses of the DNS servers.

14. To configure advanced settings for the WAN2 port, select **Advanced**, and configure the following settings:

    - **Router MAC Address**: Select a radio button:
        - **Use Default MAC Address**: Use the default router MAC address that displays on the Dashboard page and the router label. This is the default setting.
        - **Use Computer MAC Address**: If the router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
        - **Use This MAC Address**: Type the MAC address in the **MAC Address** field.
    - **WAN VLAN Tag**: Depending on the requirements of your ISP, click the toggle to enable or disable the use of a WAN VLAG tag:
        - **The toggle is blue and positioned to the right**: Your ISP requires you to use a WAN VLAN for the DHCP connection. Type the VLAN ID in the **WAN VLAN Tag** field.
        - **The toggle is gray and positioned to the left**: No WAN VLAN ID is required. This is the default setting.
    - **MTU**: Select a radio button:
        - **Auto**: Your ISP assign the MTU size automatically. In most situations, the default size is 1500 bytes.
        - **Manual**: If your ISP requires you to use a specific MTU size, select the **Manual** button and type the size in the **MTU Size** field.

15. Click the **Apply** button.

    Your settings are saved.

    It might take a few minutes before the WAN2 port is connected to your ISP.

16. To display the status of the dual WAN configuration, see Display the status of the dual-WAN interfaces on page 50.

Configure dual WAN with a PPPoE Internet connection for the WAN2 port

By default, the LAN5 WAN2 port functions as a LAN port. You can change the function of the port to a WAN port (the WAN2 port) and set up a PPPoE ISP connection for the WAN2 port.

Before you start, be sure that you have the PPPoE information that your ISP gave you. This information is different from the information for the WAN1 port.

To configure dual WAN with an ISP connection that uses a PPPoE IP address for the WAN2 port:

1. Prepare the modem or mobile router that you want to use for the WAN2 port connection:
   - **Modem**: Unplug the modem's power, leaving the modem connected to the wall jack for your Internet service.
     If the modem uses a battery backup, remove the battery.
   - **Mobile router**: Unplug the mobile router's power.
     If the mobile router uses a battery backup, remove the battery.
2. Using an Ethernet cable, connect the modem or mobile router to the WAN2 port on the router.
   The port is labeled LAN5 WAN2.
3. Plug in and turn on the modem or mobile router.
   If the modem or mobile router uses a battery backup, put the battery back in before you turn on the modem or mobile router.
4. If the router is not yet powered on, power on the router and check that the LEDs are lit.
   When you power on the router, the Power LED lights solid amber for about one minute. When the router is ready, the Power LED lights solid green.
5. Launch a web browser from a computer or mobile device that is connected to the router network.
6. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

7. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
8. Select **WAN > Internet/WAN > WAN2**.

   The Internet/WAN Setup page displays. The page displays the option to convert the LAN5 port to a WAN port (WAN2).
9. Click the toggle to convert the LAN5 port to the WAN2 port:
   - **The toggle is blue and positioned to the right**: The port functions as the WAN2 port. The page adjusts to display menu options.
   - **The toggle is gray and positioned to the left**: The port functions as the LAN5 port. This is the default setting.
10. Select **IPv4**.

    The page displays the options for the WAN2 port.
11. From the **Connection Type** menu, select **PPPoE**.

    The page adjusts.
12. Configure the following settings:
    - **Username**: Type the user name that your ISP gave you. The user name is often an email address.
    - **Password**: Type the password that you use to log in to your PPPoE service.
    - **Service Name (Optional)**: If your ISP requires a service name, type it in the field.
13. **Connection Mode**: Select the **Always On** (the default setting) or **Manually Connect** radio button.

    Connecting manually means that you do not have an Internet connection unless you manually connect to your ISP.

14. Select a radio button to specify how your IP address is configured:
    - **Get Dynamically from ISP**: Your ISP assigns the IP address settings dynamically. This is the default setting.
    - **Use Static IP address**: Your ISP assigns a static (fixed) IP address, which you must type in the **IP Address** field.

15. Select a radio button to specify how your domain name servers (DNS) are configured:
    - **Get Dynamically from ISP**: Your ISP assigns the DNS server IP addresses dynamically. This is the default setting.
    - **Use these DNS Servers**: Type the static IP addresses of the DNS 1 server, and if available, of the DNS 2 and DNS 3 servers.

16. To configure advanced settings for the WAN2 port, select **Advanced**, and configure the following settings:
    - **Router MAC Address**: Select a radio button:
      - **Use Default MAC Address**: Use the default router MAC address that displays on the Dashboard page and the router label. This is the default setting.
      - **Use Computer MAC Address**: If the router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
      - **Use This MAC Address**: Type the MAC address in the **MAC Address** field.
    - **WAN VLAN Tag**: Depending on the requirements of your ISP, click the toggle to enable or disable the use of a WAN VLAG tag:
      - **The toggle is blue and positioned to the right**: Your ISP requires you to use a WAN VLAN for the DHCP connection. Type the VLAN ID in the **WAN VLAN Tag** field.
      - **The toggle is gray and positioned to the left**: No WAN VLAN ID is required. This is the default setting.
    - **MTU**: Select a radio button:
      - **Auto**: Your ISP assign the MTU size automatically. In most situations, the default size is 1500 bytes.
      - **Manual**: If your ISP requires you to use a specific MTU size, select the **Manual** button and type the size in the **MTU Size** field.

17. Click the **Apply** button.

Your settings are saved.

It might take a few minutes before the WAN2 port is connected to your ISP.

18. To display the status of the dual WAN configuration, see Display the status of the dual-WAN interfaces on page 50.

Configure dual WAN failover detection

Failover detection is the mechanism that lets the router detect if the primary WAN interface is up. If the interface is down, the router initiates a failover to the secondary WAN interface. The router then monitors both WAN interfaces and when the primary WAN interface comes back up, failover detection lets the router switch back to the primary WAN interface.

By default the WAN1 port is set as the primary interface and the WAN2 port is set as the secondary interface. However, you can change the setting so that the WAN2 port functions as the primary interface and the WAN1 port as the secondary interface.

The router supports the following types of failover detection:

- **Ping the WAN DNS server**: The router sends pings to the DNS servers that are already configured for the primary and secondary interfaces.
- **Ping the WAN gateway**: The router sends pings to the gateways that are already configured for the primary and secondary interfaces.
- **Ping custom IP addresses**: The router sends pings to custom gateways that you must configure for the primary and secondary interfaces.
- **Query the WAN DNS server**: The router sends DNS queries to the DNS servers that are already configured for the primary and secondary interfaces.
- **Query custom IP addresses**: The router sends DNS queries to custom DNS servers that you must configure for the primary and secondary interfaces.

In a WAN failover configuration with two WAN interfaces, if a query or ping does not yield a response after the specified number of retries (the default is four retries), the router automatically switches to the active interface. This process is referred to as a *failover*.

For example, if four queries to the WAN1 port fail, the router automatically switches to the WAN2 port. After the failover, the router continues to sends queries or pings to the WAN1 port. If the WAN1 port comes back up and responds to a query or ping, the router switches back to the WAN1 port.

To configure failure detection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **WAN > Internet/WAN > Dual WAN**.

   The Internet/WAN Setup page displays. The page displays the status information.
5. Select **Configuration**.

   The page displays the failure detection options.

   The selection from the Policy menu is Failover, which is the only option. (The router does not support load-balancing.)
6. From the **Primary WAN** menu, select **WAN1** or **WAN2**.

   The selected interface functions as the primary WAN interface in the dual WAN configuration.

   The selection from the Secondary WAN menu is automatically adjusted because there are only two WAN interfaces.
7. From the **Failure Detection Method** menu, select the failure detection method and select where the router must send the ping or query:

   - **ping**: The router sends pings to the device that you select:
     - **Use WAN DNS**: The router sends pings to the DNS server IP addresses that you already configured for the WAN1 and WAN2 ports.

  - **Use WAN Gateway:** The router sends pings to the gateway IP addresses that you already configured for the WAN1 and WAN2 ports.
  - **Use WAN Custom**: The router sends pings to custom IP addresses that you must enter in the IP address fields in the WAN1 Internet Connection Test and WAN2 Internet Connection Test sections.

- **DNS lookup**:
  - **Use WAN DNS**: The router sends queries to the DNS server IP addresses that you already configured for the WAN1 and WAN2 ports.
  - **Use WAN Custom**: The router sends queries to custom IP addresses that you must enter in the IP address fields in the WAN1 Internet Connection Test and WAN2 Internet Connection Test sections.

8. If you select the **Use WAN Custom** radio button in the previous step, type the IP addresses in the **IP Address 1** and **IP Address 2** fields in both the WAN1 Internet Connection Test and WAN2 Internet Connection Test sections.
9. In the **Retry Interval** field, type the period in seconds after which the router sends a query or ping to the WAN1 and WAN2 ports to determine their status (up or down).
   By default, the period is 5 seconds. The range is from 1 to 3500 seconds.
10. In the **Number of retries** field, enter the number of times that the router resends a query or ping after it did not receive a response from the WAN1 or WAN2 ports.
    The default number of retries is 5. That means that after five failed responses, the router fails over to the active interface. For example, if four queries to the WAN1 port fail, the router automatically fails over to the WAN2 port. The range is from 1 to 10 retries.
11. Click the **Apply** button.
    Your settings are saved.
12. To display the status of the dual WAN configuration, see Display the status of the dual-WAN interfaces on page 50.

Display the status of the dual-WAN interfaces

The status of the dual-WAN connection indicates the WAN port that functions as the primary interface and the link status of each WAN interface.

If no failover occurs, the WAN port that you selected as the primary Internet interface is the active interface and the other port is the secondary Internet interface. Under normal conditions, each interface is online.

If the primary WAN interface goes down, a failover occurs, and the secondary WAN interface becomes the active interface. The link status for the primary WAN interface shows as offline.

When the primary WAN interface comes back up, the router switches back to the primary WAN interface, which once again becomes the active interface.

To display the status of the dual-WAN interfaces:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **WAN > Internet/WAN > Dual WAN**.

   The Internet/WAN Setup page displays. The page displays the status information.
5. If the status fields do not display, select **Status**.

   The page displays the dual WAN status information.

   - **Dual-WAN Policy**: Failover, which is the only option.
   - **Primary Internet Interface**: The WAN port that you selected as the primary interface.
   - **Secondary Internet Interface**: The WAN port that is automatically selected as the secondary WAN interface based on your selection of the primary WAN interface.

- **Active Internet Interface**: The WAN port that is the active WAN interface.
- **WAN1 Connection Status**: Depending on the status, this field either displays *online/Active* and shows the number of seconds in the Uptime field or displays *offline*.
- **WAN2 Connection Status**: Depending on the status, this field either displays *online/Active* and shows the number of seconds in the Uptime field or displays *offline*.

5

Manage the LAN and VLAN Settings

This chapter describes how you can manage the local area network (LAN) and virtual LAN (VLAN) settings of the router and set up static routes.

The chapter includes the following sections:

- VLAN concepts
- VLANs and LANs
- Manage EEE, flow control, and link speed for ports
- MAC address to IP address bindings
- Static routes

Note: The procedures that are described in this chapter explain how to manage configuration options through the device UI. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

VLAN concepts

This section describes general VLAN concepts, the management VLAN, and how the router uses VLANs.

Basic 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 were 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.
- **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 router-based security measures such as traffic rules and MAC ACLs to restrict access to a VLAN.

Management VLAN

A management 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 the router, the management VLAN (VLAN 1) is also the default VLAN. By default, all ports are untagged members of the default VLAN. A LAN port can be an untagged member of a single VLAN only.

Although you can change the management VLAN from VLAN 1 to another VLAN, we recommend that you do so only if you have an understanding of network management. Incorrect configuration of the management VLAN can block access to the router.

For the management VLAN to be secure, it must be used only for controlling and managing your network devices. We recommend that you 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, make sure that you make your computer or device a member of the VLAN and add its MAC address to the access control list (if applicable). Otherwise, you must log in from an allowed device or lose access to the management functions of the router. If you are unable to log in on an allowed device, you must reset the router to factory default settings to regain management access.

How the router uses VLANs and LANs

By default, all LAN ports are assigned to the default VLAN, or VLAN 1, and all untagged traffic is routed through the default VLAN. By default, VLAN 1 is also the management VLAN through which you can manage the router (see Management VLAN on page 54).

VLAN profiles: The VLANs that you configure on the router function actually as VLAN *profiles* that determine the following LAN settings, which affect any device that connects to the VLAN:

- **IPv4 settings for the VLAN**: IP address, subnet mask, Router Information Protocol (RIP) direction, and RIP version.
- **DCHP server for the VLAN**: Start and end IP addresses, and lease time.
- **DNS settings for the VLAN**: DNS proxy or IP addresses of up to three DNS servers

You can set up to eight VLANs on the router, and each VLAN must be assigned unique IPv4, DHCP server, and DNS settings.

LAN port assignment to a VLAN: LAN ports can be assigned to one or more VLANs in the following ways:

- A LAN port is assigned to at least one VLAN (by default, VLAN 1).

- A LAN port can be an *untagged* member of a single VLAN only. (By default, all LAN ports are untagged members of VLAN 1.)
- You can assign a LAN port as a *tagged* member of multiple VLANs. Typically, a LAN port that is assigned to multiple VLANs is used as a trunk port to connect the router to a switch, access point, or other router. (You cannot specifically configure a port as a trunk port or access port in the device UI, but any port can serve as a trunk port or access port if you configure the settings correctly.)
- If you configure the LAN 5 port as the WAN2 port, the WAN2 port is excluded from all VLANs, unless your ISP requires you to use a VLAN tag for the WAN2 port.

VLAN communication: The following applies to communication for devices on a VLAN and between VLANs:

- Devices on the same VLAN can communicate with each other regardless of whether the ports that are members of the VLAN are tagged or untagged.
- Devices on different VLANs cannot communicate each other regardless of whether the ports that are members of the VLANs are tagged or untagged. However, if you enable the Inter VLAN Routing feature for two or more VLANs, devices on these different VLANs *can* communicate with each other.

Example of how the router processes traffic

The predefined default VLAN on the router is the VLAN with ID 1 (VLAN 1) with IPv4 network 192.168.**1**.0/24. All LAN ports are untagged members of this VLAN 1.

For this example, assume that you did not change the default VLAN (VLAN 1) and that you add a VLAN with ID 100 (VLAN 100) with IPv4 network 192.168.**100**.0/24 that has all LAN ports as tagged members.

The router processes incoming untagged and tagged packets as follows:

- If an *untagged* packet enters the LAN1 port, VLAN 1 processes the packet:
  - If the destination for the untagged packet is a device that is connected to the LAN3 port on the 192.168.1.0/24 network (the VLAN 1 network), the packet is forwarded to the LAN3 port without any tagging because that port is an untagged member of VLAN 1.
  - If the destination for the untagged packet is a device that is connected to the LAN5 port on the 192.168.100.0/24 network (the VLAN 100 network), and the Inter VLAN Routing feature is enabled for both VLAN 1 and VLAN 100, the packet is routed from VLAN 1 to VLAN 100, and then forwarded from the LAN5 port with tag 100 because that port is a tagged member of VLAN 100.

- If a *tagged* packet enters the LAN4 port and its VLAN tag is 100, VLAN 100 processes the packet:
  - If the destination for the tagged packet is a device that is connected to the LAN2 port on the 192.168.100.0/24 network (the VLAN 100 network), the LAN2 port forwards the packet with tag 100 because that port is a tagged member of VLAN 100.
  - If the destination for the tagged packet is a device that is connected to the LAN2 port on the 192.168.1.0/24 network (the VLAN 1 network), and the Inter VLAN Routing feature is enabled for both VLAN 1 and VLAN 100, the packet is routed from VLAN 100 to VLAN 1, and then forwarded from the LAN2 port without a tag because that port is an untagged member of VLAN 1.
- If a *tagged* packet enters the LAN4 port and its VLAN tag is *not* 100, the router drops the packet because the LAN4 port is a tagged member of VLAN 100.

VLANs and LANs

The router's LAN can include multiple VLANs and LAN *subnets*.

A VLAN on the router includes its own LAN subnet. By default, the router includes one VLAN (VLAN 1) and one LAN subnet (192.168.1.x) , but the router can support multiple VLANs, each with its own LAN subnet. For example, you could add VLAN 10 and define the associated LAN subnet as 192.168.25.x or 192.168.30.x.

You can add, change, and remove VLANs, and assign LAN ports to VLANs.

Add a VLAN profile

VLAN 1 is the default VLAN, which includes all LAN ports as untagged members. You can add multiple VLANs.

When you add a VLAN, you do not just add an ID. Rather, you add an entire VLAN *profile* that determines the LAN settings for any device that connects to that VLAN.

To add a VLAN profile:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **LAN > VLAN Settings**.
   The VLAN Settings page displays.

5. Click the **Add VLAN Profile** button.
   The Add New VLAN Profile pop-up window displays.

6. In the **VLAN ID** field, type a VLAN ID.
   The ID must be in the range from 2 to 4094. (ID 1 is already in use.)

7. In the **VLAN Name** field, type a name for the VLAN.
   The name is for identification purposes.

8. Click the **Inter VLAN Routing** toggle to enable or disable routing between this VLAN and other VLANs for which Inter VLAN Routing is enabled:

   - **The toggle is blue and positioned to the right**: Traffic between this VLAN and the other VLANs on the router is allowed.
   - **The toggle is gray and positioned to the left**: Traffic is restricted to this VLAN only. This is the default setting, which adds security to the VLAN but limits the traffic options.

9. Click the **Device Management** toggle to enable or disable this VLAN as the management VLAN:

   - **The toggle is blue and positioned to the right**: The VLAN functions as the management VLAN through which you can access the router.

     CAUTION: We recommend that you do not change the management VLAN from VLAN 1 to another VLAN unless you have an understanding of network management. Incorrect configuration of the management VLAN can block access to the router.

- **The toggle is gray and positioned to the left**: The VLAN does not function as the management VLAN. This is the default setting because VLAN 1 is the default management VLAN. The router supports a single management VLAN only.

10. In the IPv4 Settings section, configure the following settings:

- **IP Address**: Type the IP address of the VLAN. This IP address and the associated subnet mask define the VLAN subnet.
- **Subnet Mask**: Type the associated subnet mask for the VLAN IP address.
- **RIP Direction**: Select how the Router Information Protocol (RIP) lets the router exchange routing information with other routers:
  - **Both**. The router broadcasts its routing table periodically and incorporates information that it receives. This is the default setting.
  - **In Only**: The router incorporates the RIP information that it receives but does not broadcast its routing table.
  - **Out Only**: The router broadcasts its routing table periodically but does not incorporate the RIP information that it receives
- **RIP Version**:
  - **Disabled**: The RIP version is disabled. This is the default setting.
  - **RIP-1**: This format is universally supported. It is adequate for most networks, unless you are using an unusual network setup.
  - **RIP-2B**: This format carries more information that RIP-1, sends the routing data in RIP-2 format, and uses subnet broadcasting.
  - **RIP-2M**: This format carries more information that RIP-1, sends the routing data in RIP-2 format, and uses multicasting.

11. In the DHCP Server section, click the Status toggle to enable or disable the DHCP server for this VLAN:

- **The toggle is blue and positioned to the right**: The DHCP server is enabled and assigns an IP address to the devices on this VLAN. This is the default setting.
- **The toggle is gray and positioned to the left**: The DHCP server is disabled. Devices on the VLAN must be manually configured with an IP address in the subnet of the VLAN.

If you enable the DHCP server for this VLAN, configure the following settings:

- **Start Address**: A start IP address in the subnet that you defined for the VLAN (see Step 10).

- **End Address**: An end IP address in the subnet that you defined for the VLAN (see Step 10).
- **Lease Time**: The time in minutes, hours, or days during which the address is assigned to (leased by) the device. When this time expires, the device must log in again. By default, the lease time is one day (24 hours).

12. In the DNS Type section, select a radio button:

- **DNS Proxy**: The router provides its own address as a DNS server to the devices on the VLAN. The router receives the actual DNS addresses from the ISP (or another router on your network) and forwards DNS requests from the devices on the VLAN.
- **Use these DNS Servers**: If you select the **Use these DNS Servers** radio button, configure the custom DNS servers:
  - **DNS 1**: The IP address of the first DNS server.
  - **DNS 2**: The IP address of the second DNS server.
  - **DNS 3**: The IP address of the third DNS server, if available.

13. Click the **Apply** button.

    Your settings are saved. The new VLAN profile is added to the VLAN Settings page.

Assign a VLAN to a LAN port

By default, each LAN port is an untagged member of the default VLAN, VLAN 1. If you added one or more VLANs (see Add a VLAN profile on page 57), you can change the VLAN ID for a LAN port.

If you add other VLANs, you also make a LAN port a tagged or untagged member of another VLAN. Or, you can exclude a LAN port from a VLAN:

- **Tagged**: The LAN port inserts the VLAN tag in the traffic that it processes. Untagged traffic is forwarded to the default VLAN. A LAN port can be a tagged member of multiple VLANs.
- **Untagged**: The LAN port does not insert the VLAN tag in the traffic that it processes. A LAN port must be an untagged member of a VLAN, but cannot be an untagged member of more than one VLAN.
- **Excluded**: The LAN port drops traffic that is not directed to the VLAN.

The following is a configuration example with tagged and untagged traffic:

Example: In a typical configuration with a VoIP phone that has two LAN ports, one port is connected (through a VLAN-aware switch) to the LAN 2 port on the router, and the other port is connected to a LAN port on a computer:

- Packets coming from the VoIP phone to the LAN 2 port on the router are tagged.
- Packets coming from the computer are passing through the VoIP phone to the LAN 2 port on the router. These packets are untagged.

When you assign the LAN 2 port on the router to VLAN 5, packets entering and leaving the port are tagged with the VLAN ID 5. However, the untagged packets entering the LAN port on the router are forwarded to the default VLAN 1.

To assign a VLAN to a LAN port:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > VLAN Settings**.
   The VLAN Settings page displays.
5. Scroll down to the Assign VLANs to Wired Ports section at the bottom of the page.
6. For a specific VLAN and the menu for one of the LAN ports, select one of the following:
   - **Tagged**: The LAN port inserts the specific VLAN tag in the traffic that it processes. A LAN port can be a tagged member of multiple VLANs.
   - **Untagged**: The LAN port does not insert the specific VLAN tag in the traffic that it processes.

A LAN port must be an untagged member of a VLAN, but cannot be an untagged member of more than one VLAN.

- **Excluded**: The LAN port drops traffic that is not directed to the VLAN.

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

Change a VLAN profile

You can change an existing VLAN profile, including the profile for VLAN 1 (the default VLAN profile for the LAN).

CAUTION: We recommend that you do not change the default VLAN profile (VLAN 1) unless you have an understanding of network management. Incorrect configuration of VLAN 1 can block access to the router.

To change a VLAN profile:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > VLAN Settings**.
   The VLAN Settings page displays.
5. Select a VLAN ID by clicking the VLAN ID or clicking anywhere in the section for the VLAN ID.

If you did not yet add a custom VLAN profile but want to change the default VLAN profile, click **VLAN ID 1**, or click anywhere in the VLAN ID 1 section.

The page expands and displays the settings for the selected VLAN profile.

6. Change the settings for the VLAN profile.
   For more information about the settings, see Add a VLAN profile on page 57.
7. Click the **Apply** button.
   Your settings are saved.

Remove a VLAN profile

If you no longer need a VLAN, you can remove its profile. You cannot remove VLAN 1, the default VLAN profile.

To remove a VLAN profile:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > VLAN Settings**.
   The VLAN Settings page displays.
5. Select a VLAN ID by clicking the VLAN ID or clicking anywhere in the section for the VLAN ID.
   The page expands and displays the settings for the selected VLAN profile.

6. Scroll down and click the **Delete** button.
   A pop-up window displays
7. Click the **OK** button.
   Your settings are saved. The VLAN is removed.

Manage EEE, flow control, and link speed for ports

The router lets you manage the following settings for each port:

- **EEE**: Energy Efficient Ethernet (EEE) mode, which combines the MAC address of a port with a family of physical layers that support operation in a low power mode. (EEE is defined by the IEEE 802.3az standard.) Lower power mode lets both the send and receive sides of the link disable some functionality for power savings when lightly loaded. By default, EEE 802.3az is disabled for a port. Note the following about EEE 802.3az:
  - Transition to low power mode does not change the link status.
  - Frames in transit are not dropped or corrupted in transition to and from low power mode.
  - Transition time is transparent to upper layer protocols and applications.
- **Flow control**: Flow control (IEEE 802.3x) works by pausing a port if the port becomes oversubscribed. It drops all traffic for short intervals of time during the congested condition. By default, flow control is disabled. (For some network situations, flow control might not work well.) You can enable flow control.
- **Link speed**: By default, the link speed of a port is set at auto-negotiation, which allows the port to function at its maximum supported speed, depending on the port speed of the device at the other side. You can also set a specific speed for a port so that the port always functions at the configured speed and auto-negotiation does not set the speed.

To manage EEE, flow control, and link speed for ports:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **LAN > Port Settings**.
   The Port Settings page displays.

5. For each port, do the following:

   - Select or clear the **EEE** check box.
     If you select the check box, IEEE 802.3az is enabled for the port. By default, IEEE 802.3az is disabled, and the check box is cleared.
   - Select or clear the **Flow Control** check box.
     If you select the check box, flow control is enabled for the port. By default, flow control is disabled, and the check box is cleared.
   - From the **Link Speed** menu for a port, either keep the default **Auto Negotiation** setting, or select a specific speed, which depends on the port:

     - The LAN1, LAN2, and LAN3 ports support 2.5 Gbps, 1 Gbps, or 100 Mbps. (You can set the port speed for each port individually.)
     - The LAN4 port supports 10 Gbps or 1 Gbps.
     - The LAN5 port or WAN2 port (depending on whether the port functions as the LAN 5 port or the WAN2 port in a dual WAN configuration) supports 10 Gbps, 5 Gbps, 2.5 Gbps, 1 Gbps, or 100 Mbps.
     - The WAN1 port supports 2.5 Gbps, 1 Gbps, or 100 Mbps.

     The default Auto Negotiation setting allows a port to function at its maximum supported speed, depending on the port speed of the device at the other side.

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

MAC address to IP address bindings

MAC-address to IP-address binding, referred to as MAC-IP binding, lets you bind a device's MAC address to an IPv4 address and the other way around. Binding means that the IPv4 address becomes static for the device. The VLAN's DHCP server assigns the same IPv4 address each time that the device connects to the router

A MAC-IP binding serves several purposes:

- **Reachability**: A MAC-IP binding ensures that a device always receives the same IP address. This can be important for network servers and common network resources.
- **Security**: To prevent a user from changing the static IP address of their device, add a MAC-IP binding for the device. If the router detects packets with an IP address that matches the IP address in the MAC-IP Binding List but does not match the related MAC address in the list (or the other way around), the packets are dropped.

Add a MAC-IP binding for a detected device

To easiest way to add a MAC-IP binding is to apply the binding to an existing device that is automatically detected on a VLAN. To add a binding, you do not need to know the MAC address or IP address of the device, but if there are multiple VLANs, it helps if you know to which VLAN the device is connected.

If you want to add a binding for a device that has not yet connected to the router, you must do so manually (see Manually add a MAC-IP binding on page 67).

The device UI uses the following icons:

 Import  Export  Add from Existing Device  Add  Edit  Delete

To add a MAC-IP binding from a detected device on a VLAN:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **LAN > Static DHCP Leases**.
   The Static DHCP Leases page displays.
5. From the **VLAN** menu, select the VLAN.
   If you did not add a VLAN, only VLAN 1 displays.
   If you already added MAC-IP bindings for the VLAN, the page displays the MAC-IP bindings for the VLAN.
6. Click the **Add from Existing Device** icon.
   The Add from Existing Devices pop-up window displays.
7. Select the check boxes for the devices for which you want to bind the MAC address to the IPv4 address.
8. Click the **Apply** button.
   Your settings are saved. The binding or bindings display on the Static DHCP Leases page for the selected VLAN.

Manually add a MAC-IP binding

To manually add a MAC-IP binding for a device, you need to know the MAC address and IP address for the device, or the MAC address and the IP address that you want to be assigned to the device.

The device UI uses the following icons:

 Import  Export  Add from Existing Device  Add  Edit  Delete

To manually add a MAC-IP binding for a VLAN:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > Static DHCP Leases**.
   The Static DHCP Leases page displays.
5. From the **VLAN** menu, select the VLAN.
   If you did not add a VLAN, only VLAN 1 displays.

   If you already added MAC-IP bindings for the VLAN, the page displays the MAC-IP bindings for the VLAN.
6. Click the **Add** icon.
   The Add Details pop-up window displays.
7. Configure the following settings:
   - **MAC Address**: Type the MAC address of the device.
   - **IP Address**: Type the IPv4 address that must be assigned to the device.
   - **Device Name**: Type a name for the device. The name is for identification purposes.
8. To add another device, click the **Add More** button, and repeat the previous step for another device.
9. Click the **Apply** button.
   Your settings are saved. The binding or bindings display on the Static DHCP Leases page for the selected VLAN.

Import a list with MAC-IP bindings

You can import a list with MAC-IP bindings for one, several, or all VLANs. An imported list overwrites any MAC-IP bindings that are already present for a VLAN that is defined

in the import list. After you import the list, you can add more IP-MAC bindings per individual VLAN.

Your file with MAC-IP bindings must be a `.csv` file that lists, for each device, the VLAN ID, IP address, MAC address, and device name on a single line, separated by commas. The following device must be on a new line. The first line must contain the following:

```
VLAN_ID,IP_Address,MAC_Address,Device_Name
```

The device UI lets you download a sample `.csv` file. (See the following procedure.)

The device UI uses the following icons:

 Import  Export  Add from Existing Device  Add  Edit  Delete

To import a list with MAC-IP bindings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > Static DHCP Leases**.

   The Static DHCP Leases page displays.

   For an import operation, you do not need to select a VLAN from the menu.
5. Click the **Import** button.

   The Import pop-up window displays.
6. To download a sample list (a `.csv` file), click the **Download Sample** link and save the file.

7. Click the **Browse** button, navigate to your list, and select it.

   CAUTION: The imported list overwrites any MAC-IP bindings that are already present for a VLAN that is defined in the import list.

8. Click the **Import** button.
   Your settings are saved. The imported list with MAC-IP bindings displays on the Static DHCP Leases page.

Change a MAC-IP binding

You can change the settings for a MAC-IP binding.

The device UI uses the following icons:

 Import  Export  Add from Existing Device  Add  Edit  Delete

To change the settings for a MAC-IP binding:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > Static DHCP Leases**.
   The Static DHCP Leases page displays.
5. From the **VLAN** menu, select the VLAN.
   If you did not add a VLAN, only VLAN 1 displays.

If you already added MAC-IP bindings for the VLAN, the page displays the MAC-IP bindings for the VLAN.

6. Select the check box for the binding.
7. Click the **Edit** button.
   The Edit Details pop-up window displays.
8. Change the settings for the binding.
   You can change the MAC address, IP address, and device name.
9. Click the **Apply** button.
   Your settings are saved. The modified IP-MAC binding displays on the Static DHCP Leases page.

Remove a MAC-IP binding

You can remove a binding. You can also easily remove all bindings for a single VLAN.

The device UI uses the following icons:

 Import  Export  Add from Existing Device  Add  Edit  Delete

To remove one or more bindings for a VLAN:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **LAN > Static DHCP Leases**.
   The Static DHCP Leases page displays.
5. From the **VLAN** menu, select the VLAN.
   If you did not add a VLAN, only VLAN 1 displays.
   If you already added MAC-IP bindings for the VLAN, the page displays the MAC-IP bindings for the VLAN.
6. Select the check box for the binding.
   To select all bindings, select the check box in the table header.
7. Click the **Delete** icon.
   A pop-up window displays.
8. Click the **OK** button.
   Your settings are saved. The binding or bindings are removed.

Export a list with MAC-IP bindings

You can export a list with MAC-IP bindings that you configured for all VLANs. Although you must configure a MAC-IP binding per individual VLAN, the exported list combines all MAC-IP bindings for all VLANs.

The first line of the exported list contains the following:

```
VLAN_ID,IP_Address,MAC_Address,Device_Name
```

The device UI uses the following icons:

Import Export Add from Existing Device Add Edit Delete

To export a list with MAC-IP bindings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **LAN > Static DHCP Leases**.
   The Static DHCP Leases page displays.
   For an export operation, you do not need to select a VLAN from the menu.
5. Click the **Export** button.
   A pop-up window displays.
6. Save the file to a location on your computer.
   The default file name is `RouterModel-DHCP-static-leases` in which `RouterModel` is the model number of your router. The default file extension is `.csv`.

Static routes

For almost all Internet traffic, routes are automatically and dynamically selected. You can also set up a fixed, static IPv4 route. Typically, you only need to add static routes when you have more than one router or multiple IP subnets on your network.

As an example of when a static route is needed, consider the following case:

- Your main Internet access is through a cable modem to your ISP. The cable modem is connected to the router.
- Your business network also includes an ADSL router that you use to access a remote office site. This ADSL router is connected to a DSL modem, which is used on-demand only.
- Your LAN subnet is 192.168.1.0, and the ADSL router's address on your LAN is 192.168.1.100.
- The public IP address range at the remote office site is 134.177.0.0.

When you set up the router, two implicit static routes were created:

1. A default route was created between the router and the cable modem that connects to your ISP.
2. A second static route was created between the router and the LAN for all 192.168.1.0 addresses.

With this configuration, if you try to access a device on the 134.177.0.0 network at the remote office site, the router forwards your request to your ISP. In turn, the ISP forwards your request to the remote office site, where the firewall will deny the request.

In this situation, you must define a static route, telling the router to access 134.177.0.0 addresses through your ADSL router at its LAN address of 192.168.1.100.

Here is an example static route setting for this configuration:

- **Destination IP address and subnet mask settings**: The route applies to all addresses at the remote site, so set the destination IP address to 134.177.0.0 and the subnet mask to 255.255.255.0.
- **Gateway IP address**: Traffic for addresses in the 134.177.0.0 network must be forwarded to the ADSL router, so set the gateway IP address to 192.168.1.100 (the ADSL router's address on your LAN).
- **Private route**: Make the static route private as a security precaution in case Routing Information Protocol (RIP) is activated. A private route is not reported in RIP messages.

Add a static route

You can add an IPv4 static route to a destination IP address and specify the subnet mask, next hop IP address, and metric.

The device UI uses the following icons:

 Add  Edit  Delete

To add a static route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **LAN > Static Routing**.
   The Static Routes page displays.
5. Click the **Add** icon.
   The table expands.
6. Specify the settings for the route:
   - **Route Name**: Type a name for the route. The name is for identification purposes.
   - **Network**: Type the IP address for the final destination of the route.
   - **Subnet Mask**: Type the IP subnet mask for the final destination of the route. If the destination is a single host, enter **255.255.255.255**.
   - **Gateway**: Type the IP address of the gateway for the route.
     This is the gateway or next router in the path from your network to the final destination of the route.
   - **Metric (Max 255)**: Type a number from 2 to 255. (You can enter 1, but that indicates a directly-connected router.)
     The metric value represents the number of routers between your network and the final destination of the route.
   - **Interface**: From the **Interface** menu, select a VLAN profile (in this context referred to as a VLAN interface) or a WAN interface.
     The destination of the route must be reachable through the selected interface.
   - **Active**: Click the **Active** toggle to make the route active or inactive after you click the Apply button:
     - **The toggle is blue and positioned to the right**: The route becomes active after you click the Apply button. This is the default setting.
     - **The toggle is gray and positioned to the left**: The route remains inactive after you click the Apply button. You can make it active a later time.
7. Click the **Apply** button.
   Your settings are saved.

   The static route is added to the table on the Static Routes page.

Change a static route

You can change an existing static route.

The device UI uses the following icons:

 Add  Edit  Delete

To change a static route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > Static Routing**.
   The Static Routes page displays.
5. In the table, select the check box for the route.
6. Click the **Edit** icon.
   The settings become editable.
7. Change the settings for the route.
   For more information about the settings, see Add a static route on page 74.
8. Click the **Apply** button.
   Your settings are saved. The modified route displays in the table.

Remove a static route

If you no longer need a static route, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a static route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **LAN > Static Routing**.
   The Static Routes page displays.
5. In the table, select the check box for the route.
6. Click the **Delete** icon.
   A pop-up window displays.
7. Click the **Proceed** button.
   You settings are saved. The route is removed from the table.

6

Manage the Firewall and Security

The router comes with a built-in basic firewall that helps to protect your network from unwanted intrusions *from* the Internet and lets you control access *to* the Internet.

This chapter includes the following sections:

Note: The procedures that are described in this chapter explain how to manage configuration options through the device UI. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

Manage protection for port scans, denial of service, and pings

Port scan protection and denial of service (DoS) protection can protect your LAN against attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. By default, DoS protection is enabled and a port scan is rejected.

You can also enable the router to respond to a ping to its WAN (Internet) port. This feature allows your router to be discovered. Enable this feature only as a diagnostic tool or if a specific reason exists.

To manage protection for port scans, denial of service, and pings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Basic Settings**.
   The Basic Settings page displays.
5. Click the **Enable Port Scan and DoS Protection** toggle to enable or disable these security features:
   - **The toggle is blue and positioned to the right**: Port scans and Denial of Service (DoS) protection are enabled. This is the default setting.
   - **The toggle is gray and positioned to the left**: Port scans and DoS protection are disabled.

6. Click the **Enable Respond to Ping on Internet Port** toggle to enable or disable this security feature:
   - **The toggle is blue and positioned to the right**: The router responds to a ping on a WAN port.
   - **The toggle is gray and positioned to the left**: The router rejects a ping on a WAN port. This is the default setting.
7. Click the **Apply** button.
   Your settings are saved.

Set up a DMZ server

A demilitarized zone (DMZ) server is helpful when you are using some Internet services and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if the IP address for that computer is entered as the DMZ server.

WARNING: DMZ servers pose a security risk. A computer designated as the DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

The router usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service or application for which you set up a port forwarding (see Port forwarding on page 90) or port triggering rule (see Port triggering on page 95). Instead of discarding this traffic, you can direct the router to forward the traffic to one computer on your network. This computer is called the DMZ server.

To set up a DMZ server:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Basic Settings**.
   The Basic Settings page displays.
5. Click the **DMZ Server** toggle to enable the DMZ server:
   - **The toggle is blue and positioned to the right**: The DMZ server is enabled and the IP Address field is available.
   - **The toggle is gray and positioned to the left**: The DMZ server is disabled. This is the default setting.
6. In the **IP Address** field, type the LAN IP address of the computer that must function as the DMZ server.
7. Click the **Apply** button.
   Your settings are saved.

Manage the SIP application-level gateway

The application-level gateway (ALG) for the Session Initiation Protocol (SIP) can enhance address and port translation. However, some types of VoIP and video traffic might not work well when the SIP ALG is enabled. For this reason you can disable the SIP ALG.

To manage the SIP ALG:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Basic Settings**.
   The Basic Settings page displays.
5. Click the **Enable SIP ALG** toggle to enable or disable the SIP ALG:
   - **The toggle is blue and positioned to the right**: The SIP ALG is enabled. This is the default setting.
   - **The toggle is gray and positioned to the left**: The SIP ALG is disabled
6. Click the **Apply** button.
   Your settings are saved.

Manage timeouts for TCP, UDP, and ICMP sessions

The router stops processing TCP, UDP, or ICMP traffic if the session time-out period for the protocol expires, or if the maximum number of concurrent TCP, UDP, and ICMP sessions is exceeded.

These are the default settings:

- **TCP session timeout**: 1800 seconds
- **UDP session timeout**: 30 seconds
- **ICMP session timeout**: 30 seconds
- **Maximum number of concurrent TCP, UDP, and ICMP sessions**: 60,000

To manage timeouts for TCP, UDP, and ICMP sessions and set the maximum number of concurrent sessions:

1. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the switch through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
2. Select **Firewall > Basic Settings**.
   The Basic Settings page displays.
3. In the Session Timeout section, configure the following settings:
   - **TCP Session Timeout**: Enter a time in seconds from 30 to 86400 seconds.
   - **UDP Session Timeout**: Enter a time in seconds from 30 to 86400 seconds.
   - **ICMP Session Timeout**: Enter a time in seconds from 15 to 60 seconds.
   - **Maximum Concurrent Connections**: Enter a total number of sessions from 10000 to 60000.

   The Current Connections field show the total number of current TCP, UDP, and ICMP sessions (connections).
4. Click the **Apply** button.
   Your settings are saved.

Manage VPN pass-through for tunnel protocols

VPN pass-through allows a device on the LAN to receive VPN traffic from the Internet over an IPSec, PPTP, or L2TP connection. Under normal circumstances, leave VPN

pass-through enabled, which is the default setting. If you disable VPN pass-through for a protocol, VPN traffic is blocked for that protocol.

To disable VPN pass-through for IPSec, PPTP, or L2TP, or for two or all of these protocols:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Basic Settings**.

   The Basic Settings page displays.
5. In the VPN Passthrough section, for one or more protocols, click the associated toggle:

   - **The toggle is blue and positioned to the right**: VPN pass-through is enabled for the protocol. This is the default setting for each protocol.
   - **The toggle is gray and positioned to the left**: VPN pass-through is disabled for the protocol.
6. Click the **Apply** button.

   Your settings are saved.

Firewall traffic rules

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open a WAN port on the router.

The router provides one default outbound traffic rule: It allows all access to the Internet (that is, the WAN). You can add rules to allow access to or prevent access from specific protocols and IP addresses on the Internet. For example, you can specify if a traffic rule applies to one IP address, a range of IP addresses, a subnet of IP addresses, or to all IP addresses on a VLAN interface or WAN interface.

A traffic rule on the router defines the following components:

- **Action**: The rule either allows or blocks traffic.
- **Service**: The rule can apply to all traffic or only to traffic for a specific predefined service or protocol. For information about setting up services, see Services, protocols, and port numbers on page 102.
- **Source interface**: The source interface is the interface from which the traffic originates. The rule can apply to all source interfaces or only to a specific WAN interface or VLAN interface.
- **Source address**: The source address is the IP address from which the traffic originates. The rule can apply to all source addresses or only to one IP address, a range of IP addresses, or a subnet of IP addresses.
- **Destination interface**: The destination interface is the interface to which the traffic is sent. The rule can apply to all destination interfaces or only to a specific WAN interface or VLAN interface.
- **Destination address**: The destination address is the IP address to which the traffic is sent. The rule can apply to all destination addresses or only to one IP address, a range of IP addresses, or a subnet of IP addresses.
- **Schedule**: The rule can apply continuously or can be turned on and off by a schedule. For information about setting up schedules, see Schedules on page 107.

CAUTION: You need some networking knowledge to set up traffic rules, because incorrectly configured traffic rules might block communication on the router.

Add a firewall traffic rule

You can add a traffic rule to the firewall to prevent or allow traffic based on its protocol, source, destination, and other criteria.

The device UI uses the following icons:

 Add  Edit  Delete

To add a firewall traffic rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Traffic Rules**.
   The Traffic Rules page displays.
5. Click the **Add** icon.
   The Add/Edit Traffic Rules pop-up window displays.
6. Configure the following settings:
   a. In the **Name** field, enter a name for the traffic rule.
   The name is for identification purposes.
   b. To immediately enable the rule after you click the Apply button, keep the **Enable Rule Status** toggle blue and positioned to the right, which is the default setting. If you do not want the rule to be enabled after you click the Apply button, click the **Enable Rule Status** toggle so that the toggle is gray and positioned to the left.

c. Select an Action radio button:

- **Allow**: Traffic that conforms to the rule is accepted from its origination and sent to its destination.
- **Deny**: Traffic that matches the rule is denied and dropped.

d. From the **Services** menu, select the predefined service.
All services are IPv4 protocols or services. To add a custom service or protocol, see Services, protocols, and port numbers on page 102.

e. From the **Source Interface** menu, select the VLAN or WAN interface from which the traffic originates. By default, the traffic can originate from any interface.

f. From the **Source Address** menu, select the IP address, subnet, or address range from which the traffic can originate:

- **Any**: The traffic can originate from any IP address. This is the default setting.
- **Single**: The traffic can originate from a single address. Enter the IP address.
- **Subnet**: The traffic can originate from a subnet. Enter the IP address and subnet.
- **Range**: The traffic can originate from a range of IP addresses: Enter the start and end IP addresses.

g. From the **Destination Interface** menu, select the VLAN or WAN interface to which the traffic is sent. By default, the traffic can be sent to any interface.

h. From the **Destination Address** menu, select the IP address, subnet, or address range to which the traffic can be sent:

- **Any**: The traffic can be sent to any IP address. This is the default setting.
- **Single**: The traffic can be sent to a single address. Enter the IP address.
- **Subnet**: The traffic can be sent to a subnet. Enter the IP address and subnet.
- **Range**: The traffic can be sent to a range of IP addresses: Enter the start and end IP addresses.

7. To apply a schedule to the traffic rule so that the traffic rule is enforced according to the schedule, select a schedule from the **Schedule** menu.

   By default, Always is selected from the menu and a schedule does not apply. For information about setting up schedules, see Schedules on page 107.

8. Click the **Apply** button.

   The new traffic rule is added to the table on the Traffic Rules page. If you enabled the new traffic rule (that is, the Enable Rule Status toggle is blue and positioned to

the right), it goes into effect immediately. The traffic rule is assigned the lowest priority in relation to existing traffic rules.

9. To change the priority for a rule, do the following:
   a. In the Reorder column of the table, click the up or down icons until the traffic rule reaches the desired position.
      The number in the Priority column show the priority in relation to the other traffic rules in the table.
   b. Click the **Apply** button.
      Your settings are saved.

Change a firewall traffic rule or its priority, or enable or disable the rule

You can change an existing firewall traffic rule or its priority, or enable or disable the rule.

The device UI uses the following icons:

 Add  Edit  Delete

To change a firewall traffic rule or its priority, or enable or disable the rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **Firewall > Traffic Rules**.
   The Traffic Rules page displays.
5. To change the settings for a rule or enable or disable the rule, do the following:
   a. In the table, select the check box for the rule.
   b. Click the **Edit** icon.
      The Add/Edit Traffic Rules pop-up window displays.
   c. Change the settings for the traffic rule, or enable or disable the rule:
      For more information about the settings, see Add a firewall traffic rule on page 86.
   d. To enable or disable the rule, click the **Enable Rule Status** toggle:
      - **The toggle is blue and positioned to the right**: The rule is enabled.
      - **The toggle is gray and positioned to the left**: The rule is disabled.
   e. Click the **Apply** button.
      Your settings are saved. The modified rule displays in the table on the Traffic Rules page.
6. To change the priority for a rule, do the following:
   a. In the Reorder column of the table, click the up or down icons until the traffic rule reaches the desired position.
      The number in the Priority column show the priority in relation toe the other traffic rules in the table.
   b. Click the **Apply** button.
      Your settings are saved.

Remove a traffic rule

If you no longer need a traffic rule, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a traffic rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Traffic Rules**.
   The Traffic Rules page displays.
5. In the table, select the check box for the rule.
6. Click the **Delete** icon.
   A pop-up window display.
7. Click the **OK** button.
   You settings are saved. The rule is removed from the table.

Port forwarding

If your business network includes a server, you can allow certain types of incoming traffic to reach the server. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

The router can forward incoming traffic for specific services to computers and servers on your local network. You can specify the services (see Services, protocols, and port numbers on page 102). You can also specify a default DMZ server to which the router forwards all other incoming services (see Set up a DMZ server on page 80).

Note: Some knowledge of protocols and port numbers is essential to add port forwarding rules that function successfully.

Add a port forwarding rule

You can add a port forwarding rule to the router to direct incoming traffic based on the traffic's protocol, source, destination, and other criteria, all of which are defined by a service (see Add a service on page 103). The incoming traffic is directed to an internal computer or server for which you can specify the IP address.

The device UI uses the following icons:

 Add  Edit  Delete

To add a port forwarding rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Port Forwarding**.
   The Port Forwarding page displays.
5. Click the **Add** icon.
   An empty row is added to the table.

6. Configure the following settings:
   a. **External Service**: From the menu in the External Service column, select an external service for incoming traffic. If the router detects incoming traffic that matches this service, the port forwarding rule goes into effect.
   If the service is not in the menu, first add it. To do so, click the **Service Management** button below the table. For more information, see Add a service on page 103. After you are done, continue the configuration of the port forwarding rule.
   b. **Internal Service**: From the menu in the Internal Service column, select an internal service that the router uses to forward traffic to the device at the internal IP address (for example, your network's web server). The service can be the same as the external service, but can also be a different service.
   If the service is not in the menu, first add it (see the previous step).
   c. **External IP Address**: From the menu in the External IP Address column, select if the external service can originate from any IP address or from a specific IP address only:
      - **Any**: The external service can originate from any IP address.
      - **Single IP Address**: The external service can originate only from a specific IP address, which you must type in the field that becomes available with this selection.

   d. **Internal IP Address**: In the field in the Internal IP Address column, type the IP address for the device on your network that provides the service (for example, your network's web server).
   e. **Enable**: To immediately enable the rule after you click the Apply button, keep the **Enable** toggle for the rule blue and positioned to the right, which is the default setting.
   If you do not want the rule to be enabled after you click the Apply button, click the **Enable** toggle for the rule so that the toggle is gray and positioned to the left.

7. Click the **Apply** button.
   The new port forwarding rule is added to the table. If you enabled the new rule, it goes into effect immediately.

Change, enable, or disable a port forwarding rule

You can change, enable, or disable a port forwarding rule.

The device UI uses the following icons:

 Add  Edit  Delete

To change, enable, or disable a port forwarding rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Port Forwarding**.
   The Port Forwarding page displays.
5. In the table, select the check box for the rule.
6. Click the **Edit** icon.
   The settings become editable.
7. Change the settings for the port forwarding rule.
   For more information about the settings, see Add a port forwarding rule on page 91.
8. Click the **Enable** toggle for the rule to enable or disable the rule:
   - **The toggle is blue and positioned to the right**: The port forwarding rule is enabled.
   - **The toggle is gray and positioned to the left**: The port forwarding rule is disabled.
9. Click the **Apply** button.

Your settings are saved. The modified port forwarding rule displays in the table.

Remove a port forwarding rule

If you no longer need a port forwarding rule, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a port forwarding rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Port Forwarding**.
   The Port Forwarding page displays.
5. In the table, select the check box for the rule.
6. Click the **Delete** icon.
   A pop-up window display.
7. Click the **OK** button.
   You settings are saved. The rule is removed from the table.

Application example: Make a local web server public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

To make a local web server public:

1. Assign your web server a fixed IP address using static IP reservation (see MAC address to IP address bindings on page 66).

   In this example, your router always gives your web server an IP address of 192.168.1.33.

2. Add a port forwarding rule that lets the router forward the HTTP service to the local address of your web server at 192.168.1.33.

   HTTP (port 80) is the standard protocol for web servers.

3. When an external user types the URL www.example.com in their browser, the browser sends a web page request message with the following destination information:

   - **Destination address**: The IP address of www.example.com, which is the address of your router.
   - **Destination port number**: 80, which is the standard port number for a web server process.

4. Your router receives the message and finds the port forwarding rule for incoming port 80 traffic.
5. The router changes the destination in the message to IP address 192.168.1.33 and sends the message to the web server.
6. Your web server at IP address 192.168.1.33 receives the request and sends a reply message to your router.
7. Your router performs Network Address Translation (NAT) on the source IP address, and sends the reply through the Internet to the user that sent the web page request.

Port triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- A service or application must use port forwarding to more than one local computer (but not simultaneously).
- A service or application must open incoming ports that are different from the outgoing port.

With port triggering, the router monitors traffic for the service or application *to* the Internet from an outbound "trigger" port that you specify. For outbound traffic from that port, the router saves the IP address of the computer that sent the traffic. The router temporarily opens the incoming port or ports that you specify in your rule and forwards that incoming traffic to that destination. You can specify the services (see Services, protocols, and port numbers on page 102) that the port triggering rules use.

Port forwarding creates a static mapping of a port number or range of ports to a single local computer. Port triggering can dynamically open ports to any computer when needed and close the ports when they are no longer needed.

Note: Some knowledge of protocols and port numbers is essential to add port triggering rules that function successfully.

Add a port triggering rule

When you add a port triggering rule to the router's firewall, you allow traffic for a service (that is, the *triggering* service) to activate a device at an internal IP address to which traffic for an *incoming* service is directed. For information about adding services, see Add a service on page 103. This procedure describes how to select a triggering service, an incoming service, the external IP address from which the services originates, and the IP address for an internal device on your network.

The device UI uses the following icons:

 Add  Edit  Delete

To add a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Firewall > Port Triggering**.
   The Port Triggering page displays.
5. Click the **Add** icon.
   An empty row is added to the table.
6. Configure the following settings:
   a. **Enable**: To immediately enable the rule after you click the Apply button, keep the **Enable** toggle for the rule blue and positioned to the right, which is the default setting.
   If you do not want the rule to be enabled after you click the Apply button, click the **Enable** toggle for the rule so that the toggle is gray and positioned to the left.
   b. In the **Name** field, type a name for the port triggering rule.
   The name is for identification purposes.
   c. **Triggering Service**: From the menu in the Triggering Service column, select the service for which the traffic triggers the port forwarding rule.
   If the service is not in the menu, first add it. To do so, click the **Service Management** button above the table. For more information, see Add a service on page 103. After you are done, continue the configuration of the port triggering rule.
   d. **Incoming Service**: From the menu in the Incoming Service column, select the incoming service for which the traffic is directed to the device at the internal IP address.
   The trigger service can be the same as the incoming service but can also be different. If the service is not in the menu, first add it (see the previous step).
   e. **External IP Address**: From the menu in the External IP Address column, select if the external service can originate from any IP address or from a specific IP address only:
      - **Any**: The external service can originate from any IP address.
      - **Single IP Address**: The external service can originate only from a specific IP address, which you must type in the field that becomes available with this selection.

f. **Internal IP Address:** In the field in the Internal IP Address column, select if any IP address on your network or a specific IP address only on your network can receive traffic for the incoming service:

- **Any**: Any IP address on your network can receive traffic for the incoming service.
- **Single IP Address**: Only a specific IP address on your network can receive traffic for the incoming service. You must type the IP address in the field that becomes available with this selection.

7. Click the **Apply** button.
   The new port triggering rule is added to the table. If you enabled the new rule, it goes into effect immediately.

Change, enable, or disable a port triggering rule

You can change, enable, or disable a port triggering rule.

The device UI uses the following icons:

 Add  Edit  Delete

To change, enable, or disable a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **Firewall > Port Triggering**.
   The Port Triggering page displays.
5. In the table, select the check box for the rule.
6. Click the **Edit** icon.
   The settings become editable.
7. Change the settings for the port triggering rule.
   For more information about the settings, see Add a port triggering rule on page 96.
8. Click the **Enable** toggle for the rule to enable or disable the rule:
   - **The toggle is blue and positioned to the right**: The port forwarding rule is enabled.
   - **The toggle is gray and positioned to the left**: The port forwarding rule is disabled.
9. Click the **Apply** button.
   Your settings are saved. The modified port forwarding rule displays in the table.

Remove a port triggering rule

If you no longer need a port triggering rule, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Firewall > Port Triggering**.
   The Port Triggering page displays.
5. In the table, select the check box for the rule.
6. Click the **Delete** icon.
   A pop-up window display.
7. Click the **OK** button.
   You settings are saved. The rule is removed from the table.

Application example: Port triggering for Internet Relay Chat

Some application servers, such as FTP and IRC servers, send replies to multiple port numbers. Using port triggering, you can tell the router to open more incoming ports when a particular outgoing port starts a session.

An example is Internet Relay Chat (IRC), an old protocol that is still in use. Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer."

The following sequence shows the effects of this port triggering rule:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule and observing the destination port number of 6667, your router creates another session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port and also sends an "identify" message to your router with destination port 113.
6. When your router receives the incoming message to destination port 33333, it checks its session table to see if a session is active for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your router receives the incoming message to destination port 113, it checks its session table and finds an active session for port 113 associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 and 113.

Enable or disable UPnP

Universal Plug and Play (UPnP) lets the router be discovered by other devices in a network that support UPnP. For enhanced security, UPnP is disabled by default. For ease of management, you can enable UPnP .

To enable or disable UPnP:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Firewall > UPnP**.
   The UPnP page displays.
5. Click the **UPnP** toggle to enable or disable UPnP
   - **The toggle is blue and positioned to the right**: UPnP is enabled. The Advertisement Period and Advertisement Time to Live fields display on the page.
   - **The toggle is gray and positioned to the left**: UPnP is disabled. This is the default setting. The Advertisement Period and Advertisement Time to Live fields are hidden on the page.
6. In the **Advertisement Period** field, type the advertisement period in minutes.
   The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points receive current device status at the expense of more network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.
7. In the **Advertisement Time to Live** field, type the advertisement time to live in hops.
   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value.
8. Click the **Apply** button.
   Your settings are saved.

The UPnP Portmap table displays the IP address of each UPnP device that is accessing the router, the ports (internal and external) that each device opened, and the protocol that each device is using.

Services, protocols, and port numbers

On the router, the term *service* represents a protocol such as FTP or a service such as an ICMP Ping Relay that is associated with a specific protocol (TCP, UDP, TCP & UDP,

IP, or ICMP), a start port, and an end port, or depending on the service, a different type of setting.

The router uses services for the following firewall features:

- Traffic rules
- Port forwarding
- Port triggering

The router has multiple services predefined. You can add new services and change existing ones, including the predefined ones.

As an example of a service, consider the following configuration:

- Your network includes a *public* web server at port 8080 of computer 1. You set up the following service:
  - **Name**: HTTPS_External
  - **Protocol**: TCP
  - **Port Start/ICMP Type/IP Protocol**: 8080
  - **Port End**: 8080

- Your network includes an *internal* web server at port 4443 of computer 2. You set up the following service:
  - **Name**: HTTPS_Internal
  - **Protocol**: TCP
  - **Port Start/ICMP Type/IP Protocol**: 4443
  - **Port End**: 4443

You can now use these two services to configure firewall rules (traffic, port forwarding, and port triggering rules). If you later want to change the port number for the HTTPS_Internal service from port number 4443 to port number 8443, you only need to change the service, not the firewall rule. You can use the same service in different firewall rules.

Add a service

Note: Some knowledge about protocols and port numbers allows you to add services that can function successfully in traffic rules.

You can add a service that you can use for multiple firewall rules. The router includes multiple predefined services.

The device UI uses the following icons:

 Add  Edit  Delete

To add a service:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Service Management**.
   The Service Management page displays.
5. Click the **Add** icon.
   The table adds a new row at the bottom so that you can define the service.
6. In the **Name** field, type a name for the service.
   The name is for identification purposes.

   Note: The name itself does not specify the protocol. The selection from the Protocol menu and the information in the Port Start/ICMP Type/IP Protocol and Port End fields define the protocol to which the service applies.

7. From the **Protocol** menu, select one of the following protocols and type the required information in the **Port Start/ICMP Type/IP Protocol** field and **Port End** field:
   - **TCP&UDP**: The service applies to both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
     You must enter a start port and an end port in the **Port Start/ICMP Type/IP Protocol** field and **Port End** field. If you want to use a single port only, enter the same port number in each field.
   - **TCP**: The service applies to TCP only.
     You must enter a start port and an end port in the **Port Start/ICMP Type/IP Protocol** field and **Port End** field. If you want to use a single port only, enter the same port number in each field.
   - **UDP**: The service applies to UDP only.
     You must enter a start port and an end port in the **Port Start/ICMP Type/IP Protocol** field and **Port End** field. If you want to use a single port only, enter the same port number in each field.
   - **IP**: The service applies to IP.
     You must enter the IP version (**4** or **6**) in the **Port Start/ICMP Type/IP Protocol** field. The Port End field does not apply.
   - **ICMP**: The service applies to Internet Control Message Protocol (ICMP).
     You must enter the protocol type (from **0** to **255**) in the **Port Start/ICMP Type/IP Protocol** field.
8. Click the **Apply** button.
   Your settings are saved. The service is added to the table.

Change a service

You can change an existing service, whether it is a predefined service or a service that you added.

The device UI uses the following icons:

 Add  Edit  Delete

To change a service:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Service Management**.
   The Service Management page displays.
5. In the table, select the check box for the service.
6. Click the **Edit** icon.
   The settings in the selected table row become editable.
7. Change the settings for the service.
   For more information about the settings, see Add a service on page 103.
8. Click the **Apply** button.
   Your settings are saved. The modified service displays in the table.

Remove a service

If you no longer need a service, you can remove it. You can also remove a predefined service.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a service:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Service Management**.
   The Service Management page displays.
5. In the table, select the check box for the service.
6. Click the **Delete** icon.
   A pop-up window displays
7. Click the **Proceed** button.
   You settings are saved. The service is removed from the table.

Schedules

You can set up schedules that you can apply to traffic rules, allowing them to be turned on and off according to the schedule.

A schedule in itself is neutral. The action of the schedule depends on the nature of the rule that you apply it to. For example, a schedule can block access to the Internet if you apply the schedule to a traffic rule that defines blocking access. However, if you apply the same schedule to a traffic rule that defines allowing access to the Internet, the schedule can allow access.

If you want to set up a schedule that goes over midnight (when the clock changes from p.m. to a.m.) you must set up two schedules: one for the p.m. period and one for the a.m. period of the next day.

For example, if you want the schedule to last from 09:00:00 p.m. in the evening to 06:00:00 a.m. the next morning, set up the following two schedules:

- **Schedule 1**: 09:00:00 p.m. to 11:59:59 p.m.
- **Schedule 2**: 12:00:00 a.m. to 06:00:00 a.m.

In the example, the overnight schedule includes a lag of one second, from 11:59:59 p.m. to 12:00:00 a.m. This one second has no effect on the schedule.

Add a schedule

You can add a schedule, specifying the start time and end time and the day or days during which the schedule must be active.

The device UI uses the following icons:

 Add  Edit  Delete

To add a schedule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Firewall > Schedules**.
   The Schedules page displays.
5. Click the **Add** icon.
   The table adds a new row at the bottom so that you can define the schedule.
6. In the **Name** field, type a name for the schedule.
   The name is for identification purposes.

7. In the **Start** field, set the start time by doing the following:
   a. In the **Start** field, click the clock icon.
      A pop-up window displays.
   b. Click the start hour, start minute, and start second, and click the **AM** or **PM** button.
      The end time must be later than the start time but cannot cross midnight.
8. In the **End** field, set the end time by doing the following:
   a. In the **End** field, click the clock icon.
      A pop-up window displays.
   b. Click the end hour, end minute, and end second, and click the **AM** or **PM** button.
      The end time must be later than the start time but cannot cross midnight.
9. In the Days section, select the check box for one or more days, or select **Weekday**, **Weekend**, or **Alldays** check box.
10. Click the **Apply** button.
    Your settings are saved.
    The schedule is added to the table.

Change a schedule

You can change an existing schedule.

The device UI uses the following icons:

 Add  Edit  Delete

To change a schedule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Firewall > Schedules**.
   The Schedules page displays.
5. In the table, select the check box for the schedule.
6. Click the **Edit** icon.
   The settings in the selected table row become editable.
7. Change the settings for the schedule.
   For more information about the settings, see Add a schedule on page 108.
8. Click the **Apply** button.
   Your settings are saved. The modified schedule displays in the table.

Remove a schedule

If you no longer need a schedule, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a schedule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Firewall > Schedules**.
   The Schedules page displays.
5. In the table, select the check box for the schedule.
6. Click the **Delete** icon.
   A pop-up window displays.
7. Click the **OK** button.
   You settings are saved. The schedule is removed from the table.

7

Monitor the Router and its Network

This chapter describes how you can monitor the router and its network.

The chapter includes the following sections:

Note: The procedures that are described in this chapter explain how to manage configuration and monitoring options through the device UI. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

Display alarms, warnings, and notifications

You can display the alarms. warnings, and notifications from any router device UI page. The following procedure describes how you can view them from the Dashboard page.

To display alarms, warnings, and notifications:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Locate the alarm bell icon at the top-right of the page.

   The icon shows a number, indicating the total number of new alarms, warnings, and notifications since the last time that you viewed them.
5. Click the alarm bell icon.

   A pop-up window display the alarms (indicated by a red bell in a circle), warnings (indicated by an orange warning triangle) and informative notifications (indicated by a blue letter “i” in a circle) with a description and time.
6. To view more alarms, warnings, and notifications, scroll down in the pop-up window.
7. To clear the alarms, warnings, and notifications, click the **Clear** link in the pop-up window.

Display the router connectivity, system, and port settings

To display the router connectivity, system, and port settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Locate the Connectivity pane, System Information pane, Ethernet Port Status pane, Internet Port Status pane, and Wireless Settings pane.

   The locations of these panes on the Dashboard depend on the width of the page and the width of your screen.

   - **Connectivity**:
     - If the NETGEAR Insight mode is enabled, the status of the connection to the Insight cloud-based management platform
     - Status of the Internet connection. A green icon indicates an Internet connection.
     - Status of the WAN1 port. A green line indicates that the connection of the WAN1 port is up.
     - If set up, status of the WAN2 port. A green line indicates that the connection of the WAN2 port is up.
     - The number of devices attached to the router.

- **System Information**:
  - **Router Name**: The device name of the router
  - **Region**: The country or region in which the router operates or for which the router is licensed
  - **Ethernet MAC Address**: The base Ethernet MAC address of the router
  - **Serial Number**: The serial number of the router
  - **Current Time**: The current time that the router detected from an NTP server or that you manually set
  - **System Up Time**: The time since the router was last restarted
  - **Insight Mode**: Not Registered if not connected to the Insight cloud-based management platform (the default state). Otherwise, Registered. For more information, see Change the Insight management mode on page 26.
  - **Firmware Version**: The version of the firmware that is running on the router

  This pane also includes the Check for Update button that you can click to check for firmware updates for the router. If an update is available, the Update Now button displays. (For more information, see Let the router check for new firmware and update the firmware on page 125).
- **Ethernet Port Status**: For each LAN and WAN Ethernet port, the following information displays:
  - **Status**: A green port icon indicates that the port is connected. A gray port icon indicates that the port is not connected.
  - **Speed**: The speed of the Ethernet connection (10000 Mbps, 5000 Mbps, 2500 Mbps, 1000 Mbps, or 100 Mbps, or 0 Mbps for a port without a connection).
- **Internet Port Status**: The following information displays, with separate columns for the WAN1 and WAN2 ports, if you configured the LAN5 port as the WAN2 port:
  - **Status**: Displays if the WAN port is online or offline
  - **Connection Type**: The WAN port connection type, which can be DHCP, PPPoE, or Static, depending on how the port receives its IP address settings
  - **IP Address**: The IPv4 address for the WAN port
  - **Gateway**: The default gateway for the WAN port
  - **DNS 1, 2, and 3 Address**: The DNS server IP addresses for the WAN port

- **MAC Address**: The MAC address of the WAN port
- **MTU Size**: The MTU size that is set for the WAN port. (By default, 1500 bytes.)

This pane also contains the **Release** and **Renew** buttons that let you release and renew the Internet connection on a WAN port (For more information, see Check the WAN port IP address on page 177).

- **IPSec VPN Status**:
  - **IPSec**: Displays if IPSec is enabled or disabled
  - **In Use**: The number of IPSec VPN tunnels that are configured (whether enabled or disabled)
  - **Connected**: The number of IPSec VPN clients that are connected (up)
  - **Disconnected**: The number of IPSec VPN clients that are disconnected (down, whether enabled or disabled)
  - **Max Supported**: The maximum number of IPSec VPN clients that can be supported. This number is fixed at 30.

Display devices attached to the router LAN ports

You can display the active wired devices (also referred to as attached devices) that are connected to the LAN ports of the router.

To display the devices attached to the router LAN ports:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Monitoring > Attached Devices**.
   The Attached Devices page displays.
   The following information displays in the table:
   - **Device Name**: The device network name.
   - **IP address**: The IP address that the router assigned to the device when it joined the network. Unless you configured a MAC-address to IP-address binding (see MAC address to IP address bindings on page 66), this address can change when a device is disconnected and rejoins the network.
   - **MAC address**: The MAC address of the connected device.
   - **Port**: The LAN port to which the device is connected.
   - **VLAN**: The VLAN in which the device operates.

Display the DHCP leases for a VLAN or add a MAC-IP binding

You can display the devices that received an IP address from the DHCP server in a VLAN. You can also add a MAC-IP binding for one or more devices. A MAC-IP binding for a device binds the MAC address to an IP address, which means that the device always receives the same IP address from the DHCP server.

To display the DHCP leases for a VLAN or add a MAC-IP binding:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **Monitoring > DHCP Leases**.
   The DHCP Leases page displays.

5. Select a VLAN ID by clicking the VLAN ID or clicking anywhere in the section for the VLAN ID.

   The page expands and displays the settings for the selected VLAN profile.

   The table displays the devices that have an active lease, which does not mean that the device is still connected to the router. (The device might have disconnected, but the lease is still active.)

   - **Hostname**: The name of the device that received an IPv4 address.
   - **IPv4 Address**: The IPv4 address that was issued by the DHCP server in the VLAN.
   - **MAC Address**: The MAC address of the device that received an IPv4 address.
   - **Lease Expires**: The time when the lease expires and the device must reconnect.
   - **Type**: The type of lease, which can be dynamic or static. If you add a MAC-IP binding for a device, the lease becomes static.

6. To add a MAC-IP binding for one or more devices, do the following:
   a. Select the check boxes for one or more devices, or select the check box in the table heading, which selects all devices in the table.
   b. Click the **Add to Static DHCP Lease List** button.
      For each selected device, the MAC address is bound to the IPv4 address. The IPv4 address becomes static. For information about changing or removing a binding, see Change a MAC-IP binding on page 70 or Remove a MAC-IP binding on page 71.

7. To display the most recent information on the page, click the **Refresh** button.

Display Ethernet traffic statistics for the WAN and LAN ports

To display Ethernet traffic statistics for the WAN and LAN ports:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Monitoring > Statistics**.

   The Statistics page displays. The page displays the network traffic statistics for both the WAN and LAN interfaces of the router since the router started or rebooted.

   For each WAN port (LAN port 5 can function as the WAN2 port) and LAN port, the table shows the following information:

   - **Status**: If the interface is up or down. For an interface that is up, the Ethernet speed and duplex information displays.
   - **Tx Pkts**: The total number of transmitted packets
   - **Tx Dropped**: The total number of transmitted packets that were dropped
   - **Tx Errors**: The total number of transmitted packets that had errors
   - **Rx Pkts**: The total number of received packets
   - **Rx Dropped**: The total number of received packets that were dropped
   - **Rx Errors**: The total number of received packets that had errors

- **Collisions**: The total number of packet collisions
- **Tx Mbps**: The last measured bandwidth for transmitted traffic in Mbps
- **Rx Mbps**: The last measured bandwidth for received traffic in Mbps

5. To display the most recent information, click the **Refresh** button.

Display, save, download, or clear the logs

You can display and manage the activity logs of the router. You can also download a detailed log file.

To display, save, download, or clear the logs:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Monitoring > Logs**.

   The Logs page displays.

   The page display a chronological list of the events that occurred on the router. This information might help you or NETGEAR technical support to troubleshoot any problems, in the unlikely event that this should be necessary.

5. To save the logs, do the following:
   a. Click the **Save** button.
   b. Follow the directions of your browser to save the file to your computer.
6. To download the detailed log entries, do the following:
   a. Click the **Download Detailed Logs** button.
   Depending on the size of the file, downloading the detailed log entries might take several minutes.
   b. Follow the directions of your browser to save the file to your computer.
7. To refresh the log entries onscreen, click the **Refresh** button.

   CAUTION: After you clear the log entries, you can no longer save or download them.

8. To clear the log entries, click the **Clear** button.

Display the status of site-to-site VPN tunnels

You can display the status of site-to-site VPN tunnels that are up or down between the router and a remote endpoint.

For more information about the site-to-site connection settings, see Site-to-site VPN settings on page 154.

To display the status of site-to-site VPN tunnels:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Monitoring > VPN Status**.

   The VPN Status page displays.

   The page displays the total number of configured VPN tunnels (whether enabled or disabled), the number of VPN tunnels that are up, and the number of VPN tunnels that are down (whether enabled or disabled).

   The table displays the following information for each configured VPN tunnel, whether the tunnel is up or down:

   - **Name**: The name of the VPN tunnel (see Add a site-to-site IPSec VPN connection on page 154).
   - **Status**: Displays if the VPN tunnel is up or down. For information about connecting or disconnecting a VPN tunnel, see Connect or disconnect a site-to-site VPN tunnel on page 160.
   - **Phase 2 Enc/Auth/Grp**: The IPSec phase II protocol, encryption, and group settings (see Add an IPSec VPN profile on page 148).
   - **Local Group**. The LAN IP address or group on the router. (see Add a site-to-site IPSec VPN connection on page 154)
   - **Remote Group**. The LAN IP address or group on the remote endpoint (see Add a site-to-site IPSec VPN connection on page 154).
   - **Remote Gateway**. The WAN IP address of the remote endpoint (see Add a site-to-site IPSec VPN connection on page 154).

8

Maintain the Router

This chapter describes how you can maintain the router.

The chapter includes the following sections:

Note: The procedures that are described in this chapter explain how to manage configuration options through the device UI. If you are using the Insight Cloud Portal or Insight app to set up and manage the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

Change the device name

The device name (also referred to as the router name or system name) is the name that displays in the network for the router. By default, the device name is the router model number.

To change the device name:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Administration > General Settings**.
   The General Settings page displays.
5. Type a new name in the **Device Name** field.
   Use the following guidelines:
   - The name must contain only alphanumeric characters and hyphens and cannot be longer than 15 characters.
   - The name must start and end with an alphanumeric character.
6. Click the **Apply** button.
   Your settings are saved.

Manage the firmware of the router

The router firmware is stored in flash memory.

You can check to see if new firmware is available and update the router to the new firmware. You can also visit the NETGEAR support website, download the firmware manually to a local computer, and update the router to the new firmware.

Depending on how you are connected to the router, we recommend the following firmware update methods:

- **WiFi connection**: If an access point is connected to the router and you are connected over WiFi to the router, let the router check the Internet to see if new firmware is available. See Let the router check for new firmware and update the firmware on page 125.
  With this method, if new firmware is available, it is downloaded directly to the router.
- **LAN port connection**: If you are connected over an Ethernet cable to a LAN port of the router, manually update the firmware from a computer. See Manually download firmware and update the router on page 126.
  With this mode, if new firmware is available, you must download it to your computer and then upload it to the router.

Let the router check for new firmware and update the firmware

For you to let the router check for new firmware, the router must be connected to the Internet.

To let the router check for new firmware and update the router:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. In the System Information pane, click the **Check for Update** button.
   The router detects new firmware if any is available and displays the latest version available. If new firmware is available, the name of the button changes to Update Now.
5. If new firmware is available, to download and install the new firmware, click the **Update Now** button.
   A pop-up window displays.
6. Click the **Update** button.
   The router locates the firmware, downloads it, and begins the update.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED and Internet LED are solid green.

   The firmware update process takes several minutes. When the update is complete, your router restarts.
7. Log back in to the router and verify that the router runs the new firmware version.
   The firmware version is displayed in the System Information pane on the Dashboard page.

Manually download firmware and update the router

Downloading firmware to a local computer and updating the router are two separate tasks that are combined in the following procedure.

To download firmware manually and update the router:

1. Visit netgear.com/support/download/, locate the support page for your product, and download the new firmware.
2. Read the new firmware release notes to determine whether you must reconfigure the router after upgrading.

3. Launch a web browser from a computer or mobile device that is connected to the router network.
4. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
5. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
6. Select **Administration > Firmware Update**.
   The Firmware Update page displays.
7. Locate and select the firmware file on your computer by doing the following:
   a. Click the **Browse** button.
   b. Navigate to the firmware file.
      The file name ends in `.bin`.
   c. Select the firmware file.
8. Click the **Update** button.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED and Internet LED are solid green.

   The firmware update process takes several minutes. When the update is complete, the router restarts.
9. Verify that the router runs the new firmware version by logging back in to the router.
   The firmware version is displayed in the System Information pane on the Dashboard page.

Manage the configuration file of the router

The configuration settings of the router are stored within the router in a configuration file. You can back up (save) this file to your computer or restore it.

Back up the router configuration

You can save a copy of the current configuration settings. If necessary, you can restore the configuration settings later.

Note: The backup file is saved in a binary format so that it is protected and cannot be opened by a regular application.

To back up the router's configuration settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Administration > Backup and Restore**.
   The Backup and Restore page displays.
5. Click the **Create Backup** button.
   A pop-up window displays.

6. Enter a password to protect the backup file, and click the **Continue** button.

   You can either use your existing password (the one that you use to log in to the router) or enter a unique password.

   The password must contain alphanumeric and special characters. The following special characters are allowed:

   `!@#$%^&*()`

   Note: We recommend that you save the password because you must enter it again if you restore the configuration from the backup file.

7. Choose a location to store the file on your computer.

   The name of the backup file is in the format `ModelName-ModelNumber-yyyymmdd-hhmmss-config.tar`.

   yyyy is the year, mm is the month, dd is the date, hh is the hour (in 24-hour format), mm are the minutes, and ss are the seconds.

   An example of the name of a backup file is `Router-ABC10-20230721-132812-config.tar`.

   The name is Router; the model is ABC10; the date is July 21, 2023; the time is 1:28:12 p.m.

8. Follow the directions of your browser to save the file.

Restore the router configuration

If you backed up the configuration file, you can restore the configuration from this file.

To restore configuration settings that you backed up:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Administration > Backup and Restore**.
   The Backup and Restore page displays.
5. Click the **Browse** button and navigate to and select the saved configuration file.
   The name of the backup file is in the format `ModelName-ModelNumber-yyyymmdd-hhmmss-config.tar`.

   yyyy is the year, mm is the month, dd is the date, hh is the hour (in 24-hour format), mm are the minutes, and ss are the seconds.

   An example of the name of a backup file is `Router-ABC10-20230721-132812-config.tar`.

   The name is Router; the model is ABC10; the date is July 21, 2023; the time is 1:28:12 p.m.
6. Click the **Restore** button.
   A pop-up window displays.
7. Type the password that you specified when you saved the backup file, and click the **Continue** button.
   The configuration is uploaded to the router. When the restoration is complete, the router reboots. This process takes about two minutes.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the restoration. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED and Internet LED are solid green.

admin user account

The admin user account lets you access the device UI of the router to make configuration changes and monitor the router network.

Change the admin user account password

The admin user account password is the password that you use to log in to the device UI of the router with the user name admin.

These are the requirements for the admin password:

- The password must be 8 to 64 alphanumeric characters and, as an option, can include the following special characters:
  ! @ # $ % ^ & * ( )
- At least one uppercase character
- At least one lowercase character
- At least one numeric character

You cannot change the user name for the admin account (the name is *admin*).

To change the password for the user name admin:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Administration > User Management**.
   The User Accounts page displays.
5. In the Change Password section, click **Change Password**, or click anywhere in the Change Password section
   The section expands.

6. In the **Old Password** field, type your current password.
   If you did not change the password, the current password is the one that you specified when you set up the router.
7. In the **New Password** and **Confirm Password** fields, type the new password.
   For the password requirements, see the introduction to this procedure.
8. Click the **Apply** button.
   Your settings are saved.

   You are logged out from the router. To log back in, use the new password.

Change the session time-out period

The session time-out applies to a device UI session. By default, you are logged out from the device UI after 45 minutes of no activity.

To change the session time-out period:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Administration > User Management**.
   The User Accounts page displays.

5. In the Idle Session Timeout section, use the **Hours** and **Minutes** fields to type the period after which a session automatically expires after no activity and you must log in again to the device UI.

   By default, a session expires after 45 minutes of no activity.

6. Click the **Apply** button.

   Your settings are saved.

Manage the admin password reset option and questions

The admin user account password is the password that you use to log in to the device UI of the router with the user name admin. If you do not know what the password is and you have password recovery enabled, you can reset the password after which you can define a new password with which you can log in to the device UI.

You can enable password recovery by selecting questions and defining answers for the password recovery process. The password recovery process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer.

To manage admin password recovery and set questions and answers:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **Administration > User Management**.

   The User Accounts page displays.

5. Click the **Password Recovery** toggle to enable or disable password recovery:
   - **The toggle is blue and positioned to the right**: Password recovery is enabled, and you can set security questions and provide answers.
   - **The toggle is gray and positioned to the left**: Password recovery is disabled, and the fields for security questions and answers are hidden. This is the default setting.
6. If you enabled password recovery, select two security questions and define answers to them.
7. Click the **Apply** button.
   Your settings are saved.

Reset the admin password

If you enabled password recovery for the admin password (see Manage the admin password reset option and questions on page 133), you can reset the router password if you forgot it. This reset process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer.

After you enter the wrong password three times, the login page displays the Forgot Password? link.

To reset the admin password:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter the wrong password three times.
   The Forgot Password? link displays. Only after you enter the wrong password three times, this link displays.
4. Click the **Forgot Password?** link.
   The Serial Number Validation page displays.
5. In the **Router's Serial Number** field, type the router's serial number.
   You can find the router's serial number on the router label.
6. Click the **Continue** button.
7. Enter your answers to the security questions.

You defined these answers when you set up the password recovery option.

8. Click the **Next** button.
9. Define a new admin password.
   These are the requirements for the admin password:
   - The password must be 8 to 64 alphanumeric characters and, as an option, can include the following special characters:
     `!@#$%^&*()`
   - At least one uppercase character
   - At least one lowercase character
   - At least one numeric character
10. Click the **Next** button.
    Your settings are saved.
11. Click the **Log In Now** button.
    The login page displays.
12. With your new admin password, log in to the router.

Set the time zone and daylight saving time

When the router synchronizes its clock with a Network Time Protocol (NTP) server, the device UI display the date and time. If the device UI does not show the correct date and time, you might need to set the time zone and adjust the daylight saving time (DST) setting.

To set the time zone and adjust the daylight saving time setting:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Administration > Time**.
   The Time page displays.
5. From the **Time Zone** menu, select the time zone for the area in which the router operates.
6. Click the **Automatically adjust time for DST** toggle to enable or disable the DST setting:
   - **The toggle is blue and positioned to the right**: The time is adjusted for DST. This is the default setting.
   - **The toggle is gray and positioned to the left**: The time is not adjusted for DST.
7. Click the **Apply** button.
   Your settings are saved. When the router connects over the Internet to an NTP server, the date and time that display on the page are adjusted according to your settings.

   For information about other time settings, see Set custom NTP servers on page 136.

Set custom NTP servers

By default, the router receives its time from NETGEAR Network Time Protocol (NTP) servers, but you can also specify custom NTP servers.

To set custom NTP servers:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Administration > Time**.
   The Time page displays.
5. Click the **Use Custom NTP Servers** toggle to enable or disable custom NTP servers and the NTP server settings on the page:
   - **The toggle is blue and positioned to the right**: The custom NTP servers and settings are enabled.
   - **The toggle is gray and positioned to the left**: The custom NTP servers and settings are disabled. This is the default setting, which lets the router receive its time from default NETGEAR NTP servers.
6. In the **Primary Server** and **Secondary Server** fields, type either the IPv4 addresses or domain names of the primary and the secondary custom NTP servers.
7. Click the **Apply** button.
   Your settings are saved. When the router connects over the Internet to the custom NTP servers, the date and time that display on the page are adjusted according to your settings.

   For information about setting the time zone, see Set the time zone and daylight saving time on page 135.

Manage the syslog server settings

If a syslog server is present on your network, you can configure the router to send its system logs to the syslog server.

To manage the syslog server settings and enable the syslog server function:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.
   The Dashboard displays.
4. Select **Administration > Syslog**.
   The Syslog page displays.
5. Click the **Remote Syslog** toggle to enable or disable the syslog server and the syslog server settings on the page:
   - **The toggle is blue and positioned to the right**: The syslog server and settings are enabled.
   - **The toggle is gray and positioned to the left**: The syslog server and settings are disabled. This is the default setting.
6. In the **Syslog Server IP Address** field, type the IPv4 address of the syslog server on your network.
7. In the **Port Number** field, type the port number at which the syslog can be reached.
   By default, the port number is 514.
8. Click the **Apply** button.
   Your settings are saved.

Enable or disable UPnP

Universal Plug and Play (UPnP) lets the router be discovered by other devices in a network that support UPnP. For enhanced security, UPnP is disabled by default. For ease of management, you can enable UPnP .

To enable or disable UPnP:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Sekect **Administration > UPnP**.

   The UPnP page displays.
5. Click the **UPnP** toggle to enable or disable UPnP

   - **The toggle is blue and positioned to the right**: UPnP is enabled. The Advertisement Period and Advertisement Time to Live fields display on the page.
   - **The toggle is gray and positioned to the left**: UPnP is disabled. This is the default setting. The Advertisement Period and Advertisement Time to Live fields are hidden on the page.
6. In the **Advertisement Period** field, type the advertisement period in minutes.

   The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points receive current device status

at the expense of more network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.

7. In the **Advertisement Time to Live** field, type the advertisement time to live in hops.
   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value.
8. Click the **Apply** button.
   Your settings are saved.

The UPnP Portmap table displays the IP address of each UPnP device that is accessing the router, the ports (internal and external) that each device opened, and the protocol that each device is using.

Manage the LEDs

By default, all LEDs are enabled and function as described in your hardware installation guide. You can manage whether the LEDs light at all. This function is useful if you want the router to function in a dark environment.

To enable or disable the LEDs:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Administration > LED Control**.
   The LED Control page displays.
5. Select or clear one of the following radio buttons:
   - **Default**. This is the default setting, allowing all LEDs to function with their default behavior.
   - **Turn off all LEDs (Power, Internet, Cloud, and SFP+)**.
   - **Turn off all LEDs except Power LED**.
6. Click the **Apply** button.
   Your settings are saved.

Reboot the router from the device UI

If you cannot physically access the router to reboot it (that is, disconnect the power and reconnect the power), you can use the device UI to reboot the router.

To reboot the router:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. In the System Information pane, click the **Reboot** button.
   A warning pop-up window displays.
5. Click the **Reboot** button.
   The pop-up window closes and the router reboots, which takes about two minutes.

Return the router to its factory default settings

Under some circumstances (for example, if you lose track of the changes that you made to the router settings or you move the router to a different network), you might want to erase the configuration and reset the router to factory default settings.

After you reset the router to factory default settings, if you are connected to the router network, you can *always* use https://www.routerlogin.net or https://www.routerlogin.com to access the device UI of the router. That means that you do not need to know the current IP address of the router to access the device UI.

Note: If you add the router to a NETGEAR Insight network location, you can view the IP address of the router through the Insight Cloud portal or Insight app. For more information, see Add the router to NETGEAR Insight using the Cloud Portal on page 23 or Add the router to NETGEAR Insight using the Insight app on page 25.

To reset the router to factory default settings, you can use either the physical **Reset** button on the router or the reset function in the device UI. However, if you did not add the router to an Insight network location, you lost the password to access the router, and the password recovery option is not enabled, you must use the physical **Reset** button.

After you reset the router to factory default settings, the following occurs:

- The router's DHCP client is enabled.
  By default, the IP address of the router is 192.168.1.1, but this IP address changes after the router receives an IP address from your ISP or a DHCP server in your network. However, if you are connected to the router network, you can *always* use https://www.routerlogin.net or https://www.routerlogin.com to access the device UI of the router.
- The default LAN is set to the default of 192.168.1.1, and the router's DHCP server is enabled.
  If you managed the router with Insight, the router is removed from your Insight account, but you can add it again.

For an extensive list of factory default settings, see the information in the appendix.

Use the device UI to reset the router

You can use the router's device UI to return the router to its factory default settings.

CAUTION: This process erases all settings that you configured in the router.

To reset the router to factory default settings through the device UI:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Administration > Backup and Restore**.
   The Backup and Restore page displays.
5. Click the **Factory Reset** button.
   A pop-up window displays.
6. Click the **Restore** button.
   The configuration is reset to factory default settings. When the reset is complete, the router reboots. This process takes about two minutes.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED and Internet LED are solid green.

Use the Reset button to reset the router

You can use the **Reset** button to return the router to its factory default settings.

CAUTION: This process erases all settings that you configured in the router.

To reset the router to factory default settings:

1. On the front panel of the router, locate the recessed **Reset** button.
2. Using a straightened paper clip, press and hold the **Reset** button for more than five seconds or until the Power LED starts blinking amber.

   If you do not press the **Reset** button long enough, the router only reboots.

3. Release the **Reset** button.

   The configuration is reset to factory default settings. When the reset is complete, the router reboots. This process takes about two minutes.

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

9

Manage IPSec VPN Tunnels

The router supports predefined and manually configured IP security (IPSec) profiles for site-to-site VPN tunnels.

This chapter describes how to set up IPSec VPN profiles and site-to-site connections on the router using the device UI.

For information about monitoring VPN site-to-site connections, see Display the site-to-site VPN configurations or connect or disconnect a VPN tunnel on page 159.

The chapter includes the following sections:

Note: If you are using the Insight Cloud Portal or Insight app to set up IPSec VPN profiles and site-to-site connections on the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

About IPSec VPN

A virtual private network (VPN) site-to-site connection, also referred to as a VPN tunnel, lets you securely connect two networks at different sites over the Internet. One site can be a remote office and the other site can be the company main office. Each location requires a VPN router. VPN access with two routers, each at a different site, lets you connect two local LANs and separate networks together as if they were physically connected and colocated.

Note: The router does not support client-to-gateway connections, whereby a computer or mobile device of a remote user connects through a VPN tunnel directly to a VPN router. The router supports site-to-site connections between two NETGEAR VPN routers or between a NETGEAR VPN router and a third-party VPN router.

The router supports the following types of VPN profiles:

- **Predefined example IPSec VPN profiles**: The device UI includes predefined example VPN IPSec profiles that you can use for paid VPN services. These profiles include *Amazon Web Services* and *Microsoft Azure* (see Predefined example IPSec VPN profiles for paid VPN services on page 147.)
- **Custom IPSec VPN profiles**: You can use the device UI to set up a custom IPSec profile (see Add an IPSec VPN profile on page 148).

After you decide on the VPN profile, you can use it to manually configure a site-to-site VPN connection (see Site-to-site VPN settings on page 154).

IPSec VPN profiles

The router includes predefined example IPSec VPN profiles for paid VPN services (see Predefined example IPSec VPN profiles for paid VPN services on page 147). For any other type of VPN service, you must add a custom IPSec profile.

Note: First set up an IPSec profile, and then define the site-to-site VPN tunnel settings.

An IPSec VPN profile defines the following protocols and security association (SA) settings:

- **IKE version**: The Internet Key Exchange (IKE) version 1 (IKEv1) or 2 (IKEv2) protocol. IKEv2 is more advanced than IKEv1, but there might be situations in which you need to use the older IKEv1. The version that you must select depends on your network requirements.

- **Phase I options**: The IKE Phase I settings define the authentication and negotiation exchange between the two VPN routers *before* the VPN tunnel is established.
  You must specify the encryption and authentication algorithms, as well as the Diffie-Hellman group algorithm for the verification and exchange of keys. Both VPN routers must use the same algorithms so that the communication between the routers can be authenticated and is secure *before* the VPN tunnel is established.
- **Phase II options**: The IKE Phase II settings define how the VPN tunnel is set up and encapsulated between the two VPN routers, and how the VPN tunnel traffic is kept secure *after* it the tunnel established.
  You must specify the encapsulation protocol, encryption algorithm, and an integrity check algorithm that allows the VPN router to guard against modification of the tunnel and the traffic that is transported through the tunnel. Here too, both VPN routers must use the same algorithms.

For more details about these settings, see Add an IPSec VPN profile on page 148.

Predefined example IPSec VPN profiles for paid VPN services

The router includes predefined example VPN IPSec profiles that you can use for paid VPN services. These profiles include *Amazon Web Services* and *Microsoft Azure*.

You can select these IPSec profiles when you add a site-to-site VPN connection (see Add a site-to-site IPSec VPN connection on page 154).

The following table lists the predefined settings for these IPSec profiles. For detailed descriptions of these settings, see Add an IPSec VPN profile on page 148.

Table 2. Predefined example IPSec VPN profiles

Settings	Amazon Web Services	Microsoft Azure
IKE Version	IKE1	IKE1
Phase I Options		
DH Group	Group2 - 1024bits	Group2 - 1024bits
Encryption	AES-128	AES-256
Authentication	SHA1	SHA1
SA lifetime	28800	28800
Phase II Options		
Protocol Selection	ESP	ESP

Table 2. Predefined example IPSec VPN profiles (Continued)

Settings	Amazon Web Services	Microsoft Azure
Encryption	AES-128	AES-256
Authentication	SHA1	SHA1
SA lifetime	3600	3600
DH Group	Group2 - 1024bits	Group2 - 1024bits

Add an IPSec VPN profile

Note: Some knowledge of IPSec VPN can make it easier for you to set up a functioning IPSec VPN profile.

Before you can set up a VPN tunnel between two VPN routers at different sites (see Add a site-to-site IPSec VPN connection on page 154), you must define the IPSec profile that secures the VPN tunnel between the sites.

Internet Key Exchange (IKE) is the protocol that is used to set up security associations (SAs) between VPN routers to ensure the following:

- The VPN tunnel is established between the correct partners (VPN routers).
- The VPN tunnel cannot be altered while traffic is passing through.
- Traffic passing through the VPN tunnel is secured.

The strength of the algorithms that you select for an IPSec VPN profile depends on the sensitivity and the speed of the traffic that must travel through the VPN tunnel for which the profile will be used.

The device UI uses the following icons:

 Add  Edit  Delete

To add an IPSec VPN profile:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **VPN > IPSec Profiles**.
   The IPSec Profiles page displays.
5. Click the **Add** icon.
   The Add/Edit IPSec Profile pop-window displays.
6. In the **Profile Name** field, type a name.
   The name is for identification purposes.
7. Select an IKE Version radio button:
   - **IKEv1**: The profile uses IKEv1. IKEv1 is superseded by IKEv2 but some VPN routers do not support IKEv2. If you do not know if the remote VPN router support IKEv2, we recommend that you use IKEv1.
   - **IKEv2**: The profile uses IKEv2. If the remote VPN router also supports IKE2, we recommend that you use IKE2.
8. In the Phase I Options section, specify the settings as described in the following table.
   The Phase I options determine how the two VPN routers exchange authentication and negotiation messages *before* the VPN tunnel is established, and how these messages are encrypted and authenticated during this phase.

Name	Setting
DH Group	The Diffie-Hellman (DH) group sets the strength of the algorithm in bits. From the menu, select one of the DH groups, each of each of which, in ascending order, provides more security but might require more computing power and slow down the Phase I traffic. The default setting is Group5 - 1536 bits, which provides an algorithm with 1536 bits.
Encryption	Select one of the following encryption algorithms, each of which, in ascending order, provides more security: • **3DES**: Triple Data Encryption Standard (3DES). • **AES-128**: Advanced Encryption Standard (AES) with a 128-bit key size. (The default setting.) • **AES-192**: AES with a 192-bit key size. • **AES-256**: AES with a 256-bit key size.
Authentication	Select one of the following authentication algorithms, each of which, in ascending order, provides more security: • **MD5**: Hash algorithm that produces a 128-bit digest. • **SHA1**: Hash algorithm that produces a 160-bit digest. (The default setting.) • **SHA2-256**: Hash algorithm that produces a 256-bit digest.
SA Lifetime	Type the period in seconds during which the IKE security association (SA) is valid. When the period times out, the next rekeying occurs. The default is 28800 seconds (8 hours). The period can be between 120 and 86400 seconds.

9. In the Phase II Options section, specify the settings as described in the following table.

   The Phase II options determine how the VPN tunnel is set up and encapsulated between the two VPN routers and how the tunnel traffic is kept secure through encryption and authentication *after* the VPN tunnel is established.

Name	Setting
Protocol Selection	The protocol is Encapsulating Security Payload (ESP), which authenticates, encrypts, and guards against data changes during transmission. This is the fixed setting.
Encryption	Select one of the following encryption algorithms, each of which, in ascending order, provides more security: • **3DES**: Triple Data Encryption Standard (3DES). • **AES-128**: Advanced Encryption Standard (AES) with a 128-bit key size. (The default setting.) • **AES-192**: AES with a 192-bit key size. • **AES-256**: AES with a 256-bit key size. • **AES128-GCM-16**: AES with a 128-bit key size and a GCM (Galois/Counter Mode) 16-byte Integrity Check Value (ICV). • **AES256-GCM-16**: AES with a 256-bit key size and a GCM 16-byte ICV.
Authentication	Select one of the following authentication algorithms, each of which, in ascending order, provides more security: • **MD5**: Hash algorithm that produces a 128-bit digest. • **SHA1**: Hash algorithm that produces a 160-bit digest. (The default setting.) • **SHA2-256**: Hash algorithm that produces a 256-bit digest.
SA Lifetime	Type the period in seconds during which the IKE security association (SA) is valid. When the period times out, the next rekeying occurs. The default is 3600 seconds (1 hour). The period can be between 120 and 28800 seconds.
DH Group	The Diffie-Hellman (DH) group sets the strength of the algorithm in bits. From the menu, select one of the DH groups, each of each of which, in ascending order, provides more security but might require more computing power and slow down the Phase II traffic. The default setting is Group5 - 1536 bits, which provides an algorithm with 1536 bits.

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

Change an IPSec VPN profile

You can change an IPSec VPN profile that you added. You cannot change a predefined IPSec VPN profile.

Note: If you change an IPSec profile, make sure that you change the settings accordingly on the remote VPN router.

The device UI uses the following icons:

 Add  Edit  Delete

To change an IPSec VPN profile:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.
   The Dashboard displays.
4. Select **VPN > IPSec Profiles**.
   The IPSec Profiles page displays.
5. In the table, select the check box for the IPSec profile.
6. Click the **Edit** icon.
   The Add/Edit IPSec Profile pop-up window displays.
7. Change the settings for the schedule.
   For more information about the settings, see Add an IPSec VPN profile on page 148.

8. Click the **Apply** button.
   Your settings are saved. The modified IPSec profile displays in the table.

Remove an IPSec VPN profile

If you no longer need an IPSec VPN profile, you can remove it. You cannot remove a predefined IPSec VPN profile.

The device UI uses the following icons:

 Add  Edit  Delete

To remove an IPSec VPN profile:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **VPN > IPSec Profiles**.
   The IPSec Profiles page displays.
5. In the table, select the check box for the IPSec profile.
6. Click the **Delete** icon.
   A pop-up window displays.
7. Click the **OK** button.
   You settings are saved. The IPSec profile is removed from the table.

Site-to-site VPN settings

To set up a site-to-site IPSec VPN tunnel, you do not need to install any software (such as OpenVPN), but the VPN router at the remote site must be capable of supporting IPSec VPN. The site-to-site VPN settings determines the WAN and LAN IP addresses at which the router can reach the remote VPN router.

When you define the settings for a site-to-site VPN tunnel, you must select an IPSec profile that is either predefined (see Predefined example IPSec VPN profiles for paid VPN services on page 147) or that you already set up (Add an IPSec VPN profile on page 148).

In addition, you must define the following VPN settings:

- **Remote endpoint IP address or FQDN**: The WAN address settings of the remote VPN router. The address can be either an IP address or a fully qualified domain name (FQDN).
- **IKE authentication method**: The pre-shared key, which is a password.
- **Local group**: The LAN IP address settings of the local VPN router (that is, the router that you are configuring).
- **Remote group**: The LAN IP address settings of the remote VPN router.
- **Dead peer detection (DPD)**: The DPD detection time and the action that must occur when the router detects that the remote VPN router is not responsive.

Note: The settings that are defined on both VPN routers must match. That is, on each VPN router, the IP addressing scheme must be coordinated with the other VPN router and both the IPSec phase I options and IPSec phase II options must be identical on both VPN routers. If you use two NETGEAR VPN routers for a site-to-site VPN connection, both routers must also be running the same firmware version.

Add a site-to-site IPSec VPN connection

Note: Some knowledge of IPSec VPN tunnels can make it easier for you to set up a functioning VPN connection.

When you add an IPSec VPN tunnel connection, you must do the following, as described in the procedure that follows this list:

- Select an IPSec VPN profile that is predefined (see Predefined example IPSec VPN profiles for paid VPN services on page 147) or that you already set up (Add an IPSec VPN profile on page 148).

- Set the WAN IP address or fully qualified domain name (FQDN) of the remote VPN router.
- Define the password (pre-shared key) that must be used for IKE authentication between the VPN routers.
- Set the local LAN addresses that are used for the VPN tunnel on the router.
- Set the remote LAN addresses that are used for the VPN tunnel on the remote VPN router.
- Specify dead peer detection (DPD) options between the VPN routers.

The device UI uses the following icons:

 Add  Edit  Delete

To add a site-to-site IPSec VPN connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **VPN > Site-to-Site**.
   The Site-to-Site page displays.
5. Click the **Add** button.
   The Add New Connection pop-up window displays.
6. To enable the VPN tunnel after you click the Apply button, keep the **Enable Connection** toggle blue and positioned to the right (the default setting).

This means that the router tries to establish a VPN tunnel with the remote VPN router immediately after you click the Apply button. If you do not want this to happen, click the **Enable Connection** toggle so that it is gray and positioned to the left.

7. In the **Connection Name** field, type a name.
   The name is for identification purposes.
8. From the **IPSec Profile** menu, select an existing profile.
   For more information, see Predefined example IPSec VPN profiles for paid VPN services on page 147 or Add an IPSec VPN profile on page 148.
9. From the **Interface** menu, select the **WAN1** or **WAN2** interface.
   If you did not configure dual WAN (see Set Up and Configure a Dual WAN Connection on page 37), you cannot select the WAN2 interface and the selection is set at WAN1.
10. From the **Remote Endpoint Type** menu, select **Static IP** or **FQDN** and, in the **Remote Endpoint** field, type either the WAN IP address or the domain name of the remote VPN router.
11. In the **Pre-shared Key** field, type the password (pre-shared key) that must be used for IKE authentication between the router and the remote VPN router.
    The same password must be used on the remote VPN router.
    The display the password on the page, click the eye icon.
12. In the Local Group Setup section, specify the settings as described in the following table.
    These setting specify the LAN IP addresses that the VPN tunnel can access on the router.

Setting	Options
Local Identifier Type	Select the type of local identifier: • **IP Address**: The IP address that you want to use for the router. • **Local WAN IP**: The WAN IP address of the router. When you select this option, the Local Identifier field automatically displays the WAN IP address of the router. • **Local FQDN**: The domain name for the router.
Local Identifier	Depending on your selection from the **Local Identifier Type** menu, type either the IP address or domain name. If you select **Local WAN IP**, the field automatically displays the WAN IP address of the router.
Local IP Type	Select the type of local IP addresses and specify the address settings: • **Subnet**: The VPN tunnel can access a local subnet on the router. Type the IP address and subnet mask. • **Single**: The VPN tunnel can access a single IP address on the router. Type the IP address.

13. In the Remote Group Setup section, specify the settings as described in the following table.

    These setting specify the LAN IP addresses that the VPN tunnel can access on the remote VPN router.

    CAUTION: The remote LAN IP addresses and the local LAN IP addresses cannot be in the same subnets. For example, if the local subnet that you specified in the previous step is 192.168.1.x, the remote subnet that you specify in this step can be 192.168.2.x. but cannot be 192.168.1.x.

Setting	Options
Remote Identifier Type	Select the type of remote identifier: • **Remote WAN IP**: The WAN IP address of the remote VPN router. • **Remote FQDN**: The domain name for the remote VPN router.
Remote Identifier	Depending on your selection from the **Remote Identifier Type** menu, type either the IP address or domain name.
Remote IP Type	Select the type of remote IP addresses and specify the address settings: • **Subnet**: The VPN tunnel can access a remote subnet on the remote VPN router. Type the IP address and subnet mask. • **Single**: The VPN tunnel can access a single IP address on the remote VPN router. Type the IP address.

14. In the DPD Option section, specify the settings as described in the following table.
    If the router detects a connection failure with the remote VPN router, it tears down the VPN tunnel and attempts to reestablish it.

Setting	Options
Enable DPD Options	By default, the **Enable DPD Option** toggle is blue and positioned to the right, which means that dead peer detection (DPD) is enabled. To disable DPD, click the **Enable DPD Option** toggle so that the toggle is gray and positioned to the left.
DPD Delay	The period in seconds between consecutive DPD messages. The default is 10 seconds. The period can be between 10 and 300 seconds.
Detection Time	The period in seconds during which the router must receive a DPD response from the remote VPN router. If this period is exceeded, the configured DPD action occurs. The default is 30 seconds. The period can be between 30 and 1800 seconds.
DPD Action	Select the action that must occur if no timely DPD response is received from the remote VPN router: • **Restart**: The router tears down the VPN tunnel and attempts to reestablish it. • **Clear**: The router tears down the VPN tunnel but does not attempt to reestablish it.

15. Click the **Apply** button.
    Your settings are saved. The VPN connection is added to the table on the Site-to-Site page.

If you enabled the new connection (see Step 6), the router immediately attempts to establish the VPN tunnel with the remote VPN router. If you did not enable the new connection, you can do so later (see Connect or disconnect a site-to-site VPN tunnel on page 160).

Display the site-to-site VPN configurations or connect or disconnect a VPN tunnel

You can display the site-to-site VPN configurations.

To display a site-to-site VPN configuration or connect or disconnect a VPN tunnel:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.

   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:

   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **VPN > Site-to-Site**.

   The Site-to-Site page displays.

   The table displays the following information for each site-to-site VPN configuration:

   - **Connection Name**: The name for the site-to-site configuration.
   - **Enabled**: Displays if the VPN configuration is enabled (the check box is selected) or disabled (the check box is cleared).
   - **Remote Endpoint**: The WAN IP address of the remote endpoint.
   - **Interface**: The router interface that is used to reach the remote endpoint. (This is almost always the WAN interface.)

- **IPSec Profile**: The IPSec profile that you selected for the site-to-site configuration.
- **Local Traffic Selection**: The LAN IP address or group on the router.
- **Remote Traffic Selection**: The LAN IP address or group on the remote endpoint.
- **Status**: The status of the VPN tunnel: CONNECTING, CONNECTED, or DOWN.
- **Action**: Display the Connect icon (if the tunnel is down) or the Disconnect icon (if the tunnel is up). To bring up or down the tunnel, do the following:
  - **Connect**: Click the **Connect** icon to let the router bring up the tunnel.
  - **Disconnect**: Click the **Disconnect** icon to let the router bring down the tunnel.

Connect or disconnect a site-to-site VPN tunnel

You can connect (bring up) or disconnect (bring down) a site-to-site VPN tunnel with the click of a button.

To connect or disconnect a site-to-site VPN tunnel:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.
   The Dashboard displays.
4. Select **VPN > Site-to-Site**.
   The Site-to-Site page displays.

5. For the VPN tunnel that you want to connect or disconnect, do one of the following in the Action column:
   - **Connect**: Click the **Connect** icon to let the router bring up the tunnel.
   - **Disconnect**: Click the **Disconnect** icon to let the router bring down the tunnel.

Change a site-to-site VPN connection

You can change a site-to-site VPN connection.

Note: If you change a site-to-site VPN connection, make sure that the settings still work for the remote VPN router.

The device UI uses the following icons:

 Add  Edit  Delete

To change a site-to-site VPN connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **VPN > Site-to-Site**.
   The Site-to-Site page displays.
5. In the table, select the check box for the connection.
6. Click the **Edit** icon.

The Add New Connection pop-up window displays.

7. Change the settings for the connection.
   For more information about the settings, see Add a site-to-site IPSec VPN connection on page 154.
8. Click the **Apply** button.
   Your settings are saved. The modified connection displays in the table.

Remove a site-to-site VPN connection

If you no longer need a site-to-site VPN connection, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

To remove a site-to-site VPN connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **VPN > Site-to-Site**.
   The Site-to-Site page displays.
5. In the table, select the check box for the connection profile.
6. Click the **Delete** icon.

A pop-up window displays.

7. Click the **OK** button.
   You settings are saved. The connection is removed from the table.

Example of a site-to-site VPN tunnel

Consider the following site-to-site VPN example with two NETGEAR routers:

- **NETGEAR VPN router (the local router or local endpoint)**:
  - An ISP assigns the local router a public WAN IP address of 203.0.113.44
  - The local group LAN subnet is 192.168.1.0/24
  - A server that is connected to the local router receives a DHCP-assigned IP address of 192.168.1.25
- **Remote VPN router (the remote endpoint)**:
  - The remote router receives a WAN IP address of 233.252.0.155 (which is the remote gateway IP address)
  - The remote group LAN subnet is 192.168.100.0/24
  - The remote router is connected to an existing office network that includes a storage device with IP address 192.168.100.200

In this VPN configuration, after the VPN tunnel is up, the following applies to a client on the local network (depending on any additional security settings for individual devices):

- The client can ping the remote endpoint (at address 233.252.0.155) and the local router (at address 203.0.113.44) because the client and both routers function in the same VPN network.
- The client can access devices in the LAN subnet 192.168.100.x at the site of the remote endpoint. For example, the client can access a share of the storage device at \\192.168.100.200.
- The client can access devices in the LAN subnet 192.168.1.x at the site of the local endpoint. For example, the client can access the server at \\192.168.1.25.

In general, clients at each site can access devices at both sites, at an IP address in the LAN subnet of each router.

10

Diagnostics and Troubleshooting

This chapter describes how you can perform diagnostics and troubleshoot the router and network using the device UI. Insight users have many additional options that are not described in this user manual, such as the topology viewer.

The chapter includes the following sections:

Note: If you are using the Insight Cloud Portal or Insight app to perform diagnostics and troubleshoot the router, visit kb.netgear.com/000065768 for knowledge base articles about NETGEAR Insight.

Check the Internet speed

You can check the Internet speed of the router.

To check the Internet speed:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.
   The Dashboard displays.
4. Select **Troubleshoot > Speed Test**.
   The Speed Test page displays.
5. Click the **Test Speed** button.
   The Privacy Policy pop-up window displays.
6. Click the **Agree** button.
   After a short delay, the page displays the measured latency (delay) in ms, download speed in Mbps, and upload speed in Mbps.
7. (Optional) To stop the speed test, click the **Stop** button.

   Note: If you do not stop the speed test, the test stops by itself after about 40 seconds, and the name of the Test Speed button changes to Test Again.

8. To view the test history, click the **View History** link.
   A table shows the results of previous tests.

Ping the IP address or domain name of a device or network location

You can ping the IP address of a device or network location from the router to see if the router can reach it. If so, you can view the results of the ping test.

To ping the IP address or domain name of a device or network location:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.
   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.
   The Dashboard displays.
4. Select **Troubleshoot > Ping Test**.
   The Ping Test page displays.
5. Specify the settings that are described in the following table.

Setting	Description
Ping Count	The number of pings that the router must send. The range is from 1 to 1024. The default number is 16.
Packet Size	The size of each ping packet. The range is from 4 to 1024. The default size is 64 bytes.
Ping Interval	The interval between pings. The range is from 1 to 10. The default interval is 1 second.

(Continued)

Setting	Description
Ping Timeout	The period after which a ping times out. The range is from 1 to 300 . The default period is 3 seconds.
Remote Host	The IP address or domain name that the router must ping.
Ping Interface	From the **Ping Interface** menu, select a specific interface or VLAN from which to send the ping, or select **Any** to send the ping from any interface or VLAN: • WAN interfaces are for the physical WAN ports • LAN interfaces are for the physical LAN ports • br-lan, or if you set up a VLAN2 and VLAN3, br-vlan2 and br-vlan3 are the Linux bridge interfaces • VLAN interfaces are the virtual interfaces that are created on top of the physical LAN port For example, "VLAN3 – Ethernet (eth1.3)" is the virtual interface that is created on top of the physical LAN1 port, and it is a bridge port of bridge interface br-vlan3.

6. To start the ping test, click the **Start** button.
7. To stop the ping test before the ping count is reached or if the ping times out, click the **Stop** button.
   The Ping Result section displays the results of your query.

Look up a DNS domain name or IP address

You can look up the DNS domain name or IP address for a web, FTP, mail, or other server on the Internet.

To look up the DNS domain name or IP address for a server on the Internet:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. Select **Troubleshoot > DNS Lookup**.
   The DNS Lookup page displays.
5. In the **Remote Host** field, type the domain name or IP address for which you want to look up the DNS translation.
6. Click the **Start** button.
   The DNS Lookup Result section displays the results of your query.

Trace a route

You can trace a route and display how traffic traverses from the router to its destination on a hop-by-hop basis. The route is displayed after all hops of the traffic path are identified.

To trace a route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.

- If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

For more information about the credentials, see Credentials for the device UI on page 22.

The Dashboard displays.

4. Select **Troubleshoot > Trace Route**.
   The Trace Route page displays.
5. In the **Remote Host** field, type the domain name or IP address for which you want to trace the route.
6. Click the **Start** button.
   The Traceroute Result section displays the results of your query.

Capture Ethernet packets

You can capture Ethernet packets that are received and transmitted by the router and save the file with captured packets to your computer. During the packet capture process, normal functioning of the router is not affected.

The packet capture capability can be useful for analyzing and monitoring the network deployment, debugging protocols, determining network bottlenecks, and, in general, troubleshooting any irregularities in the network.

You can select to capture any packets or packets on a selected LAN or WAN interface, or on a VLAN interface.

Note: To view the captured packets, you need an application that can open `.pcap` files.

To capture packets:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.

3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.

4. Select **Troubleshoot > Packet Capture**.
   The Packet Capture page displays.

   After you configure the packet capture settings and start the capture process, the status of the process displays in the Packet Capture section at the top of the page.

5. Specify the settings that are described in the following table.

Setting	Description
Capture Interface	From the **Capture Interface** menu, select a specific interface or VLAN on which packets must be captured, or select **Any** to capture packets on any interface and VLAN: • WAN interfaces are for the physical WAN ports • LAN interfaces are for the physical LAN ports • br-lan, or if you set up a VLAN2 and VLAN3, br-vlan2 and br-vlan3 are the Linux bridge interfaces • VLAN interfaces are the virtual interfaces that are created on top of the physical LAN port For example, "VLAN3 – Ethernet (eth1.3)" is the virtual interface that is created on top of the physical LAN1 port, and it is a bridge port of bridge interface br-vlan3.
Max. Capture File Size	Type the maximum size that the file with captured packets is limited to. The range is from 64 to 4096 KB. The default is 1024 KB.

(Continued)

Setting	Description
Client Filter	To capture packets for a specific client only, click the **Client Filter** toggle so that it is blue and positioned to the right and type the client's MAC address in the **Client Filter** field. The MAC address must be in hexadecimal format with each octet separated by a hyphen, for example 00-11-22-33-44-55. By default, the Client Filter toggle is gray and positioned the left, indicating that client filtering is disabled and packets for *all* clients are captured.
Capture Duration	Type the maximum duration of the capture process (that is, if you do not click the **Stop** button). The range is from 10 to 3600 seconds. By default, the maximum duration is 300 seconds.

6. To start the packet capture process, click the **Start** button.
   If any captured packets are already stored on the router, you are prompted to allow the packet capture process to overwrite the old information.
7. To stop the packet capture process, click the **Stop** button.
   If you do not stop the process manually, the process is automatically stopped when the capture duration period is exceeded.
8. To download the file with captured packets, do the following:
   a. Click the **Download** button.
   b. Follow the directions of your browser to save the file to your computer.

Sequence to restart the router network

When you restart the router network, follow this sequence:

1. Disconnect the router from the modem or network router.
2. Turn off the router.
3. If you use a modem, do the following:
   a. Unplug the modem's power, leaving the modem connected to the wall jack for your Internet service.
   b. If the modem uses a battery backup, remove the battery, wait 10 seconds, and put the battery back in.

4. Reconnect the router to the modem or network router.
5. If you use a modem, turn on the modem and wait two minutes.
6. Turn on the router and wait until the Power LED and Internet LED light solid green.

Troubleshoot with the LEDs

For general information about the LEDs and LED icons, see the hardware installation guide for your router.

When you connect the router to a power source and you did not disable the LEDs (see Manage the LEDs on page 140), the LEDs light as described here:

1. **Power LED**: When you turn on the router, the Power LED lights solid amber. In about one minute, the Power LED turns solid green, indicating that the startup procedure is complete and the router is ready.
2. **Internet LED**: When you turn on the router, the Internet LED remains off. After about one minute, the router attempts to get an Internet connection and the Internet LED lights blinking amber. When the router establishes an Internet connection, the Internet LED lights solid green.
3. **LAN LEDs**: When the startup procedure is complete, verify that for a LAN port to which a device is connected, the associated LAN LED lights green (solid or blinking) or amber (solid or blinking). The LED color depends on the speed of the Ethernet link.

You can use the LEDs for troubleshooting. For more information, see the following sections:

- Power LED remains off
- Power LED does not turn green
- Internet LED remains blinking amber or off
- Cloud LED does not light blue if you use NETGEAR Insight
- A LAN LED is off while a device is connected

Power LED remains off

If the Power LED remains off when you connect the router to a power source, check the following:

- Make sure that the power adapter is securely connected to your router and securely connected to a working power outlet.
- If you use a power strip or surge protector, make sure that it is turned on.

- Make sure that you are using the power adapter that NETGEAR supplied for this product.

Power LED does not turn green

When you turn on the router, the Power LED lights solid amber. In about one minute, the Power LED turns solid green, indicating that the startup procedure is complete and the router is ready.

When the router is upgrading firmware, the Power LED blinks amber temporarily and finally lights solid green.

If the Power LED remains solid amber five minutes after startup, or is blinking amber at any other time (not including a firmware upgrade), this indicates a problem with the router. In that situation, do the following:

- Restart the router to see if it recovers. If the problem occurs again, try one more time.
- If the router does not recover, press and hold the **Reset** button on the back to return the router to its factory default settings. For more information, see Use the Reset button to reset the router on page 144. If the problem occurs again, try one more time.

If the error persists, a hardware problem might be the cause. Contact NETGEAR technical support at netgear.com/support/.

Internet LED remains blinking amber or off

When you turn on the router, the Internet LED remains off. In about one minute, the router attempts to get an Internet connection and the Power LED lights blinking amber. When the router establishes an Internet connection, the Internet LED light solid green.

If the Internet LED remains blinking amber or off, the router did not get an Internet connection. Check the following:

- Make sure that the Ethernet cable connection is secure at the yellow WAN1 port (do *not* use a LAN port for this connection) of the router and at an Ethernet port on the modem or network router.
- Make sure that power is turned on to the connected modem or network router. When you connect the router's WAN1 port to a modem or network router, use the cable that was supplied with the device. This cable can be a standard straight-through Ethernet cable or an Ethernet crossover cable.
- Make sure that your Internet service provider (ISP) is not experiencing an Internet outage.

- Make sure that you completed the initial log-in process (see Set up the router with an Internet connection on page 12). You can also manually set up your Internet connection (see Manage the Internet Settings for the WAN1 port on page 29).
- If you use a modem and the type of WAN connection of your modem is PPPoE or requires a static IP address, make sure that you configured the Internet settings correctly.
  For more information, see Manually configure a PPPoE Internet connection for the WAN1 port on page 34 or Manually configure a static Internet connection for the WAN1 port on page 32.

Cloud LED does not light blue if you use NETGEAR Insight

If you do *not* add the router to a NETGEAR Insight network location, the Cloud LED is off. This is normal LED behavior.

If you *do* add the router to an Insight network location to manage the router through the Insight Cloud portal or Insight app, the Cloud LED lights as follows:

- **Blue**: The router is connect to the Insight cloud-based management platform.
- **Off**: The router did not get a connection to the Insight cloud-based management platform.

If you use the Insight Cloud portal or Insight app to manage the router and the Cloud LED remains off, try the following troubleshooting steps until the problem is resolved:

1. Make sure that the Insight mode in the device UI is enabled.
   For more information, see Change the Insight management mode on page 26.
2. Make sure that the Ethernet cable connection between the router and your modem or network router is good.
3. Make sure that the router is connected to the Internet and that the Internet connection is good.
4. Make sure that the router is running the latest firmware version.
   For more information, see Manage the firmware of the router on page 125.
5. Restart your network and wait five minutes to see if the Cloud LED lights blue.
   For more information, see Sequence to restart the router network on page 171.
6. If the problem is still not resolved, use the **Reset** button to return the router to its factory default settings, reconfigure the router, and check to see if the router can get a connection to the Insight cloud-based management platform.
   For more information, see Use the Reset button to reset the router on page 144.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact technical support at netgear.com/support.

A LAN LED is off while a device is connected

If a LAN LED remains off while a powered-on device is connected, check these items:

- Make sure that the Ethernet cable connectors are securely plugged in at the router and the network device.
- Make sure that the connected network device is turned on.
- Make sure that you are using the correct Ethernet cable. Use a standard Category 5e or higher-rated Ethernet cable. If the network device incorporates Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.
- Check to see if the LEDs are disabled (see Manage the LEDs on page 140).

You cannot log in to the device UI of the router

If you are connected to the router network, you can *always* use https://www.routerlogin.net or https://www.routerlogin.com to access the device UI of the router. That means that you do not need to know the current IP address of the router to access the device UI.

If you are unable to log in to the router's device UI from a computer, check the following:

- Your browser might display a security warning because of the self-signed certificate on the router, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see kb.netgear.com/000062980//.
- Make sure that you are using the correct login information. The user name is **admin** and the password is the one that you specified when you first logged in. The user name and password are case-sensitive.
  If you added the router to a NETGEAR Insight network location and are also managing the router through the Insight Cloud portal or Insight app, enter the Insight network password for that location.

  Note: When you add the router to an Insight network location, the password for the device UI is replaced by the password for the Insight network location.

- Make sure that the IP address of your computer is in the same subnet as the router. If you disabled the router's DHCP client and configured a fixed (static) IP address when you connected the router to your network (see Add a VLAN profile on page

57 or Change a VLAN profile on page 62), change the IP address and subnet mask on your computer to so that the IP addresses of your computer and the router are in the same IP subnet.

- Try quitting the browser and launching it again.
- Make sure that JavaScript is enabled in your browser.

Troubleshoot Internet browsing

If a computer or mobile device is connected to the router but unable to load any web pages from the Internet, it might be for one of the following reasons:

- The computer of mobile device might not recognize any DNS server addresses.
  If you manually entered a DNS address when you set up the router (that is, the router uses static IP address settings), restart the computer or mobile device so that it can detect the DNS addresses.
- The computer or mobile device might not use the correct TCP/IP settings.
  If the computer or mobile device obtains its information through DHCP, restart the computer or mobile device and verify that its IP address is in the DHCP address range that the router is using.
  For information about TCP/IP problems, see Troubleshoot the network using your computer's ping utility on page 178.

Changes are not saved

If you are logged in to the router's device UI and the router does not save the changes that you make on a page, do the following:

- When entering configuration settings, always click the **Apply** button in the device UI before moving to another page or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. It is possible that the changes occurred but that the old settings remain in the web browser's cache.

Check the WAN port IP address

Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the Dashboard.

To check the WAN port (Internet) IP address:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. In the address field of your browser, enter **https://www.routerlogin.net**.
   The login page displays.

   Your browser might display a security warning. For more information, see Log in to the device UI on page 27.
3. Enter one of the following passwords:
   - Enter the router user name and password. The user name is **admin**. The password is the one that you specified when you set up the router. The user name and password are case-sensitive.
   - If you are also managing the router through the Insight Cloud Portal or Insight app, enter the Insight network password for the Insight network location to which the router is added.

   For more information about the credentials, see Credentials for the device UI on page 22.

   The Dashboard displays.
4. In the Internet Port Status pane, the connection status information displays.

   Note: The information that displays depends on the type of Internet connection. If the Internet connection is PPPoE, other information might display than if the Internet connection is an IP address that the ISP assigns dynamically (the most common situation).
5. Check to see that a valid IP address is shown in the IP address field.
   If no IP address is shown, the router did not obtain an IP address from your ISP.
6. If no IP address is shown, click the **Renew** button.
   The router attempts to obtain an IP address from your ISP.

If the router cannot obtain an IP address from the ISP, you might need to restart your network. For more information, see Sequence to restart the router network on page 171.

If the router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- You might be using incorrect settings for your ISP connection.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account as the account name.
- If your ISP allows only one Ethernet MAC address to connect to the Internet and checks for your computer's MAC address, do one of the following:
  - Inform your ISP that you bought a new network device and ask them to use the router's MAC address.
  - Configure the router to use your computer's MAC address.

For more information about changing the ISP settings (that is, the settings for the Internet connection), see Manage the Internet Settings for the WAN1 port on page 29 and Set Up and Configure a Dual WAN Connection on page 37.

You enter the wrong password and can no longer log in to the router

If you enter the wrong admin password five times, access to the router's device UI is blocked for 5 minutes. Wait 5 minutes, and try again.

If you forgot your password and you did not enable password recovery (see Manage the admin password reset option and questions on page 133), you must reset the router to factory default settings (see Use the Reset button to reset the router on page 144) so that you can regain access to the device UI.

Troubleshoot the network using your computer's ping utility

Many computers contain a ping utility that can send an echo request packet to a designated device, which then responds with an echo reply. You can troubleshoot the network using the ping utility in your computer.

Test the LAN path to your router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a Windows-based computer:

1. From the Windows taskbar, click the **Start** button and find and select **Run**.
2. In the field provided, enter **ping** followed by the IP address of the router, as in this example:
   ping 192.168.1.1
3. Click the **OK** button.
   A message such as the following one displays:
   ```
   Pinging <IP address> with 32 bytes of data
   ```
   If the path is working, you see this message:
   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```
   If the path is not working, you see this message:
   ```
   Request timed out
   ```

If the path is not functioning correctly, one of the following problems might be occurring:

- Wrong physical connections
  Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.
- Wrong network configuration
  Verify that the IP addresses for your computer and the router are correct and that the addresses are in the same subnet.

Test the path from your computer to a remote device

After you verify that the LAN path works correctly, test the path from your computer to a remote device.

To test the path from your computer to a remote device:

1. From the Windows taskbar, click the **Start** button and find and select **Run**.
2. In the field provided, enter **ping -n 10** *IP address*.
   IP address is the IP address of a remote device such as a remote DNS server.

If the path is functioning correctly, replies as described in Test the LAN path to your router on page 179 display.

If you do not receive replies, check the following:

- Your computer lists the IP address of the router as the default gateway. (If the IP configuration of your computer is assigned by DHCP, this information might not be visible in your computer.)
- The network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Your modem is connected and functioning.

A

Supplemental information

This appendix includes technical information about your router.

The appendix covers the following topics:

- Factory default settings
- Technical specifications

Factory default settings

You can reset the router to the factory default settings, which are shown in the following table.

For more information about resetting the router to its factory settings, see Return the router to its factory default settings on page 142.

Table 3. Factory default settings

Feature	Default Setting
Management and login settings	
Management mode	Standalone *and* NETGEAR Insight remote management (Both modes are supported simultaneously.)
User login URL	www.routerlogin.net (or www.routerlogin.com or 192.168.1.1)
User name	**admin**, nonconfigurable
Router login password	The first time that you log in to the device UI, you must define the router login password. If you add the router to a NETGEAR Insight network location and are also managing the router through the Insight Cloud portal or Insight app, enter the Insight network password for the Insight network location. For more information, see Credentials for the device UI on page 22.
Idle session time-out	45 minutes
Password recovery	Disabled
Internet connection	
WAN MAC address	Use default hardware address
WAN MTU size	Determined by the protocol that is used for the Internet connection
Port speed	AutoSensing
Default VLAN and LAN	
LAN IP address	192.168.1.1
Subnet mask	255.255.255.0
DHCP server	Enabled
DHCP range	192.168.1.2 to 192.168.1.250
DHCP starting IP address	192.168.1.2
DHCP ending IP address	192.168.1.250

Table 3. Factory default settings (Continued)

Feature	Default Setting
VLANs	VLAN 1 with all LAN ports as untagged members
General system settings	
Time zone	North America: Pacific Standard Time Europe: GMT Other continents: Varies by region
Time adjusted for daylight saving time	Enabled, depending on the selected time zone
NTP client	Enabled
Syslog	Disabled
UPnP	Disabled
LEDs	All enabled
Services	Preconfigured services: FTP, HTTP, HTTPS, DNS-TCP, DNS-UDP, ICMP Destination Unreachable, ICMP Ping Reply, ICMP Ping Request, IMAP3, NFS, POP3, SMTP, and SNMP
WAN security and Firewall	
Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
Outbound (communications going out to the Internet)	Enabled (all)
Port scan and DoS protection	Enabled
DMZ server	None
Respond to ping on Internet port	Disabled
SIP ALG	Enabled
TCP session time-out	1800 seconds
ICMP session time-out	30 seconds
Maximum concurrent connections	60,000
IPSec pass-through	Enabled
PPTP pass-through	Enabled
L2TP pass-through	Enabled

Table 3. Factory default settings (Continued)

Feature	Default Setting
Traffic rules	None set up
Port forwarding rules	None set up
Port triggering rules	None set up
VPN	
IPSec profiles	Amazon Web Services Microsoft Azure

Technical specifications

The following table shows the technical specifications. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 4. Technical specifications

Feature	Description
Protocols for Internet connections	IPv4, DHCP, PPPoE
Power adapter	AC Input: 100-240V, 50/60Hz, 1.3A The plug is localized to the country of sale.
Hardware interfaces	One RJ-45 10G/Multi-Gigabit port that supports 10G, 5G, 2.5G, 1G, and 100M, and that is configurable as the LAN5 port or WAN2 port. One RJ-45 Multi-Gigabit WAN port that supports 2.5G, 1G, and 100M Three RJ-45 Multi-Gigabit LAN ports that supports 2.5G, 1G, and 100M One 10G/1G SFP+ LAN fiber port All RJ-45 Multi-Gigabit ports support Auto Uplink (Auto MDI-X)
Dimensions (L x W x H)	17.3 x 3.9 x 1.7 in (440 x 100 x 43 mm)
Weight	3.34 lb (1513 g)
Operating temperature	32°F to 104°F (0°C to 40°C)
Operating humidity	Up to 90% maximum relative humidity, noncondensing
Storage temperature	–4°F to 158°F (–20°C to 70°C)

Table 4. Technical specifications (Continued)

Feature	Description
Storage humidity	Up to 95% maximum relative humidity, noncondensing
Major Regulatory Compliance	Environment: RoHS Safety: CE/LVD, CSA EMI: FCC Part 15 Class B, CE mark