

**NETGEAR®**

# User Manual

---

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

Model PR460X

May 2025  
202-12671-06

**NETGEAR, Inc.**

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

## **Support and Community**

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

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

## **Regulatory and Legal**

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

## **Trademarks**

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

## Revision History

Publication Part Number	Publish Date	Comments
202-12671-06	May 2025	<p>We added the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Change the color theme of the device UI</a> on page 34</li> <li>• <a href="#">Manage secure DNS</a> on page 53 and subsections: <ul style="list-style-type: none"> <li>◦ <a href="#">About secure DNS</a> on page 54</li> <li>◦ <a href="#">Enable a secure DNS</a> on page 55</li> <li>◦ <a href="#">Add a new secure DNS</a> on page 56</li> <li>◦ <a href="#">Edit a secure DNS</a> on page 58</li> <li>◦ <a href="#">Remove a secure DNS</a> on page 59</li> <li>◦ <a href="#">Enable fallback to plain DNS</a> on page 60</li> </ul> </li> <li>• <a href="#">Configure dual WAN load balancing</a> on page 81</li> <li>• <a href="#">Link aggregation</a> on page 113 and subsections: <ul style="list-style-type: none"> <li>◦ <a href="#">Enable link aggregation</a> on page 113</li> <li>◦ <a href="#">Make a link aggregation connection</a> on page 117</li> <li>◦ <a href="#">Set up a static link aggregation group</a> on page 115</li> <li>◦ <a href="#">Set up a dynamic link aggregation group</a> on page 116</li> </ul> </li> </ul> <p>We added an automatic sequential IP address option to the DHCP server:  <a href="#">Add a VLAN profile</a> on page 89.</p> <p>We made minor changes and improvements.</p>
202-12671-05	December 2024	<p>We added the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Dual WAN traffic rule</a> on page 127 and subsections</li> <li>• <a href="#">Outbound NAT rule</a> on page 138</li> <li>• <a href="#">Simple Network Management Protocol</a> on page 200 and subsections</li> <li>• <a href="#">Configure remote device management and DPD options for a site-to-site IPSec VPN connection</a> on page 231</li> </ul> <p>We revised the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Manage the Internet Settings for the WAN1 port</a> on page 45</li> <li>• <a href="#">Set Up and Configure a Dual WAN Connection</a> on page 66</li> <li>• <a href="#">Add a site-to-site IPSec VPN connection</a> on page 227</li> </ul>

(Continued)

Publication Part Number	Publish Date	Comments
202-12671-04	October 2024	<p>We added the chapter <a href="#">Manage WireGuard VPN Tunnels</a> on page 291.</p> <p>We added the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">About the device UI and the NETGEAR Engage Controller</a> on page 18</li> <li>• <a href="#">Engage Controller management</a> on page 29 and the subsections <a href="#">How the Engage Controller and the device UI interact with each other</a> on page 30 and <a href="#">Use the NETGEAR Engage Controller to add a PR460X Pro Router to an Engage site</a> on page 31</li> <li>• <a href="#">Display the status of client-to-site WireGuard VPN tunnels</a> on page 178</li> </ul> <p>We changed the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Introduction</a> on page 15</li> <li>• <a href="#">How to manage the router</a> on page 17</li> <li>• <a href="#">Decide on the router management method</a> on page 28</li> <li>• <a href="#">Credentials for the device UI</a> on page 42</li> </ul> <p>In addition, we revised all procedures to include additional information about the password that you must use to log in to the device UI.</p> <p>We made minor changes and improvements.</p>
202-12671-03	July 2024	<p>We added the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Change the language of the device UI</a> on page 34</li> <li>• <a href="#">Display the status of active client-to-site OpenVPN tunnels or disconnect a tunnel</a> on page 177</li> <li>• <a href="#">Client-to-site OpenVPN settings</a> on page 254 and subsections: <ul style="list-style-type: none"> <li>◦ <a href="#">Enable and configure OpenVPN on the router</a> on page 254</li> <li>◦ <a href="#">Configure duplicate connections, client isolation, a domain name, and a split tunnel for a client-to-site OpenVPN connection</a> on page 259</li> <li>◦ <a href="#">Export the router's OpenVPN client configuration file</a> on page 262</li> <li>◦ <a href="#">Install OpenVPN client software and the VPN router client configuration file on a remote client</a> on page 263 and subsections</li> </ul> </li> </ul> <p>We added an appendix: <a href="#">Configure IPSec VPN Client Settings</a> on page 331.</p> <p>We changed the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Add a VLAN profile</a> on page 89</li> <li>• <a href="#">Add a VPN user account</a> on page 267</li> <li>• <a href="#">Change a VPN user account</a> on page 268</li> <li>• <a href="#">Renew a certificate authority</a> on page 279</li> </ul>

(Continued)

Publication Part Number	Publish Date	Comments
202-12671-02	April 2024	<p>We added the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Dynamic DNS</a> on page 61 and subsections</li> <li>• <a href="#">Enable the mDNS Gateway</a> on page 111</li> <li>• <a href="#">Enable or disable LLDP and display the LLDP neighbors</a> on page 199</li> <li>• <a href="#">Display the status of active client-to-site IPSec VPN tunnels or disconnect a tunnel</a> on page 175</li> <li>• IPSec client-to-site VPN sections: <ul style="list-style-type: none"> <li>◦ <a href="#">Predefined IPSec VPN profiles for client-to-site VPN connections</a> on page 220</li> <li>◦ <a href="#">Client-to-site IPSec VPN settings</a> on page 238 and subsections</li> <li>◦ <a href="#">VPN user accounts</a> on page 266 and subsections</li> <li>◦ <a href="#">Certificates</a> on page 271 and subsections</li> </ul> </li> <li>• <a href="#">Manage the QoS Settings</a> on page 305 and subsections</li> <li>• <a href="#">Install and Launch Third-Party Applications</a> on page 309 and subsections</li> </ul> <p>We revised the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">Manually configure a PPPoE Internet connection for the WAN1 port</a> on page 51 and <a href="#">Configure dual WAN with a PPPoE Internet connection for the WAN2 port</a> on page 74</li> <li>• <a href="#">How the router uses VLANs and LANs</a> on page 87</li> <li>• <a href="#">Manage timeouts for TCP, UDP, and ICMP sessions</a> on page 124</li> <li>• <a href="#">Display the router connectivity, system, port, IPSec VPN, and VLAN settings</a> on page 166</li> <li>• <a href="#">About IPSec VPN</a> on page 218</li> <li>• <a href="#">IPSec VPN profiles</a> on page 218</li> <li>• <a href="#">Predefined IPSec VPN profiles for site-to-site VPN connections</a> on page 219</li> <li>• <a href="#">Add a site-to-site IPSec VPN connection</a> on page 227</li> </ul> <p>We made multiple minor changes and improvements.</p>
202-12671-01	August 2023	First publication.

# Contents

## **Chapter 1 Introduction**

Additional documentation.....	17
How to manage the router.....	17
About the device UI and the NETGEAR Engage Controller.....	18
About the device UI and NETGEAR Insight.....	19

## **Chapter 2 Set Up and Access the Router**

Set up the router with an Internet connection.....	21
Example of a router setup with a connection to a modem.....	22
Set up the router to connect to a modem.....	23
Set up the router to connect to the LAN of an existing router.	24
Set up the router offline using a directly connected computer.....	26
Decide on the router management method .....	28
Engage Controller management.....	29
How the Engage Controller and the device UI interact with each other.....	30
Use the NETGEAR Engage Controller to add a PR460X Pro Router to an Engage site.....	31
Log in to the device UI.....	32
Change the language of the device UI.....	34
Change the color theme of the device UI.....	34
Insight remote management.....	35
Pre-onboard the router with Insight and plug-and-play.....	37
How Insight and the device UI interact with each other.....	37
Add the router to NETGEAR Insight using the Cloud Portal ..	39
Add the router to NETGEAR Insight using the Insight app.....	40
Change the Insight management mode.....	41
Credentials for the device UI.....	42

## **Chapter 3 Manage the Internet Settings for the WAN1 port**

Manually configure a dynamic Internet connection for the WAN1 port.....	46
Manually configure a static Internet connection for the WAN1 port.....	48
Manually configure a PPPoE Internet connection for the WAN1 port.....	51
Manage secure DNS.....	53
About secure DNS.....	54

Enable a secure DNS.....	55
Add a new secure DNS.....	56
Edit a secure DNS.....	58
Remove a secure DNS.....	59
Enable fallback to plain DNS.....	60
Dynamic DNS.....	61
Add a dynamic DNS profile.....	61
Change, enable, or disable a dynamic DNS profile.....	63
Remove a dynamic DNS profile.....	64

## **Chapter 4 Set Up and Configure a Dual WAN Connection**

About Dual WAN and WAN failover.....	67
Configure dual WAN with a dynamic Internet connection for the WAN2 port.....	68
Configure dual WAN with a static Internet connection for the WAN2 port.....	71
Configure dual WAN with a PPPoE Internet connection for the WAN2 port.....	74
Configure dual WAN failover detection.....	78
Configure dual WAN load balancing.....	81
Display the status of the dual-WAN interfaces.....	83

## **Chapter 5 Manage the LAN and VLAN Settings**

VLAN concepts.....	86
Basic VLAN concepts.....	86
Management VLAN.....	87
How the router uses VLANs and LANs.....	87
Example of how the router processes traffic.....	88
VLANs and LANs.....	89
Add a VLAN profile.....	89
Assign a VLAN to a LAN port.....	93
Change a VLAN profile.....	94
Remove a VLAN profile.....	95
Manage IEEE, flow control, and link speed for ports.....	97
MAC address to IP address bindings.....	99
Add a MAC-IP binding for a detected device.....	99
Manually add a MAC-IP binding.....	100
Import a list with MAC-IP bindings.....	102
Change a MAC-IP binding.....	103
Remove a MAC-IP binding.....	104
Export a list with MAC-IP bindings.....	105
Static routes.....	106
Add a static route.....	107
Change a static route.....	109

Remove a static route.....	110
Enable the mDNS Gateway.....	111
Link aggregation.....	113
Enable link aggregation.....	113
Set up a static link aggregation group.....	115
Set up a dynamic link aggregation group.....	116
Make a link aggregation connection.....	117

## **Chapter 6 Manage the Firewall and Security**

Manage protection for port scans, denial of service, and pings.	120
Set up a DMZ server.....	121
Manage the SIP application-level gateway.....	122
Manage timeouts for TCP, UDP, and ICMP sessions.....	124
Manage VPN pass-through for tunnel protocols.....	125
Firewall traffic rules.....	126
Dual WAN traffic rule.....	127
Add a dual WAN traffic rule.....	128
Change a dual WAN traffic rule or its priority, or enable or disable the rule.....	130
Remove a dual WAN traffic rule.....	131
General outbound traffic rule.....	132
Add a general outbound traffic rule.....	133
Change a general outbound traffic rule or its priority, or enable or disable the rule.....	135
Remove a general outbound traffic rule.....	137
Outbound NAT rule.....	138
Add an outbound NAT rule.....	138
Change an outbound NAT rule and enable or disable the rule.....	140
Remove an outbound NAT rule.....	141
Port forwarding.....	142
Add a port forwarding rule.....	143
Change, enable, or disable a port forwarding rule.....	145
Remove a port forwarding rule.....	146
Application example: Make a local web server public.....	147
Port triggering.....	148
Add a port triggering rule.....	148
Change, enable, or disable a port triggering rule.....	150
Remove a port triggering rule.....	151
Application example: Port triggering for Internet Relay Chat.	152
Enable or disable UPnP.....	153
Services, protocols, and port numbers.....	155
Add a service.....	156
Change a service.....	158

Remove a service.....	159
Schedules.....	160
Add a schedule.....	160
Change a schedule.....	162
Remove a schedule.....	163

## **Chapter 7 Monitor the Router and its Network**

Display alarms, warnings, and notifications.....	165
Display the router connectivity, system, port, IPsec VPN, and VLAN settings.....	166
Display devices attached to the router LAN ports.....	169
Display the DHCP leases for a VLAN or add a MAC-IP binding.	170
Display Ethernet traffic statistics for the WAN and LAN ports...	171
Display, save, download, or clear the logs.....	173
Display the status of site-to-site VPN tunnels.....	174
Display the status of active client-to-site IPsec VPN tunnels or disconnect a tunnel.....	175
Display the status of active client-to-site OpenVPN tunnels or disconnect a tunnel.....	177
Display the status of client-to-site WireGuard VPN tunnels.....	178

## **Chapter 8 Maintain the Router**

Change the device name.....	182
Manage the firmware of the router.....	183
Let the router check for new firmware and update the firmware.....	183
Manually download firmware and update the router.....	184
Manage the configuration file of the router.....	186
Back up the router configuration.....	186
Restore the router configuration.....	187
admin user account.....	189
Change the admin user account password.....	189
Change the session time-out period.....	190
Manage the admin password reset option and questions....	191
Reset the admin password.....	192
Set the time zone and daylight saving time.....	194
Set custom NTP servers.....	195
Manage the syslog server settings.....	196
Enable or disable UPnP.....	197
Enable or disable LLDP and display the LLDP neighbors.....	199
Simple Network Management Protocol.....	200
Configure the SNMP system name, contact and location....	201
Configure the SNMPv1 and SNMPv2 client.....	202
Configure the SNMPv3 user account.....	203

Manage the SNMPv1, SNMPv2, and SNMPv3 trap recipients.	204
Add an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps.....	204
Change an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receives traps.....	207
Delete an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps.....	208
Configure trap flags.....	209
Display the supported MIBs.....	211
Manage the LEDs.....	211
Reboot the router from the device UI.....	213
Return the router to its factory default settings.....	214
Use the device UI to reset the router.....	214
Use the Reset button to reset the router.....	216

## **Chapter 9 Manage IPsec VPN and OpenVPN Tunnels**

About IPsec VPN.....	218
IPsec VPN profiles.....	218
Predefined IPsec VPN profiles for site-to-site VPN connections.....	219
Predefined IPsec VPN profiles for client-to-site VPN connections.....	220
Add a custom IPsec VPN profile.....	221
Change an IPsec VPN profile.....	225
Remove an IPsec VPN profile.....	226
Site-to-site VPN settings.....	227
Add a site-to-site IPsec VPN connection.....	227
Configure remote device management and DPD options for a site-to-site IPsec VPN connection.....	231
Display the site-to-site VPN configurations or connect or disconnect a VPN tunnel.....	233
Connect or disconnect a site-to-site VPN tunnel.....	234
Change a site-to-site VPN connection.....	235
Remove a site-to-site VPN connection.....	236
Example of a site-to-site VPN tunnel.....	237
Client-to-site IPsec VPN settings.....	238
Operating systems, tunneling protocol, and authentication supported for VPN clients.....	240
Add a client-to-site IPsec VPN connection.....	240
Configure client isolation, a split tunnel, and DPD options for a client-to-site IPsec VPN connection.....	243
Display the client-to-site VPN configurations.....	246
Enable or disable a client-to-site IPsec VPN connection.....	247
Change a client-to-site VPN connection.....	248

Remove a client-to-site VPN connection.....	249
Client-to-site VPN tunnel examples.....	250
Client-to-site VPN tunnel with the router directly connected to the Internet through a modem.....	251
Client-to-site VPN tunnel with the router behind another router.....	252
Client-to-site OpenVPN settings.....	254
Enable and configure OpenVPN on the router.....	254
Enable and configure OpenVPN with TUN mode on the router.....	255
Enable and configure OpenVPN with TAP mode on the router.....	257
Configure duplicate connections, client isolation, a domain name, and a split tunnel for a client-to-site OpenVPN connection..	259
Export the router's OpenVPN client configuration file.....	262
Install OpenVPN client software and the VPN router client configuration file on a remote client.....	263
Install the OpenVPN client utility and configuration file for TUN mode on a Windows-based computer.....	263
Install the OpenVPN client utility and configuration file for TAP mode on a Windows-based computer.....	264
Install the OpenVPN client utility and configuration file for TUN mode on a Mac.....	264
Install the OpenVPN client utility and configuration file for TAP mode on a Mac.....	265
Install the OpenVPN Connect app and client configuration file for TUN mode on an Android device.....	265
Install the OpenVPN Connect app and client configuration file for TUN mode on an iOS device.....	266
VPN user accounts.....	266
Add a VPN user account.....	267
Change a VPN user account.....	268
Remove a VPN user account.....	270
Certificates.....	271
Create a certificate authority.....	272
Import an existing certificate authority.....	275
Manage imported and created certificate authorities.....	277
Export a certificate authority or private key.....	277
Display details about a certificate authority.....	278
Renew a certificate authority.....	279
Remove a certificate authority.....	280
Create a server certificate.....	281
Import an existing server certificate.....	284
Manage imported and created server certificates.....	285
Export a server certificate or private key.....	285

Display details about a server certificate.....	287
Renew a server certificate.....	288
Remove a server certificate.....	289

## **Chapter 10 Manage WireGuard VPN Tunnels**

About WireGuard VPN.....	292
About configuring WireGuard on the router.....	292
Enable and configure WireGuard VPN on the router.....	293
Configure client isolation and the MTU for a client-to-site WireGuard VPN connection.....	295
WireGuard VPN client accounts.....	296
Add a WireGuard VPN client account.....	297
Change a WireGuard VPN client account.....	299
Remove a WireGuard VPN client account.....	300
Export the router's WireGuard VPN client configuration file or QR code.....	302
Install the WireGuard utility or app and configuration file on a WireGuard client.....	303

## **Chapter 11 Manage the QoS Settings**

Use a speed test to automatically configure SQM for a WAN port.....	306
Manually configure SQM for a WAN port.....	307

## **Chapter 12 Install and Launch Third-Party Applications**

Overview of supported applications.....	310
Install and launch an application.....	310
Disable or enable an application.....	311
Uninstall an application.....	312

## **Chapter 13 Diagnostics and Troubleshooting**

Check the Internet speed.....	315
Ping the IP address or domain name of a device or network location.....	316
Look up a DNS domain name or IP address.....	317
Trace a route.....	318
Capture Ethernet packets.....	319
Sequence to restart the router network.....	321
Troubleshoot with the LEDs.....	322
Power LED remains off.....	322
Power LED does not turn green.....	323
Internet LED remains blinking amber or off.....	323
Cloud LED does not light blue if you use NETGEAR Insight.	324
A LAN LED is off while a device is connected.....	325

You cannot log in to the device UI of the router.....	325
Troubleshoot Internet browsing.....	326
Changes are not saved.....	326
Check the WAN port IP address.....	327
You enter the wrong password and can no longer log in to the router.....	328
Troubleshoot the network using your computer's ping utility...	329
Test the LAN path to your router.....	329
Test the path from your computer to a remote device.....	330

## **Appendix A Configure IPSec VPN Client Settings**

Windows-based computers.....	332
IKEv2 EAP - MSCHAPv2 VPN setup on a Windows-based computer.....	332
Transfer the CA certificate to a Windows-based computer for IKEv2 EAP - MSCHAPv2 VPN setup.....	332
Configure VPN settings on a Windows-based computer for IKEv2 EAP - MSCHAPv2 VPN setup.....	333
Mac computers.....	333
IKEv2 EAP - MSCHAPv2 VPN setup on a Mac computer.....	334
Transfer the CA certificate to a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup.....	334
Configure VPN settings on a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup.....	334
Set PSK on a MAC computer for IKEv2 EAP - MSCHAPv2 VPN setup.....	335
IKEv2 PSK VPN setup on a Mac computer.....	336
Configure VPN settings on a Mac computer for IKEv2 PSK VPN setup.....	336
Set PSK on a Mac computer for IKEv2 PSK VPN setup.....	336
IKEv1 PSK + XAuth VPN setup on a Mac computer.....	337
Configure VPN settings on a Mac computer for IKEv1 PSK + XAUTH VPN setup.....	337
Set PSK on a Mac computer for IKEv1 PSK + XAUTH VPN setup.....	337
iOS/iPad devices.....	338
IKEv2 EAP - MSCHAPv2 VPN setup on an iOS/iPad device...	338
Transfer the CA certificate to an iOS/iPad device for IKEv2 EAP - MSCHAPv2 VPN setup.....	339
Configure VPN settings on an iOS/iPad device for IKEv2 EAP - MSCHAPv2 VPN setup.....	339
IKEv2 PSK VPN setup on an iOS/iPad device.....	340
Configure VPN settings on an iOS/iPad device for IKEv2 PSK VPN setup.....	340

Set PSK on an iOS/iPad device for IKEv2 PSK setup.....	341
IKEv1 PSK + XAUTH VPN setup on an iOS/iPad device.....	341
Configure VPN settings on an iOS/iPad device for IKEv1 PSK + XAUTH VPN setup.....	341
Set PSK and enable XAUTH on an iOS/iPad device for IKEv1 PSK + XAUTH VPN setup.....	342
Android devices.....	343
IKEv2 EAP - MSCHAPv2 VPN setup on an Android device....	343
Transfer the CA Certificate to an Android device for IKEv2 EAP - MSCHAPv2 VPN setup.....	343
Configure VPN settings on an Android device for IKEv2 EAP - MSCHAPv2 VPN setup.....	344
IKEv2 PSK VPN setup on an Android device.....	345
Configure VPN settings on an Android device for IKEv2 PSK setup.....	345

## **Appendix B Supplemental information**

Factory default settings.....	347
Technical specifications.....	350

# 1

## Introduction

---

This manual is for the NETGEAR 10G/Multi-Gigabit Dual WAN Pro Router with Insight Cloud Management Model PR460X.

Model PR460X 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, IPSec client-to-site VPN, and VLAN capabilities with a DHCP server for each VLAN. Model PR460X is in this manual referred to as the router.

This manual describes the router's device user interface (UI).

If you onboard and manage the router through the NETGEAR Engage Controller application, 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 the Engage Controller are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to the Engage Controller.

Similarly, if you manage the router using the NETGEAR Insight Cloud Portal or NETGEAR Insight app, you can also use the device UI to manage the router. That is, these management methods are not mutually exclusive either 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:

- [Additional documentation](#)
- [How to manage the router](#)
- [About the device UI and the NETGEAR Engage Controller](#)
- [About the device UI and NETGEAR Insight](#)

**!** **NOTE:** For more information about the topics that are covered in this manual, visit the support website at [netgear.com/support/](https://netgear.com/support/).

❗ **NOTE:** Firmware updates with new features and bug fixes are made available from time to time at [netgear.com/support/download/](http://netgear.com/support/download/). 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/](https://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](https://kb.netgear.com/000065768).

Router management with the NETGEAR Engage Controller is described in the Engage Controller user manual, which is available at [netgear.com/support/download/](https://netgear.com/support/download/).

## How to manage the router

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

- **NETGEAR Engage Controller:** You can use the NETGEAR Engage Controller to discover and manage the router. The NETGEAR Engage Controller provides central management and configuration of switches and other supported devices through an audio-video (AV)-friendly, portable app for Windows and MacOS.

The Engage Controller can synchronize a limited number of features such as VLAN- and DHCP-related features with the router, and the other way around. You can use the router's device UI to configure many other features, such as WAN, security, and VPN features.

- **NETGEAR Insight:** 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.
  - **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.

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.

- **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. (You can also completely disable Insight in the device UI if you only want to use the device UI.)

At any time, you can either disable Insight in the device UI and let the Engage Controller onboard the router or keep Insight enabled and change to the hybrid management method with Insight.

**! NOTE:** The Engage Controller and Insight are mutually exclusive management methods.

## About the device UI and the NETGEAR Engage Controller

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

This manual does not describe NETGEAR Engage Controller procedures. These procedures are documented in the Engage Controller user manual, which you can download from the NETGEAR Download Center by visiting [netgear.com/support/download](http://netgear.com/support/download).

If you let the Engage Controller onboard the router as an Engage managed device, the controller can synchronize its VLAN profiles with the router up to the maximum number of supported VLANs on the router, and the other way around. (The router's VLAN are synchronized with the controller as VLAN data profiles.)

In addition, the Engage Controller can manage the router's DHCP server-related features, DHCP address reservations, and the optional mDNS gateway. You can use the router's device UI to configure and manage other router features, such as WAN, security, and VPN features. For more information, see [How the Engage Controller and the device UI interact with each other](#) on page 30.

# 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](https://netgear.com/business/services/insight/subscription) and [kb.netgear.com/000061848/](https://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/000065774](https://kb.netgear.com/000065774).

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 37.

# 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:

- [Set up the router with an Internet connection](#)
- [Decide on the router management method](#)
- [Engage Controller management](#)
- [Log in to the device UI](#)
- [Change the language of the device UI](#)
- [Change the color theme of the device UI](#)
- [Insight remote management](#)
- [Credentials for the device UI](#)

**!** **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/000065774](https://kb.netgear.com/000065774).

# 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 23.
  - **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 24.
- ❗ **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 26.

# 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:

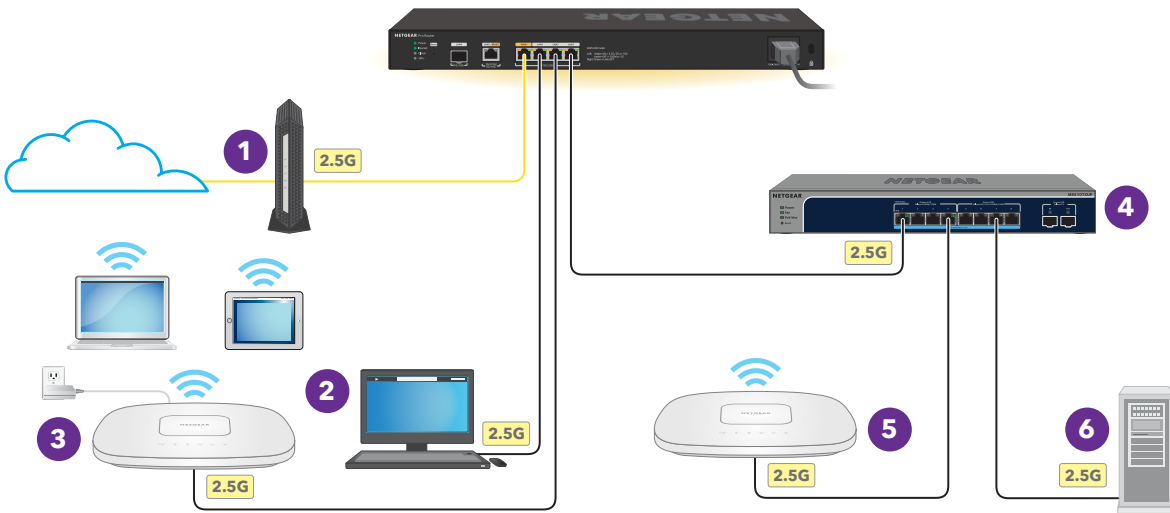


Figure 1. Example connections for a router setup with a connection to a modem

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 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](https://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](http://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](https://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 45.

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 that let you add the router to your network and configure, monitor, and control the router:

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

For information about how to discover and onboard the router using the NETGEAR Engage Controller, see [Use the NETGEAR Engage Controller to add a PR460X Pro Router to an Engage site](#) on page 31. You can also download the Engage Controller user manual from the NETGEAR Download Center by visiting [netgear.com/support/download](http://netgear.com/support/download).

- **Device UI:** 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, you can let the Engage Controller onboard the router and use the device for features that the Engage Controller cannot manage, or you can use Insight with the hybrid management method in which you use the Insight Cloud Portal or Insight app and the device UI.

Management through the Engage Controller and management through the device UI are not mutually exclusive but complement each other. For features that are supported on both the router and the Engage Controller, changes to the Engage Controller are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to the Engage Controller.

Similarly, for features that are supported on both the router and the Insight cloud-based management platform, management through Insight 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.

At any time, you can either disable Insight in the device UI and let the Engage Controller onboard the router or keep Insight enabled and change to the hybrid management method with Insight.

- **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 39.

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

- [netgear.com/business/services/insight/subscription/](https://netgear.com/business/services/insight/subscription/)
- [kb.netgear.com/000061848](https://kb.netgear.com/000061848)
- **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 40.

## Engage Controller management

The router does not need to be connected to the Internet for the Engage Controller to onboard the router, but the computer on which the Engage Controller is running must be in the same subnet as the router.

**❗ NOTE:** The Engage Controller and NETGEAR Insight are mutually exclusive management methods.

Under the following conditions, the Engage Controller can onboard the router:

- The router is in factory-default state.
- The router is installed and Insight is disabled in the device UI. (By default, Insight is enabled in the device UI.)

If Insight is enabled on the router, whether or not the router is connected to the Internet, the Engage Controller *cannot* onboard the router (onboarding is denied), and you must first disable Insight in the device UI (see [Change the Insight management mode](#) on page 41).

# How the Engage Controller and the device UI interact with each other

If you manage the router using the Engage Controller, 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 the Engage Controller are synchronized to the device UI, and the other way around, changes to the device UI are synchronized to the Engage Controller.

If you let the Engage Controller onboard the router as an Engage managed device, the controller and router can synchronize the following features:

- VLAN profiles up to the maximum number of supported VLANs on the router. The router's VLAN are synchronized with the controller as VLAN data profiles.
- DHCP server-related features
- DHCP address reservations
- mDNS gateway

You can use the device UI for other router features, such as WAN, security, and VPN features.

**ⓘ NOTE:** Synchronization between the device UI and Engage Controller might take several minutes. During the synchronization period, do not make the same changes on both the device UI and the Engage Controller or conflicting changes on the device UI and the Engage Controller.

The Engage Controller and the device UI interact with each other in the following ways, depending on the connected state:

- **Online:** The Engage Controller onboarded the router to an Engage site. You can use either the Engage Controller or the device UI to manage the router. The device UI and Engage Controller are synchronized with each other.

For information about how The Engage Controller affects the router admin password, see [Credentials for the device UI](#) on page 42.

- **Disconnected:** The Engage Controller onboarded the router to an Engage site but the router does not have a connection to the Engage Controller, for example, because the router is being rebooted or a network disruption occurred. After the router restarts or a network disruption is resolved, the state returns to Online. Otherwise, you can try to resync the connection (for more information, see the Engage Controller user manual).

❗ **NOTE:** If the router lost its connection to the Engage Controller, the router cannot synchronize with the Engage Controller. 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 the Engage Controller. 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 Engage Controller is restored.

- **Removed:** You removed the router as a managed device from the Engage Controller. The Engage Controller and the device UI no longer interact with each other.

## Use the NETGEAR Engage Controller to add a PR460X Pro Router to an Engage site

You can use the NETGEAR Engage Controller to discover and manage the switch. The Engage Controller provides central management and configuration of switches and other supported devices through an audio-video (AV)-friendly, portable app for Windows and MacOS. In this section we are referring to the Engage Controller as the *controller*.

❗ **NOTE:** This section refers to a setup where the controller is already installed. To download and install the controller, see the instructions in the Engage Controller user manual. You can download the manual from the NETGEAR Download Center by visiting [netgear.com/support/download](http://netgear.com/support/download).

You can add a single PR460X Pro Router only to an Engage site.

### To add a PR460X Pro Router to a site:

1. On your computer, in the folder in which you installed the controller, double-click the **Engage** application icon, or double-click the **Engage** shortcut.  
The controller opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.  
The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.  
The Edit Network Setup pop-up window displays.  
Do one of the following:
  - **Make no changes to the network setup for the site:** Click the **Apply** button.
  - **Change the network setup for the site:** Change the network setup and click the **Apply** button. For more information, see the Engage Controller user manual.

The Managed Devices page adjusts.

4. Click the **Onboard** button for the PR460X Pro Router.

The Add Device pop-up window displays.

5. To let the controller onboard the PR460X Pro Router so that it can take control of the Pro Router, specify one of the following options for the device password:

- **Custom device password:** If the PR460X Pro Router uses a custom device password, enter it.
- **Default device password:** To automatically enter the default device password, turn on the **Use device default password** toggle so that it displays blue or green and is positioned to the right.

To use this option, the PR460X Pro Router must be in factory default state.

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

6. Click the **Add** button.

The Select the LAN port for the Router pop-up window displays

7. From the **Connected LAN port** menu, select the PR460X Pro Router LAN port to which the controller is connected.
8. Click the **Apply** button.

Your settings are saved.

The Pro Router is moved to the Managed Devices table, and the onboarding process is now in progress.

❗ **NOTE:** At the end of this procedure, the controller pushes the site password to the PR460X Pro Router (which replaces the local device password or default password). If the firmware version on the PR460X Pro Router does not support the controller, the controller automatically updates the firmware, after which the PR460X Pro Router restarts. When these processes are complete, the PR460X Pro Router becomes a managed device and moves to the Online state. This process might take up to 1 minute.

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

## 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 23 or [Set up the router to connect to the LAN of an existing router](#) on page 24. 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/](http://kb.netgear.com/000062980/).

The login page displays.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

# Change the language of the device UI

By default, the language of the device UI is set to English. However, you can set the language to a specific one.

## To change the language of 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. At the top of the page, click the **Language** icon and select a language.

The language changes immediately.

# Change the color theme of the device UI

You can set the device UI to light theme, dark theme, or choose the device default option. The device default colour theme is light.

### To change the theme of 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. At the top of the page, click the **Color theme** icon and select a theme:
  - **Light theme**
  - **Dark theme**
  - **Device default**

The screen theme changes immediately and your settings are saved.

## 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:

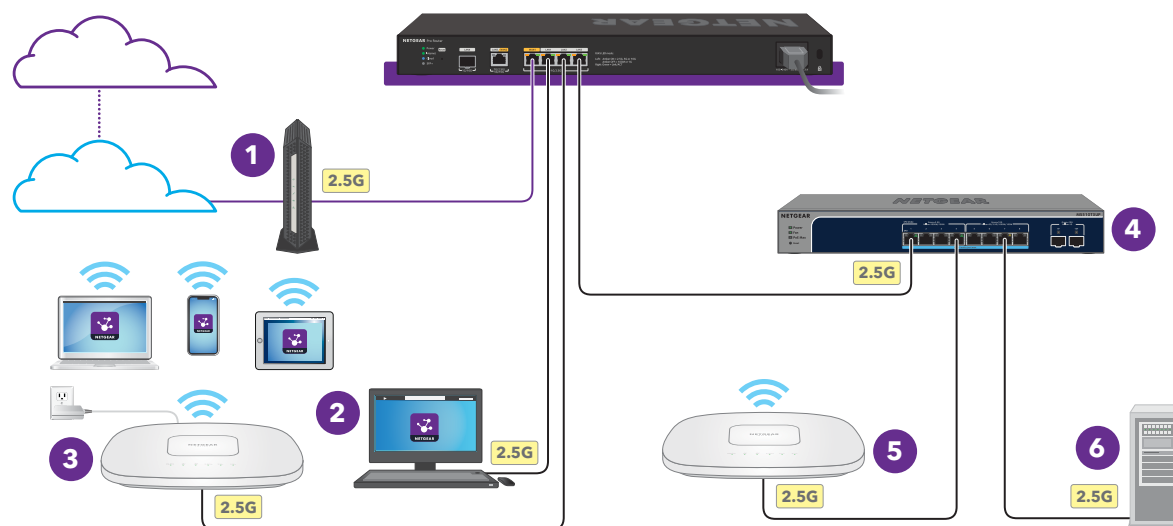


Figure 2. Example connections for a router setup with Insight remote management through the Cloud Portal or Insight app

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 can 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.

# 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](https://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.

## 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.

**! NOTE:** Synchronization between the device UI and Insight might take up to 15 minutes. During the synchronization period, do not make the same changes on both the device UI and Insight or conflicting changes on the device UI and 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 42.

- **Not Registered:** You did not add the router to an Insight network location. This 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 reenables 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 41.

# 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 40.

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](https://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](https://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](https://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 37.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

## 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 to a management application such as the NETGEAR Engage Controller application or NETGEAR Insight.

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

- **You onboard the router to the NETGEAR Engage Controller application: Use the Engage site password.**

If you add the router to an Engage Controller site, the Engage Controller *site password* replaces the router admin password for the device UI. To access the device UI, you must then enter the Engage Controller site password.

- **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.**

**! NOTE:** NETGEAR Insight and the Engage Controller and are mutually exclusive management methods.

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 189).

For information about how the Insight network password functions and for knowledge base articles about NETGEAR Insight, visit [kb.netgear.com/000065774](http://kb.netgear.com/000065774).

The following table lists the credential options for access to the device UI in relation to the Engage controller.

Table 1. Credentials for access to the device when the router is onboarded to an Engage Controller site

Onboarded to an Engage Controller site	Credentials	Main UI menu
No	Local device password	Full main UI menu
Yes	Engage Controller site password	Full main UI menu
First added to a site and then removed from both the site and the controller	Engage Controller site password until you set a new local device password	Full main UI menu

The following table lists the essential credential options for access to the device UI in relation to NETGEAR Insight.

Table 2. Credentials for access to the device UI when NETGEAR Insight manages the router

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 <sup>1</sup>	Insight network password

1. You disable the Insight mode after you already added the router to an Insight network location.

# 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 66.

This chapter contains the following sections:

- [Manually configure a dynamic Internet connection for the WAN1 port](#)
- [Manually configure a static Internet connection for the WAN1 port](#)
- [Manually configure a PPPoE Internet connection for the WAN1 port](#)
- [Manage secure DNS](#)
- [Dynamic DNS](#)

**!** **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/000065774](http://kb.netgear.com/000065774) 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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

The gateway is the ISP gateway to which your router connects.

10. To add an additional WAN1 IP address, click the **Additional WAN IP Addresses** toggle so that it displays blue and is positioned to the right.

The page adjusts. Depending on how you want to specify additional IP addresses, do one of the following:

- **Manually enter an additional IP address:**
  - a. Select the **Add IP Address** radio button.
  - b. Click the **Add** button.
  - c. In the **IP Address** field, enter an IP address.
- **Set an IP address range:**
  - a. Select the **Add IP Address Range** radio button.
  - b. Click the **Add** button.
  - c. Set the IP address range.

Your settings are saved.

To delete additional IP addresses, select the check box next to the IP address and click the **Delete** icon.

11. To add another IP address, repeat the previous step.
12. Select a radio button to specify how your domain name servers (DNS) are configured:
  - **Get Automatically 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.
13. If your ISP requires you to use a vendor class identifier (VCI) string, type it in the **Vendor Class Identifier String (Option 60)** field.

14. If your ISP requires you to use a client identifier (client ID) string, type it in the **Client Identifier String (Option 61)** field.

15. 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.

16. 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 your ISP gave you.

The gateway is the ISP gateway to which your router connects.

8. To add an additional WAN1 IP address, click the **Additional WAN IP Addresses** toggle so that it displays blue and is positioned to the right.

The page adjusts. Depending on how you want to specify additional IP addresses, do one of the following:

- **Manually enter an additional IP address:**

- a. Select the **Add IP Address** radio button.
- b. Click the **Add** button.
- c. In the **IP Address** field, enter an IP address.
- **Set an IP address range:**
  - a. Select the **Add IP Address Range** radio button.
  - b. Click the **Add** button.
  - c. Set the IP address range.

Your settings are saved.

To delete additional IP addresses, select the check box next to the IP address and click the **Delete** icon.

9. To add another IP address, repeat the previous step.
10. 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.

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 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.

12. 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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. In the Connection Mode section, select a radio button to select how the PPPoE connection is established:
- **Always On:** The PPPoE connection is always on. This is the default setting.
  - **Manually Connect:** Connecting manually means that the router does not have a PPPoE Internet connection unless you manually connect to the PPPoE ISP.
- With this selection, the Connect button displays on the page. After you complete the PPPoE configuration on the page and click the Apply button, click the **Connect** button to make a PPPoE connection.
- The Connection Status field displays Disconnected or Connected, according to the status of the PPPoE connection.
- After the router is connected over PPPoE, the name of the button changes to Disconnect so that you manually can terminate the PPPoE connection.

**ⓘ NOTE:** The PPPoE ISP assigns an IP address.

9. To add an additional WAN1 IP address, click the **Additional WAN IP Addresses** toggle so that it displays blue and is positioned to the right.
- The page adjusts. Depending on how you want to specify additional IP addresses, do one of the following:
- **Manually enter an additional IP address:**
    - a. Select the **Add IP Address** radio button.
    - b. Click the **Add** button.
    - c. In the **IP Address** field, enter an IP address.
  - **Set an IP address range:**
    - a. Select the **Add IP Address Range** radio button.
    - b. Click the **Add** button.
    - c. Set the IP address range.

Your settings are saved.

To delete additional IP addresses, select the check box next to the IP address and click the **Delete** icon.

10. To add another IP address, repeat the previous step.
11. Select a radio button to specify how your domain name servers (DNS) are configured:

- **Get Automatically 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.
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 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 1492 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.

## Manage secure DNS

Secure DNS connections increase security and user privacy by encrypting the data sent between DNS resolvers and other networking devices. To set up a secure DNS on your router, see [Enable a secure DNS](#) on page 55. For more information about secure DNS types, see [About secure DNS](#) on page 54.

The secure DNS connections have an optional built-in fallback to plain DNS state. If a secure DNS connection to a server is blocked, some browsers default to non-encrypted communication. For more information about this option, see [Enable fallback to plain DNS](#) on page 60.

## About secure DNS

You can set up a secure DNS on the router using either DNS over Transport Layer Security (DoT), DNS over HTTPS (DoH), or DNS over Quick UDP Internet Connections (DoQ).

### DoT: DNS over Transport Layer Security (TLS)

DoT is secure and simple, but identifiable as DNS traffic.

- **Protocol:** Uses TLS (Transport Layer Security) to encrypt DNS queries and responses.
- **Port:** Typically operates on port 853.
- **Advantages:**
  - Security: Provides strong encryption and authentication, ensuring that DNS queries are protected from eavesdropping and tampering.
  - Simplicity: Easier to implement in environments where TLS is already used for other services.
- **Disadvantages:**
  - Visibility: DNS traffic can be identified as DNS due to the use of a dedicated port (853).
  - Performance: May introduce latency due to the overhead of establishing and maintaining TLS connections.

### DoH: DNS over HTTPS

DoH is secure and private, integrated with web traffic, but more complex than DoT.

- **Protocol:** Uses HTTPS (HTTP over TLS) to encrypt DNS queries and responses.
- **Port:** Operates on port 443, the same port used for regular HTTPS traffic.
- **Advantages:**
  - Privacy: DNS queries are indistinguishable from regular HTTPS traffic, making it harder for third parties to identify and block DNS traffic.
  - Integration: Can be easily integrated into existing web infrastructure and benefits from the widespread adoption of HTTPS.
- **Disadvantages:**
  - Complexity: More complex to implement and manage compared to DoT.
  - Performance: Might have higher latency due to the overhead of HTTP and TLS.

## DoQ: DNS over Quick UDP Internet Connections (QUIC)

DoQ is secure, high performance, and resilient, but less widely adopted than DoT and DoH.

- **Protocol:** Uses QUIC (Quick UDP Internet Connections) to encrypt DNS queries and responses.
- **Port:** Typically operates on port 784.
- **Advantages:**
  - Performance: QUIC is designed to reduce latency and improve performance, especially in environments with high packet loss or variable network conditions.
  - Security: Provides strong encryption and authentication similar to TLS.
  - Resilience: Better handling of network changes and interruptions compared to TCP-based protocols.
- **Disadvantages:**
  - Adoption: QUIC is relatively new and less widely adopted compared to TLS and HTTPS.
  - Complexity: Requires support for QUIC, which might not be available in all environments.

## Enable a secure DNS

You can set up a secure DNS connection on the router by enabling the secure DNS setting, and then adding a new secure DNS connection. For more information, see [Add a new secure DNS](#) on page 56.

When you set up a secure DNS, you can also enable the fallback to plain DNS setting. For more information, see [Enable fallback to plain DNS](#) on page 60.

The device UI uses the following icons:



### To enable a secure DNS:

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 32.
3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Advanced Settings**.

The Advanced Settings page displays.

5. Click the **Secure DNS** toggle to enable or disable the secure DNS setting:
  - **The toggle is blue and positioned to the right:** Secure DNS is enabled.
  - **The toggle is gray and positioned to the left:** Secure DNS is disabled.

By default, the **Secure DNS** toggle is disabled

When you enable the secure DNS setting, the Fallback to Plain DNS toggle and the DNS list display.

6. Click the **Apply** button.

Your settings are saved.

## Add a new secure DNS

To add a new secure DNS, you must first enable the secure DNS feature. For more information about setting up a secure DNS, see [Enable a secure DNS](#) on page 55.

The router lets you select from multiple DNS service providers, but you need to set up an account with one or more of these DNS providers.

**NOTE:** You can add a maximum of three secure DNS configurations to the router.

The device UI uses the following icons:

 Add  Edit  Delete

### To add a new secure DNS:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Advanced Settings**.

The Advanced Settings page displays.

5. Click the **Add** icon.

6. From the **Type** menu, select the type of secure DNS you want to add:

- **DoH**
- **DoT**
- **DoQ**

The default selection is DoH.

7. From the **DNS Service Provider** menu, select the DNS service provider for the secure DNS.

You must set up an account with a DNS service provider.

8. Click the **Apply** button.

Your settings are saved.

# Edit a secure DNS

You can edit a secure DNS using the device UI. To edit a secure DNS, you must first enable the secure DNS feature. For more information about setting up a secure DNS, see [Enable a secure DNS](#) on page 55.

The device UI uses the following icons:

 Add  Edit  Delete

## To edit a secure DNS:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Advanced Settings**.

The Advanced Settings page displays.

5. Select the DNS you want to edit.
6. From the **Type** menu, select the type of secure DNS:
  - **DoH**
  - **DoT**
  - **DoQ**

- From the **DNS Service Provider** menu, select the DNS service provider for the secure DNS.

You must set up an account with a DNS service provider.

- Click the **Edit** icon.
- Click the **Apply** button.

Your settings are saved.

## Remove a secure DNS

You can remove a secure DNS using the device UI. To remove a secure DNS, you must first enable the secure DNS feature. For more information about setting up a secure DNS, see [Enable a secure DNS](#) on page 55.

The device UI uses the following icons:



### To remove a new secure DNS:

- Launch a web browser from a computer or mobile device that is connected to the router network.
- 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 32.

- Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

- Select **WAN > Internet/WAN > Advanced Settings**.

The Advanced Settings page displays.

5. Select the DNS you want to delete.
6. Click the **Delete** icon.
7. Click the **Apply** button.

Your settings are saved.

## Enable fallback to plain DNS

You can enable fallback to plain DNS so that if the secure DNS fails, it reverts to an unencrypted, or plaintext, DNS.

You must enable the secure DNS setting before you can enable fallback to plain DNS. For more information, see [Enable a secure DNS](#) on page 55.

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Advanced Settings**.

The Advanced Settings page displays.

5. Click the **Fallback to Plain DNS** toggle to enable or disable fallback to plain DNS:
  - **The toggle is blue and positioned to the right:** Fallback to plain DNS is enabled.
  - **The toggle is gray and positioned to the left:** Fallback to plain DNS is disabled.

By default, the Fallback to Plain DNS toggle is disabled.

6. Click the **Apply** button.

Your settings are saved.

## Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows a device with a varying WAN (public) IPv4 address to be located using a fully qualified domain name (FQDN), also referred to as an Internet domain name.

If your network has a static (fixed) IP address, you can register a FQDN to be linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned WAN IP address, you do not know in advance what the router's IP address will be, and the address can change frequently.

A dynamic DNS (DDNS) service provider lets you register a FQDN, allows the router to be located on the Internet through its FQDN, and relates the DNS requests for the FQDN to the router's frequently changing IP address. The router notifies the DDNS server provider of changes in the WAN IP address so that services that are running on the router's network can continue to be accessed by others on the Internet.

The router lets you select from multiple DDNS service providers, but you need to set up an account with one or more of these DDNS providers.

**NOTE:** If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the DDNS service does not work because private addresses are not routed on the Internet.

If you use WAN failover with VPN you must use a FQDN, regardless of the type of Internet IP address (fixed, dynamic, or PPPoE). For more information about WAN failover, see [Set Up and Configure a Dual WAN Connection](#) on page 66.

## Add a dynamic DNS profile

You can add one or more dynamic DNS profiles that define the domain names under which the router can be reached over the Internet.

The device UI uses the following icons:

 Add  Edit  Delete

### To add a dynamic DNS 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Dynamic DNS**.

The Dynamic DNS page displays.

5. Click the **Add** button.

The Add/Edit Dynamic DNS pop-up window displays.

6. Configure following settings:
  - a. In the **Profile Name** field, type a name for the profile.

The name is for identification purposes.
  - b. **Enable**: To immediately enable the profile after you click the Apply button, keep the **Enable** toggle for the profile blue and positioned to the right, which is the default setting. If you do not want the profile to be enabled after you click the Apply button, click the **Enable** toggle for the profile so that the toggle is gray and positioned to the left.
  - c. From the **Service Provider** menu, select a predefined service provider.
  - d. In the **Domain Name** field, type one of the following, depending on the service provider that you selected:

- Fully qualified domain name, such as myhost.dyndns.org
  - Domain name, such as mydomain.com
  - Host name and domain name, separated by the @ symbol. For example, type myhostname@mydomain.com.
- e. In the **Username** field, type the user name that is associated with the DDNS account and that lets you log in to the DDNS service.
  - f. Depending on the service provider that you selected, do one of the following:
    - **Password:** In the **Password** field, type the password that is associated with the DDNS account and that lets you log in to the DDNS service.
    - **API Token:** In the **API Token** field, type the global API key or API token.
  - g. Use the **Time** field and the **min** menu to set the interval for the router to check the external IP address.
7. Click the **Add** button.

Your settings are saved. The new DDNS profile is added to the Dynamic DNS table.

In the table, the Last Check Time field displays when the router checked the external IP address.

In the table, the External IP Address field displays the public IP address that is assigned to the router or to the gateway behind which the router is located (that is, the router is behind NAT).

## Change, enable, or disable a dynamic DNS profile

You can change, enable, or disable a dynamic DNS profile.

The device UI uses the following icons:

 Add  Edit  Delete

### To change, enable, or disable a dynamic DNS 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Dynamic DNS**.

The Dynamic DNS page displays.

5. Select the check box for the profile.

6. Click the **Edit** button.

The Add/Edit Dynamic DNS pop-up window displays.

7. Change the settings for the dynamic DNS profile.

For more information about the settings, see [Add a dynamic DNS profile](#) on page 61.

8. Click the **Enable** toggle to enable or disable the dynamic DNS profile:

- **The toggle is blue and positioned to the right:** The dynamic DNS profile is enabled.
- **The toggle is gray and positioned to the left:** The dynamic DNS profile is disabled.

9. Click the **Update** button.

Your settings are saved. The modified dynamic DNS profile display in the Dynamic DNS table.

In the table, the Last Check Time field displays when the router checked the external IP address.

In the table, the External IP Address field displays the public IP address that is assigned to the router.

## Remove a dynamic DNS profile

If you no longer need a dynamic DNS profile, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

**To remove a dynamic DNS 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Dynamic DNS**.

The Dynamic DNS page displays.

5. Select the check box for the profile.
6. Click the **Delete** icon.

A pop-up window displays.

7. Click the **OK** button.

Your settings are saved. The rule is removed from the table.

# 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:

- [About Dual WAN and WAN failover](#)
- [Configure dual WAN with a dynamic Internet connection for the WAN2 port](#)
- [Configure dual WAN with a static Internet connection for the WAN2 port](#)
- [Configure dual WAN with a PPPoE Internet connection for the WAN2 port](#)
- [Configure dual WAN failover detection](#)
- [Configure dual WAN load balancing](#)
- [Display the status of the dual-WAN interfaces](#)

**!** **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/000065774](http://kb.netgear.com/000065774) 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. At any time, traffic is going through *one* WAN port only.

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 68](#)
  - **Static connection:** [Configure dual WAN with a static Internet connection for the WAN2 port on page 71](#)
  - **PPPoE connection:** [Configure dual WAN with a PPPoE Internet connection for the WAN2 port on page 74](#)
3. Configure dual WAN failover and the type of failover detection (see [Configure dual WAN failover detection on page 78](#)).

## 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 32.

7. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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. To add an additional WAN2 IP address, click the **Additional WAN IP Addresses** toggle so that it displays blue and is positioned to the right.

The page adjusts. Depending on how you want to specify additional IP addresses, do one of the following:

- **Manually enter an additional IP address:**
  - a. Select the **Add IP Address** radio button.
  - b. Click the **Add** button.
  - c. In the **IP Address** field, enter an IP address.
- **Set an IP address range:**
  - a. Select the **Add IP Address Range** radio button.
  - b. Click the **Add** button.
  - c. Set the IP address range.

Your settings are saved.

To delete additional IP addresses, select the check box next to the IP address and click the **Delete** icon.

15. To add another IP address, repeat the previous step.
16. 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.
17. If your ISP requires you to use a vendor class identifier (VCI) string, type it in the **Vendor Class Identifier String (Option 60)** field.
18. If your ISP requires you to use a client identifier (client ID) string, type it in the **Client Identifier String (Option 61)** field.
19. 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.

20. Click the **Apply** button.

Your settings are saved.

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

21. To display the status of the dual WAN configuration, see [Display the status of the dual-WAN interfaces](#) on page 83.

## 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 32.
7. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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. To add an additional WAN2 IP address, click the **Additional WAN IP Addresses** toggle so that it displays blue and is positioned to the right.

The page adjusts. Depending on how you want to specify additional IP addresses, do one of the following:

- **Manually enter an additional IP address:**
  - a. Select the **Add IP Address** radio button.
  - b. Click the **Add** button.
  - c. In the **IP Address** field, enter an IP address.
- **Set an IP address range:**
  - a. Select the **Add IP Address Range** radio button.
  - b. Click the **Add** button.
  - c. Set the IP address range.

Your settings are saved.

To delete additional IP addresses, select the check box next to the IP address and click the **Delete** icon.

14. To add another IP address, repeat the previous step.
15. 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.

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 83.

## 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 32.
7. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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. In the Connection Mode section, select a radio button to select how the PPPoE connection is established:

- **Always On:** The PPPoE connection is always on. This is the default setting.
- **Manually Connect:** Connecting manually means that the router does not have a PPPoE Internet connection unless you manually connect to the PPPoE ISP.

With this selection, the Connect button displays on the page. After you complete the PPPoE configuration on the page and click the Apply button, click the **Connect** button to make a PPPoE connection.

The Connection Status field displays Disconnected or Connected, according to the status of the PPPoE connection.

After the router is connected over PPPoE, the name of the button changes to Disconnect so that you manually can terminate the PPPoE connection.

**ⓘ NOTE:** The PPPoE ISP assigns an IP address.

14. To add an additional WAN2 IP address, click the **Additional WAN IP Addresses** toggle so that it displays blue and is positioned to the right.

The page adjusts. Depending on how you want to specify additional IP addresses, do one of the following:

- **Manually enter an additional IP address:**
  - a. Select the **Add IP Address** radio button.
  - b. Click the **Add** button.
  - c. In the **IP Address** field, enter an IP address.
- **Set an IP address range:**
  - a. Select the **Add IP Address Range** radio button.
  - b. Click the **Add** button.
  - c. Set the IP address range.

Your settings are saved.

To delete additional IP addresses, select the check box next to the IP address and click the **Delete** icon.

15. To add another IP address, repeat the previous step.

16. Select a radio button to specify how your domain name servers (DNS) are configured:

- **Get Automatically 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.

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 1492 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 83.

## 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.

**!** **NOTE:** A dual WAN traffic rule takes priority over a WAN failover. Therefore, after a WAN failover, traffic that is subject to a traffic rule for a specific WAN interface might stop if that WAN interface is down. That is, the traffic might not failover to the other WAN interface. For more information, see [Dual WAN traffic rule](#) on page 127.

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 five 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 send 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

6. From the **Policy** menu, select **Failover**.

7. 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.

8. 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.
9. 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.
10. 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 3600 seconds.
11. 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.
12. Click the **Apply** button.  
Your settings are saved.
13. To display the status of the dual WAN configuration, see [Display the status of the dual-WAN interfaces](#) on page 83.

# Configure dual WAN load balancing

Load balancing facilitates the router to distribute network traffic across the dual WAN connection based on predefined weights. The weights represent the capacity of each device on the WAN connection, indicating how much load or traffic the connection can handle. You can adjust the weight settings of the dual WAN connection and set different weight distributions for the primary WAN and secondary WAN. By default, both WAN1 and WAN2 carry 50 percent of the weight distribution.

**! NOTE:** The system separates Internet sessions based on the load between the primary WAN and secondary WAN, instead of the overall bandwidth or data rate.

**! NOTE:** A dual WAN traffic rule takes priority over load balancing. For more information, see [Dual WAN traffic rule](#) on page 127.

The router supports the following types of load balancing failover detection methods:

- **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.

## To configure load balancing:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

6. From the **Policy** menu, select **Load Balancing**.

7. In the **Weight Settings** section, use the **WAN1** menu to select the weight setting for WAN1.

The selection from the **WAN2** menu is automatically adjusted because there are only two WAN interfaces.

8. 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.

9. 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.
10. 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 3600 seconds.
11. 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.
12. Click the **Apply** button.  
Your settings are saved.
13. To display the status of the dual WAN configuration, see [Display the status of the dual-WAN interfaces](#) on page 83.

## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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](#)
- [ManageEEE, flow control, and link speed for ports](#)
- [MAC address to IP address bindings](#)
- [Static routes](#)
- [Enable the mDNS Gateway](#)
- [Link aggregation](#)

**!** **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/000065774](http://kb.netgear.com/000065774) 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 87).

**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 32 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 than RIP-1, sends the routing data in RIP-2 format, and uses subnet broadcasting.
  - **RIP-2M:** This format carries more information than 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. As an option, you can turn on the **Sequential IP Address** toggle so that the DHCP server allocates sequential IP addresses.
- **The toggle is blue and positioned to the right:** The DHCP server assigns a sequential IP address to the devices on this VLAN.
  - **The toggle is gray and positioned to the left:** The DHCP server does not assign a sequential IP address to the devices on this VLAN. This is the default setting.
- ❗ **NOTE:** By default, the DHCP sever assigns an IP address based on hash of client's MAC address. This allows the IP address to remain stable even if the DHCP lease expires. If you choose the sequential IP address mode, the IP address might move when the DHCP lease expires.
13. 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.
14. As an option, add one or more NTP servers by doing the following:
- a. Click the **NTP Server (Option 42)** toggle so that the toggle is blue and positioned to the right, which enables NTP server option 42.  
By default, the toggle is gray and positioned to the left.
  - b. In the **NTP Server 1**, **NTP Server 2**, and **NTP Server 3** fields, type IP addresses for NTP servers.  
You can specify one, two, or three NTP servers, which communicate the time through DHCP option 42 to the VLAN members.
- The NTP server or servers are communicated through DHCP option 42.

15. As an option, in the **Domain Name** field, type the fully qualified domain name (FQDN) for the domain that the VLAN members join.

This domain name is communicated through DHCP option 15.

16. 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 89), 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 89.

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.

Note the following:

- You cannot remove the default VLAN profile with ID 1.
- Before you remove a VLAN profile, first remove or modify the settings that are associated with the VLAN profile. For example, change any VPN settings, traffic rules, and IP address reservation settings that are associated with the VLAN profile that you want to remove.

**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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 confirmation 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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.

- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

**! NOTE:** For the LAN4 port, which is an SFP+ port, auto-negotiation is not only determined by the speed that the connected device supports but also by the direct attach cable (DAC) or transceiver module that you insert into the port. For example, if you connect a switch that does support 10 Gbps but you use a DAC that supports only 1 Gbps, the link speed is set at 1 Gbps. To allow for 10 Gbps speed, both the DAC or transceiver module and the connected device must be capable of supporting 10 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. This can be important for network servers and common network resources.

## Add a MAC-IP binding for a detected device

The 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 100).

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

Although the IP address for the MAC-IP binding (that is, the reserved IP address) does not need to be within the defined DHCP range, we recommend the following:

- **Static DHCP client:** For a DHCP client that must receive a static IP address, reserve an IP address outside the defined DHCP range.
- **Dynamic DHCP client:** For a DHCP client that must receive a dynamic IP address, reserve an IP address in the defined DHCP range.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

Depending on the browser that you are using, a pop-up window might display.

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:

- A Pro AV switch has an IP address 192.168.1.100.
- The Pro AV switch is both the gateway and the DHCP server for all audio video (AV) devices in the 192.168.100.0/24 IP subnet.
- Your management laptop has an IP address in the 192.168.1.0/24 subnet but needs to be able to manage the AV devices in the 192.168.100.0/24 IP subnet.

You must set up a static route so that the management laptop in one IP subnet can reach the AV devices in the other IP subnet:

1. For the network in the static route, specify the IP address for the final destination of the route, which is the 192.168.100.0 IP subnet (in combination with the subnet mask).
2. For the subnet mask in the static route, specify 255.255.255.0 (which is the same as /24).
3. For the gateway in the static route, specify 192.168.1.100, which is the IP address of the Pro AV switch.

This static route allows traffic from the management laptop to the AV devices to be routed to the Pro AV switch, from where it can reach the AV devices on the 192.168.100.0/24 IP subnet.

## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.
3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 107.
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:



### 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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

## Enable the mDNS Gateway

A multicast DNS (mDNS) gateway allows devices and services to be shared across different VLANs and WiFi networks.

Shared devices include printers, scanners, storage devices, and other hardware devices. Services include multiple telephone, music, and video streaming services, file sharing services, and other services and applications. For example, if a group of clients are on VLAN 20 and a printer is on VLAN 1, an mDNS gateway can make the printer discoverable to the clients. (For a client to be able to access the printer, inter-VLAN routing must be enabled on VLANs 1 and 20, or you must set up a traffic rule that enables the clients to access the printer.) Or, if a meeting participant wants to use a phone connected to VLAN 20 to cast a presentation to a large-screen device connected to VLAN 30, an mDNS gateway policy can make this possible.

If a WiFi access point is connected to the router, a service can run either on a wired or WiFi device, but for a WiFi client to be able to access the service, the WiFi client must be connected to a WiFi network on an AP that has the mDNS gateway feature enabled. In a network with multiple devices that support the mDNS gateway feature, you can set one device, such as the router, as the mDNS reflector, which re-advertises shared devices and services throughout the network.

On the router, you cannot configure mDNS policies, but the router can function as an mDNS reflector. Enabling the mDNS gateway on the router means enabling the router as the mDNS reflector.

### To enable the mDNS Gateway:

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 32.
3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **LAN > mDNS Gateway**.

The mDNS Gateway page displays.

5. Enable the mDNS gateway by clicking the **Enable mDNS Gateway** toggle so that so the toggle is blue and positioned to the right.

By default, the mDNS gateway is disabled and the **Enable mDNS Gateway** toggle is gray and positioned to the left.

6. Click the **Apply** button.

Your settings are saved.

After a while, services and shared devices that the router discovers in the network display in the Discovered Devices table on the page:

- **Service:** The type service (for example, Googlecast) or shared device (for example, printer)
- **Port:** The port at which the service or shared device can be reached
- **Host Name:** The name of the host on which the service is installed or the name of the shared device (for example, printer)
- **IP Address:** The IP address of the host on which the service is installed or the IP address of the shared device (for example, printer)
- **VLAN:** The VLAN ID that includes as members the service or shared device. This VLAN is also referred to as the service VLAN.

7. To refresh the page, click the **Refresh** button.


# Link aggregation

Link aggregation allows you to combine multiple Ethernet links into a single logical link. Network devices treat the link aggregation group (LAG) as a single link, which increases throughput, fault tolerance, or both, between devices.


The router supports both static LAGs and Link Aggregation Control Protocol (LACP) for dynamic LAGs.

For a LAG to function you must:

- Make sure that all ports that participate in the LAG (the ports on both devices) use the same speed, duplex mode, and flow control setting. See [Manage IEEE, flow control, and link speed for ports](#) on page 97 for information about changing these settings on the router.
- Set up a physical link aggregation connection (see [Make a link aggregation connection](#) on page 117).
- Select the ports on the router that must participate in the LAG, as described in this task.
- Enable the LAG on the router and on the connected network device.

 **CAUTION:** Configure a LAG properly on router and switch before connecting Ethernet cables to avoid creating a network loop before and after the LAG setting changes:

- If two ports are linked before LAG configuration, then a loop may form between these two ports.
- If Ethernet cables are not unlinked before disabling a LAG, then a loop may form between these two ports.

 **NOTE:** In a properly implemented network, auto-LAG and auto-trunk features need an established link before LAG or Trunk become active automatically.

In such environments, there is no restriction when links are established and how a LAG is configured.

## Enable link aggregation

To make link aggregation connections between the router and another network device, see [Make a link aggregation connection](#) on page 117.

**To enable link aggregation:**

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **LAN > Link Aggregation**.

The Link Aggregation page displays.

5. Enable link aggregation by clicking the **Enable Link Aggregation** toggle:

- **The toggle is blue and positioned to the right:** Link aggregation is enabled.
- **The toggle is gray and positioned to the left:** Link aggregation is disabled. This is the default setting.

6. Select the LAG type from the menu.

- **Static LAG**

For more information, see: [Set up a static link aggregation group](#) on page 115.

- **Dynamic LAG**

For more information, see: [Set up a dynamic link aggregation group](#) on page 116.

7. Click the **Apply** button.

Your settings are saved.

## Set up a static link aggregation group

Set up a static link aggregation group (LAG) to combine multiple Ethernet links into a single logical link between two networked devices.

### To set up a dynamic LAG on 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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **LAN > Link Aggregation**.  
The Link Aggregation page displays.
5. Enable link aggregation by clicking the **Enable Link Aggregation** toggle:
  - **The toggle is blue and positioned to the right:** Link aggregation is enabled.
  - **The toggle is gray and positioned to the left:** Link aggregation is disabled. This is the default setting.
6. From the **LAG Type** menu, select **Static**.
7. From the **HASH Policy** menu, choose from one of the following options:
  - **Layer 2: Source + Destination**
  - **Layer 2+3: Source + Destination**
  - **Layer 3+4: Source + Destination**

8. To add ports to the LAG, click on the port image for LAN 1, LAN2, or LAN3 to select the port.

When a LAG is present, a green checkmark displays on the icon for the port.

A LAG must consist of at least two ports.

9. Click the **Apply** button.

Your settings are saved.

## Set up a dynamic link aggregation group

Set up a dynamic link aggregation group (LAG) to combine multiple Ethernet links into a single logical link between two networked devices. Dynamic LAGs use Link Aggregation Control Protocol (LACP), which helps to prevent errors in the LAG setup.

### **To set up a dynamic LAG on 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **LAN > Link Aggregation**.

The Link Aggregation page displays.

5. Enable link aggregation by clicking the **Enable Link Aggregation** toggle:

- **The toggle is blue and positioned to the right:** Link aggregation is enabled.
  - **The toggle is gray and positioned to the left:** Link aggregation is disabled.  
This is the default setting.
6. From the **LAG Type** menu, select **Dynamic/LACP**.
  7. In the **LACP System Priority** field, enter a number from 1 to 65535.  
The default number is 65535.
  8. From the **LACP Interval** menu, choose either a slow or fast LACP interval speed.  
The default selection is slow.
  9. From the **HASH Policy** menu, choose from one of the following options:
    - **Layer 2: Source + Destination**
    - **Layer 2+3: Source + Destination**
    - **Layer 3+4: Source + Destination**
  10. To add ports to the LAG, click on the port image for LAN 1, LAN2, or LAN3 to select the port.  
When a LAG is present, a green checkmark displays on the icon for the port.  
A LAG must consist of at least two ports.
  11. Click the **Apply** button.  
Your settings are saved.

## Make a link aggregation connection

Before you make a physical link aggregation connection to another network device (usually a switch or WiFi access point) that also supports link aggregation, you must first set up a LAG on the router. If you do not, the LAG cannot take effect. Whether a LAG on the router functions to support increased bandwidth or fault tolerance depends on the LAG configuration on the other network device.

All ports that participate in a LAG (that is, the ports on both devices) must use the same speed, full duplex mode, and flow control setting. For information about changing these settings on the router, see [Manage EEE, flow control, and link speed for ports](#) on page 97.

### To make link aggregation connections between the router and another network device:

Using Ethernet cables, connect each port that must be a member of the LAG on the router to each port that must be a member of the same LAG on another network device.

- The ports on the other network device are members of the same LAG.
- The LAG consists of the same total number of ports.
- The ports use the same speed, full duplex mode, and flow control setting as the ports in the LAG on the router.

# 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:

- [Manage protection for port scans, denial of service, and pings](#)
- [Set up a DMZ server](#)
- [Manage the SIP application-level gateway](#)
- [Manage timeouts for TCP, UDP, and ICMP sessions](#)
- [Manage VPN pass-through for tunnel protocols](#)
- [Firewall traffic rules](#)
- [Dual WAN traffic rule](#)
- [General outbound traffic rule](#)
- [Outbound NAT rule](#)
- [Port forwarding](#)
- [Port triggering](#)
- [Enable or disable UPnP](#)
- [Services, protocols, and port numbers](#)
- [Schedules](#)

**!** **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/000065774](http://kb.netgear.com/000065774) 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 142) or port triggering rule (see [Port triggering](#) on page 148). 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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:** 250,000

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

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Firewall > Basic Settings**.

The Basic Settings page displays.

5. 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 250000.

The Current Connections field show the total number of current TCP, UDP, and ICMP sessions (connections).

6. 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

The router supports the following types of traffic rules:

Table 3. Traffic rules

Traffic rule	Description
Dual WAN traffic rule	The Dual WAN traffic rule allows you to configure the WAN interface through which traffic leaves the router. For more information, see <a href="#">Dual WAN traffic rule</a> on page 127.
General outbound traffic rule	The general outbound traffic rule allows you to configure, permit, or block certain outbound traffic. For more information, see <a href="#">General outbound traffic rule</a> on page 132.

Table 3. Traffic rules (Continued)

Traffic rule	Description
Outbound NAT rule	The outbound NAT rule controls how the router translates the source IP address of traffic that leaves a WAN port. For more information, see <a href="#">Outbound NAT rule</a> on page 138.
Port forwarding	Port forwarding allows certain types of incoming traffic to reach the server in a business network. For more information, see <a href="#">Port forwarding</a> on page 142.
Port triggering	Port triggering is a dynamic extension of port forwarding. Unlike port forwarding, which is always active after it is configured, port triggering works by creating a port forwarding rule (inbound firewall rule) that is only activated when it is triggered by detecting specified outbound packets. After the rule is triggered, specified inbound packets (from the Internet) are forwarded to the computer that triggered it. For more information, see <a href="#">Port triggering</a> on page 148.

## Dual WAN traffic rule

The dual WAN traffic rule allows you to configure the WAN interface through which traffic leaves the router.

A dual WAN traffic rule takes priority over a WAN failover. As an example, assume that you set up two Dual WAN traffic rules:


- Rule 1: Traffic of VLAN 1 is sent to the WAN1 interface.
- Rule 2: Traffic of VLAN 2 is sent to the WAN2 interface.

Traffic of VLAN 3 is not subject to a dual WAN traffic rule. If the WAN1 interface goes down and traffic fails over to the WAN2 interface, traffic from VLAN2 and VLAN3 remains flowing, but traffic from VLAN 1 stops because rule 1 requires traffic to pass through the WAN 1 interface.

A dual WAN traffic rule on the router defines the following components:

- **Name:** The name of the dual WAN rule.
- **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 155.
- **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 address:** The destination address is the IP address to which the traffic is sent. The rule can apply to all destination addresses, to a single IP address, or a subnet of IP addresses.
- **WAN Interface:** The WAN interface to which the rule applies.

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

## Add a dual WAN traffic rule

You can add dual WAN traffic rules 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 dual WAN 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Dual WAN > Rules**.

The 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 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. From the **Service** 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 155.

- d. 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.

- e. 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.

- f. 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.

7. From the **WAN Interface** menu, select a WAN interface:

- **WAN1 Only**
- **WAN2 Only**

8. Click the **Apply** button.

The new dual WAN rule is added to the table on the Rules page. If you enabled the new dual WAN rule (that is, the **Enable Rule Status** toggle is blue and positioned to the right), it goes into effect immediately. The dual WAN traffic rule is assigned the lowest priority in relation to existing 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 rule reaches the desired position.

The number in the Priority column show the priority in relation to the other rules in the table.

- b. Click the **Apply** button.

Your settings are saved.

## Change a dual WAN traffic rule or its priority, or enable or disable the rule

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

The device UI uses the following icons:



### To change a dual WAN 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Dual WAN > Rules**.

The 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 Rule pop-up window displays.

- c. Change the settings for the rule, or enable or disable the rule:

For more information about the settings, see [Add a dual WAN traffic rule](#) on page 128.

- 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 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 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.

## Remove a dual WAN traffic rule

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

The device UI uses the following icons:



### To remove a dual WAN 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **WAN > Internet/WAN > Dual WAN > Rules**.

The Rules page displays.

5. In the table, select the check box for the rule.

6. Click the **Delete** icon.

A pop-up window displays.

7. Click the **OK** button.

Your settings are saved. The rule is removed from the table.

## General outbound traffic rule

You can use a general outbound traffic rule to configure, allow, or block certain outbound traffic, regardless of the WAN interface through which the traffic leaves the router.

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 155.
- **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 160.

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

## Add a general outbound traffic rule

You can add a general outbound 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 general outbound 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 155.

- 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 160.
  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 general outbound traffic rule or its priority, or enable or disable the rule

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

The device UI uses the following icons:

 Add  Edit  Delete

### To change a general outbound 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 general outbound traffic rule](#) on page 133.

- 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 to the other traffic rules in the table.

- b. Click the **Apply** button.

Your settings are saved.

## Remove a general outbound traffic rule

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

The device UI uses the following icons:

 Add  Edit  Delete

### To remove a general outbound 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 displays.

7. Click the **OK** button.


Your settings are saved. The rule is removed from the table.

# Outbound NAT rule

Outbound NAT rules control how the router translates the source IP address of traffic that leaves a WAN port. These rules are designed for multiple WAN IP addresses, that is, if you add two additional WAN IP address to one WAN port, you can create two outbound NAT rules. You can create one outbound NAT rule for the source IP address of traffic from a VLAN to translate to one IP address. You can also create another outbound NAT rule that is the source IP address of traffic from another VLAN to translate to another IP address.

An outbound NAT rule on the router defines the following components:

- **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 155.
- **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 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.
- **Outbound Interface:** The interface on which traffic is matched as it exits the firewall.
- **Translation IP Address:** Translate matched traffic to the specified source IP address.

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

## Add an outbound NAT rule

You can add an outbound NAT 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 an outbound NAT 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Firewall >Outbound NAT Rules**.

The Outbound NAT Rules page displays.

5. Click the **Add** icon.

The Add/Edit Outbound NAT Rule pop-up window displays.

6. Configure the following settings:

- a. In the **Name** field, enter a name for the 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. From the **Service** 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 155.

- d. 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.
- e. 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.
- f. From the **Outbound Interface** menu, one of the following:
- **WAN1**
  - **WAN2**
- g. From the **Translation IP Address** menu, select a translation IP address.
7. Click the **Apply** button.

The new outbound NAT rule is added to the table on the Outbound NAT Rules page. If you enabled the new outbound NAT rule (that is, the Enable Rule Status toggle is blue and positioned to the right), it goes into effect immediately.

## Change an outbound NAT rule and enable or disable the rule

You can change an existing outbound NAT rule and enable or disable the rule.

The device UI uses the following icons:



### To change an outbound NAT traffic rule and 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Firewall > Outbound NAT Rules**.

The Outbound NAT 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 Outbound NAT Rule 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 an outbound NAT rule](#) on page 138.

- 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 Outbound NAT Rules page.

## Remove an outbound NAT rule

If you no longer need an outbound NAT rule, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

**To remove an outbound NAT 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Firewall > Outbound NAT Rules**.

The Outbound NAT Rules page displays.

5. In the table, select the check box for the rule.
6. Click the **Delete** icon.

A pop-up window displays.

7. Click the **OK** button.


Your 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 155). 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 121).

 **CAUTION:** If the router is functioning behind another firewall and you configure port forwarding, double NAT might occur. For more information, see [kb.netgear.com/30186](http://kb.netgear.com/30186).

 **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 156). 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 156. 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:



## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 143.

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:



### 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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 99).  
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](http://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](http://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 155) 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 156. 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 156. 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:



### 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 148.

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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 displays.
7. Click the **OK** button.

Your 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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:



## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 156.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

Your 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 **All days** 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:



## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 160.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

Your 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:

- [Display alarms, warnings, and notifications](#)
- [Display the router connectivity, system, port, IPSec VPN, and VLAN settings](#)
- [Display devices attached to the router LAN ports](#)
- [Display the DHCP leases for a VLAN or add a MAC-IP binding](#)
- [Display Ethernet traffic statistics for the WAN and LAN ports](#)
- [Display, save, download, or clear the logs](#)
- [Display the status of site-to-site VPN tunnels](#)
- [Display the status of active client-to-site IPSec VPN tunnels or disconnect a tunnel](#)
- [Display the status of active client-to-site OpenVPN tunnels or disconnect a tunnel](#)
- [Display the status of client-to-site WireGuard VPN tunnels](#)

**!** **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/000065774](http://kb.netgear.com/000065774) 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 displays 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, port, IPSec VPN, and VLAN settings

The Dashboard provides an overview of the router status.

## To display the router connectivity, system, port, IPSec VPN, and VLAN 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 41.
  - **Fan Speed:** The speed of the internal cooling fan in revolutions per minute (RPM)
  - **Temperature:** The temperature inside the chassis
  - **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 183).
- **Ethernet Port Status:** For each LAN and WAN Ethernet port and the LAN4 fiber 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 fiber connection (10000 Mbps or 1000 Mbps). For a port without a connection, the page displays 0 Mbps.
- **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
- **Subnet Mask:** The IP address subnet mask 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 327).

- **IPSec VPN Status:** The following information displays for both site-to-site and client-to-site VPN connections:
  - **In Use:** The number of IPSec VPN tunnels that are in use
  - **Connected:** The number of IPSec VPN tunnels that are connected (up)
  - **Disconnected:** The number of IPSec site-to-site VPN tunnels that are disconnected (down, whether enabled or disabled)
  - **Max Supported:** The maximum number of combined site-to-site and client-to-site VPN tunnels that can be supported. This number is fixed at 60.
- **VLAN Status:** The following information displays for the VLAN ID that you select from the **VLAN Status** menu:
  - **VLAN Name:** The name assigned to the VLAN
  - **VLAN ID:** The identifier (ID) assigned to the VLAN
  - **IP Address:** The IP address that is associated with the VLAN
  - **Subnet Mask:** The IP address subnet mask that is associated with the VLAN
  - **DHCP Range:** The IP address range from which the DHCP server assigns IP addresses to the clients in the VLAN
  - **MAC Address:** The MAC address that is associated with the VLAN

# 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 99), 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.)

- **MAC Address:** The MAC address of the device that received an IPv4 address
- **IP Address:** The IPv4 address that was issued by the DHCP server in the VLAN
- **Device Name:** The name 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 103 or [Remove a MAC-IP binding](#) on page 104.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Monitoring > Logs**.

The Logs page displays.

The page displays 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 227.

### 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

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

The VPN Status page displays.

The Site-to-Site Tunnel Status table 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 227)
- **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 234.
- **Phase 2 Enc/Auth/Grp:** The IPsec Phase 2 authentication algorithm, encryption algorithm, and DH group (see [Predefined IPsec VPN profiles for site-to-site VPN connections](#) on page 219 or [Add a custom IPsec VPN profile](#) on page 221)
- **Local Group:** The LAN IP address or group on the router (see [Add a site-to-site IPsec VPN connection](#) on page 227)
- **Remote Group:** The LAN IP address or group on the remote endpoint (see [Add a site-to-site IPsec VPN connection](#) on page 227)
- **Remote Gateway:** The WAN IP address of the remote endpoint (see [Add a site-to-site IPsec VPN connection](#) on page 227)

## Display the status of active client-to-site IPsec VPN tunnels or disconnect a tunnel

You can display the status of active client-to-site IPsec VPN tunnels that are up between an IPsec VPN client and the router.

For more information about the client-to-site IPsec connection settings, see [Client-to-site IPsec VPN settings](#) on page 238.

## To display the status of active client-to-site IPSec VPN tunnels or disconnect an IPSec client 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

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

The VPN Status page displays.

The Client-to-Site Tunnel Status table displays the total number of active VPN tunnels.

The table displays the following information for each active VPN tunnel:

- **Name:** The name of the VPN tunnel (see [Add a client-to-site IPSec VPN connection](#) on page 240)
- **Peer IP Address:** The WAN IP address of the VPN client (see [Add a client-to-site IPSec VPN connection](#) on page 240)
- **LAN IP Address:** The LAN IP address that the router assigned to the VPN client from the configured pool of LAN IP addresses (see [Add a client-to-site IPSec VPN connection](#) on page 240)
- **User:** The user name for the VPN client (see [Add a VPN user account](#) on page 267)
- **Phase1 Enc/Auth/Grp** and **Phase2 Enc/Auth/Grp:** The IPSec Phase 1 and Phase 2 authentication algorithms, encryption algorithms, and DH groups for the VPN

tunnel (see [Predefined IPSec VPN profiles for client-to-site VPN connections](#) on page 220) or [Add a custom IPSec VPN profile](#) on page 221)

5. To disconnect a VPN client tunnel, click the **Disconnect** icon in the Disconnect column for the VPN client.

## Display the status of active client-to-site OpenVPN tunnels or disconnect a tunnel

You can display the status of active client-to-site OpenVPN tunnels that are up between an OpenVPN client and the router.

For more information about the client-to-site OpenVPN connection settings, see [Client-to-site OpenVPN settings](#) on page 254.

### To display the status of active client-to-site OpenVPN tunnels or disconnect an OpenVPN client 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

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

The VPN Status page displays.

The OpenVPN Status table displays the total number of active VPN tunnels.

The table displays the following information for each active VPN tunnel:

- **Name:** The name of the VPN tunnel (see [Enable and configure OpenVPN with TUN mode on the router](#) on page 255 or [Enable and configure OpenVPN with TAP mode on the router](#) on page 257)
- **Peer IP Address:** The WAN IP address of the VPN client
- **LAN IP Address:** The LAN IP address that the router assigned to the VPN client from the configured pool of LAN IP addresses (see [Enable and configure OpenVPN with TUN mode on the router](#) on page 255 or [Enable and configure OpenVPN with TAP mode on the router](#) on page 257)
- **Port:** The port number for the OpenVPN connection (see [Enable and configure OpenVPN with TUN mode on the router](#) on page 255 or [Enable and configure OpenVPN with TAP mode on the router](#) on page 257)
- **User:** The user name for the VPN client (see [Add a VPN user account](#) on page 267)
- **Connection Time:** The period that the tunnel has been up
- **Tx MB:** The amount of transmitted traffic in MB
- **Rx MB:** The amount of received traffic in MB

5. To disconnect a VPN client tunnel, click the **Disconnect** icon in the Disconnect column for the VPN client.

## Display the status of client-to-site WireGuard VPN tunnels

You can display the status of client-to-site WireGuard VPN tunnels that are up between a WireGuard VPN client and the router as well as the disconnected tunnels.

For more information about the client-to-site WireGuard VPN connection settings, see [Manage WireGuard VPN Tunnels](#) on page 291.

### To display the status of client-to-site WireGuard 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

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

The VPN Status page displays.

The OpenVPN Status table displays the total number of active VPN tunnels.

The table displays the following information for each active VPN tunnel:

- **Name:** The name of the VPN client (see [Add a WireGuard VPN client account](#) on page 297)
- **Status:** The status of the VPN tunnel (Connected or Disconnected)
- **Peer IP Address:** The LAN IP address that the router assigned to the VPN client from the configured pool of LAN IP addresses (see [Enable and configure WireGuard VPN on the router](#) on page 293)
- **LAN IP Address:** The LAN IP address assigned in the client's LAN subnet
- **Port:** The port number for the WireGuard VPN connection (see [Enable and configure WireGuard VPN on the router](#) on page 293)
- **Public Key:** The public key that is used by the VPN client (see [Add a WireGuard VPN client account](#) on page 297)
- **Latest Handshake:** The time of the most recent handshake between the router and the VPN client
- **Tx MB:** The amount of transmitted traffic in MB
- **Rx MB:** The amount of received traffic in MB

**!** **NOTE:** For information about disabling a client's WireGuard VPN tunnel, see [Change a WireGuard VPN client account](#) on page 299.

# 8

## Maintain the Router

---

This chapter describes how you can maintain the router.

The chapter includes the following sections:

- [Change the device name](#)
- [Manage the firmware of the router](#)
- [Manage the configuration file of the router](#)
- [admin user account](#)
- [Set the time zone and daylight saving time](#)
- [Set custom NTP servers](#)
- [Manage the syslog server settings](#)
- [Enable or disable UPnP](#)
- [Enable or disable LLDP and display the LLDP neighbors](#)
- [Simple Network Management Protocol](#)
- [Manage the LEDs](#)
- [Reboot the router from the device UI](#)
- [Return the router to its factory default settings](#)

**!** **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/000065774](http://kb.netgear.com/000065774) 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 183.

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 184.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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/](http://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 32.

5. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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

`ProRouter-PR00X-20240721-132812-config.tar`.

The name is Pro Router; the model is PR00X; the date is July 21, 2024; 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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

`ProRouter-PR00X-20240721-132812-config.tar`.


The name is Pro Router; the model is PR00X; the date is July 21, 2024; 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 New 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.

- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 191), 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 32.

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 displays 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 195.

## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 194.

## 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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.
3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **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.

# Enable or disable LLDP and display the LLDP neighbors

Link Layer Discovery Protocol (LLDP) is a layer 2 protocol allowing devices to advertise link and endpoint information that can be used to discover link neighbors and their capabilities.

You can enable or disable LLDP at a global level (that is, for all ports) and at a port level. For example, you can enable LLDP globally, but then disable it on individual ports.

By default LLDP is enabled globally and on all ports, except, for security reasons, on the WAN1 port.

## To enable or disable LLDP and display the LLDP neighbors:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > LLDP**.

The LLDP page displays.

5. Click the **Enable LLDP** toggle to enable or disable LLDP globally:

- **The toggle is blue and positioned to the right:** LLDP is globally enabled. This is the default setting.
  - **The toggle is gray and positioned to the left:** LLDP is globally disabled.
6. In the Port section, click the toggle for an individual port to enable or disable LLDP for the port:
- **The toggle is blue and positioned to the right:** LLDP is enabled for the port. This is the default setting for all ports except for the WAN1 port.
  - **The toggle is gray and positioned to the left:** LLDP is disabled for the port.
7. Click the **Apply** button.
- Your settings are saved.
- After a while, the LLDP Neighbors table is populated with detected LLDP neighbors.
8. To refresh the information on the page, click the **Refresh** button.
- The following information displays in the table:
- **Local Port:** The router port on which the neighbor is detected
  - **Chassis ID Subtype:** The chassis ID subtype of the neighbor (for example, MAC)
  - **Chassis ID:** The chassis ID of the neighbor (for example, the MAC address)
  - **Port ID Subtype:** The port ID subtype of the neighbor (for example, MAC)
  - **Port ID:** The port ID of the neighbor (for example, the MAC address)
  - **System Name:** The system name of the neighbor
  - **Management IP Address:** The management IP address of the neighbor
  - **TTL:** The time-to-live (TTL) period during which the LLDP advertisement of the router is saved on the neighbor
  - **Capabilities:** The device capabilities that the neighbor advertises

## Simple Network Management Protocol

You can configure SNMP settings for SNMPv1, SNMPv2, and SNMPv3. The router supports the configuration of SNMP communities and users that can monitor the router over SNMP, receive trap messages, or do both.

The router uses both standard public MIBs for standard functionality and private MIBs that support additional router functionality.

# Configure the SNMP system name, contact and location

## You can configure the SNMP system name, system contact, and system location.

To add the SNMP system name, contact and 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Configuration**.

The SNMP Configuration page displays.

5. In the **System Name** field, type a system name.
6. In the **System Contact** field, type a system contact.
7. In the **System Location** field, type a system location.
8. Click the **Apply** button.

Your settings are saved.

# Configure the SNMPv1 and SNMPv2 client

You can configure the SNMPv1 and SNMPv2 client so that SNMP community members can view the configuration of the router as read-only through SNMP. To access the router over SNMP, you need to use the client IP address of the router.

The device UI uses the following icons:



## To configure the SNMPv1 and SNMPv2 client:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Configuration**.

The SNMP Configuration page displays.

5. Enable the **SNMP v1/v2** toggle so that it displays blue and is positioned to the right.  
By default, the SNMP toggle is disabled, displays gray, and is positioned to the left.
6. In the **Community Private String** field, type a community private string.
7. In the **Community Public String** field, type a community public string.
8. In the **Client IP Address** field, type the IP address of the client.
9. Click the **Apply** button.

Your settings are saved.

## Configure the SNMPv3 user account

Any user can connect to the router using the SNMPv3 protocol, but for authentication and encryption, the router supports only one user, which is the admin user. Therefore, you can configure only one SNMPv3 profile. To access the router over SNMPv3, you need to use the SNMPv3 user name.

### To configure authentication and encryption settings for the SNMPv3 admin 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Configuration**.

The SNMP Configuration page displays.

5. Enable the **SNMPv3** toggle so that it displays blue and is positioned to the right.  
By default, the SNMP toggle is disabled, displays gray, and is positioned to the left.
6. In the **User Name** field, type the SNMP v3 user name.

This defines who is allowed to authenticate and access the SNMP data.

7. From the **Authentication Algorithm** menu, select one of the following options as the algorithm to use for authentication:

- **MD5**: Message Digest 5 (MD5) is the authentication protocol.
  - **SHA**: Secure Hash Algorithm (SHA) is the authentication protocol. SHA provides stronger security than MD5.
  - **SHA 224**: A cryptographic hash algorithm that is reliable and safe in a variety of applications.
  - **SHA-256**: A secure hash algorithm that is superior to SHA-224.
  - **SHA-384**: A secure hash algorithm that is superior to SHA-256.
  - **SHA-512**: A secure hash algorithm that is superior to SHA-384.
8. In the **Authentication Password** field, enter a password.  
The password must be between 8 and 64 characters and cannot contain spaces.  
With any selection of authentication protocol, the admin login password for the device UI is used as the SNMPv3 authentication password.
9. To enable encryption, do the following:
- a. From the **Encryption Algorithm** menu, select one of the following options as the algorithm to use for encryption:
    - **AES**
    - **AES-128**
  - b. In the **Encryption Password** field, type an encryption code of eight or more alphanumeric characters.  
The password must be between 8 and 64 characters and cannot contain spaces.
10. Click the **Apply** button.  
Your settings are saved.

## Manage the SNMPv1, SNMPv2, and SNMPv3 trap recipients

You can configure SNMPv1 and SNMPv2 communities, and SNMPv3 users that must be able to receive traps.

### Add an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps

You can add an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps.

## To add an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps:

The device UI uses the following icons:

 Add  Edit  Delete

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Trap**.

The SNMP Trap page displays.

5. Depending on the community or user you want to add, do one of the following:
  - **Add an SNMPv1 or SNMPv2 community as a trap recipient:**
    - a. In the **SNMP v1/v2 Configuration** section, click the **Add** icon.  
The Add/Edit SNMP v1/v2 Configuration pop-up window displays.
    - b. In the **Community Name** field, type the name of the SNMP community that includes the host.
    - c. In the **Trap Receiver IP Address** field, type the IP address of the SNMP community.
    - d. In the **Port** field, type the port number on the device you want to use.
    - e. From the **Version** menu, select the SNMP version that is used by the host:

- **SNMPv1**: The router uses SNMPv1 to send traps to the receiver. This is the default setting.
- **SNMPv2**: The router uses SNMPv2 to send traps to the receiver.
- f. Click the **Apply** button.  
Your settings are saved and the trap configuration is added.
- **Add an SNMPv3 user as a trap recipient:**
  - a. In the **SNMP v3 Configuration** section, click the **Add** icon.  
The Add/Edit SNMP v3 Configuration pop-up window displays.
  - b. In the **User Name** field, type the SNMP v3 user name.  
This name defines who can authenticate and access the SNMP data.
  - c. In the **Trap Receiver IP Address** field, type the IP address of the client.
  - d. In the **Port** field, type the port number on the router you want to use.
  - e. From the **Authentication Algorithm** menu, select one of the following options as the algorithm to use for authentication:
    - **MD5**: Message Digest 5 (MD5) is the authentication protocol.
    - **SHA**: Secure Hash Algorithm (SHA) is the authentication protocol. SHA provides stronger security than MD5.
    - **SHA 224**: A cryptographic hash algorithm that is reliable and safe in a variety of applications.
    - **SHA-256**: A secure hash algorithm that is superior to SHA-224.
    - **SHA-384**: A secure hash algorithm that is superior to SHA-256.
    - **SHA-512**: A secure hash algorithm that is superior to SHA-384.
  - f. In the **Authentication Password** field, type a password.  
The password must be between 8 and 64 characters and cannot contain spaces.  
With any selection of authentication protocol, the admin login password for the device UI is used as the SNMPv3 authentication password.
  - g. To enable encryption, do the following:
    - i. From the **Encryption Algorithm** menu, select one of the following options as the algorithm to use for encryption:
      - **AES**: This is the default setting.
      - **AES-128**
    - ii. In the **Encryption Password** field, type an encryption code of eight or more alphanumeric characters.

The password must be between 8 and 64 characters and cannot contain spaces.

- iii. Click the **Apply** button.

Your settings are saved and the trap configuration is added.

## Change an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receives traps

You can change an existing SNMPv1 or SNMPv2 community or an SNMPv3 user that receives traps.

The device UI uses the following icons:



### To change an SNMPv1 or SNMPv2 community or an SNMPv3 user that receives traps:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Trap**.

The SNMP Trap page displays.

5. Depending on the community or user you want to add, do one of the following:

- **Change an SNMPv1 or SNMPv2 community configuration as a trap recipient:**
  - a. In the **SNMP v1/v2 Configuration** section, select the check box for the trap configuration.
  - b. Click the **Edit** icon.  
The Add/Edit SNMP v1/v2 Configuration pop-up window displays.
  - c. Change the settings as needed.  
For more information about the settings, see [Add an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps](#) on page 204.
  - d. Click the **Save** button.  
Your settings are saved.
- **Change the SNMPv3 user trap recipient configuration:**
  - a. In the **SNMP v3 Configuration** section, select the check box for the trap configuration.
  - b. Click the **Edit** icon.  
The Add/Edit SNMP v3 Configuration pop-up window displays.
  - c. Change the settings as needed.  
For more information about the settings, see [Add an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps](#) on page 204.
  - d. Click the **Save** button.  
Your settings are saved.

## Delete an SNMPv1 or SNMPv2 community or an SNMPv3 user that must receive traps

You can delete SNMPv1 or SNMPv2 community or an SNMPv3 user that receives traps. The device UI uses the following icons:

 Add  Edit  Delete

### To delete an SNMPv1 or SNMPv2 community or an SNMPv3 user that receives traps:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Trap**.

The SNMP Trap page displays.

5. In the **SNMP v1/v2 Configuration** or **SNMP v3 Configuration** section, select the check box for the trap configuration.

6. Click the **Delete** icon.

Your settings are saved.

## Configure trap flags

You can enable or disable specific traps. When the condition that is identified by an active trap occurs on the router, a trap message is sent to any enabled SNMP trap receivers (also referred to as hosts), and a message is written to the trap log.

### To configure the trap flags:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > SNMP Trap**.

The Trap Flags page displays.

By default, all of the following trap flags are disabled, and their associated toggles are gray and positioned to the left:

- **Authentication:** When enabled, SNMP traps are sent when events involving authentication occur, such as when a user attempts to access the device UI but does not provide a valid user name and password.
- **Link Up/Down:** When enabled, SNMP traps are sent when the administrative or operational state of a physical or logical interface link changes.
- **VPN Status:** When enabled, a SNMP trap is generated when the VPN status changes or an event happens. For example, when OpenVPN connects or disconnects.

 **NOTE:** WireGuard VPN is not supported for status reporting through SNMP.

- **Traffic Stats:** When enabled, a query is sent to get the statistics that are displayed in the Statistics page of the device UI. (**Monitoring > Statistics**).

5. To enable a trap flag, click the associated toggle.

The toggle is blue and positioned to the right.

6. Click the **Apply** button.

Your settings are saved.

# Display the supported MIBs

## To display the MIBs that are supported by 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Administration > SNMP > Supported MIBs**.

The Supported MIBs page displays.

The Name field displays the RFC number, if applicable, and the name of the MIB.

The Description field displays the RFC title or MIB description.

**! NOTE:** A Request for Comments (RFC) is a document from the Internet Engineering Task Force (IETF).

# 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 39 or [Add the router to NETGEAR Insight using the Insight app](#) on page 40.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 and OpenVPN Tunnels

---

The router supports predefined and manually configured IP security (IPSec) profiles for site-to-site VPN tunnels, client-to-site IPSec VPN tunnels, and client-to-site OpenVPN tunnels.

This chapter describes how to set up IPSec VPN profiles, site-to-site connections, client-to-site IPSec VPN connections, and client-to-site OpenVPN connections on the router using the device UI.

The chapter includes the following sections:

- [About IPSec VPN](#)
- [IPSec VPN profiles](#)
- [Site-to-site VPN settings](#)
- [Client-to-site IPSec VPN settings](#)
- [Client-to-site OpenVPN settings](#)
- [VPN user accounts](#)
- [Certificates](#)

**!** **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/000065774](http://kb.netgear.com/000065774) for knowledge base articles about NETGEAR Insight.

# About IPSec VPN

The router supports the following types of virtual private networks (VPNs) or VPN tunnels:

- **Site-to-site connection:** 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.
- **Client-to-site connection:** Lets you securely connect a client (usually a single device such as a computer, tablet, or smartphone) at a remote site such as a home office to a VPN router at a business office. Once the tunnel is established, the remote client can access the network at the business office as if the client were locally connected. This type of VPN connection is also called a client-to-gateway connection, where the VPN router is the gateway.

The router supports the following types of VPN profiles:

- **Predefined IPSec VPN profiles:** The device UI includes the following types of predefined VPN profiles:
  - **VPN profiles for paid or free VPN services:** VPN IPSec profiles that you can use for paid or free VPN services. These profiles include *Amazon Web Services (AWS)* and *Microsoft Azure* (see [Predefined IPSec VPN profiles for site-to-site VPN connections](#) on page 219.) Although the profile names include *Amazon* and *Microsoft*, you can use these profiles for any services, including free services.
  - **Default VPN profiles:** Default profiles that you can use for site-to-site VPN services (see [Predefined IPSec VPN profiles for site-to-site VPN connections](#) on page 219) or client-to-site VPN services (see [Predefined IPSec VPN profiles for client-to-site VPN connections](#) on page 220).
- **Custom IPSec VPN profiles:** You can use the device UI to set up a custom IPSec profile (see [Add a custom IPSec VPN profile](#) on page 221).

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 227) or a client-to-site connection (see [Client-to-site IPSec VPN settings](#) on page 238).

## IPSec VPN profiles

An IPSec VPN profile is a set of protocols and encryption, authentication, and integrity-check algorithms that form a building block for an VPN tunnel configuration. You must first set up an IPSec profile (or use a predefined IPSec profile), and then define the VPN tunnel settings.

An IPsec VPN profile defines the following protocols and algorithms, also referred to as 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 partners *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 partners 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 partners, and how the VPN tunnel traffic is kept secure *after* the tunnel established.

You must specify the encapsulation protocol, encryption algorithm, and an integrity check algorithm that allows the VPN partner to guard against modification of the tunnel and the traffic that is transported through the tunnel. Here too, both VPN partners must use the same algorithms.

For more details about these settings, and for information about how to set up a custom IPsec VPN profile, see [Add a custom IPsec VPN profile](#) on page 221.

The router also includes predefined IPsec VPN profiles for VPN services:

- [Predefined IPsec VPN profiles for site-to-site VPN connections](#) on page 219
- [Predefined IPsec VPN profiles for client-to-site VPN connections](#) on page 220

## Predefined IPsec VPN profiles for site-to-site VPN connections

The router includes predefined VPN IPsec profiles that you can use for or free paid site-to-site VPN services. These profiles include *Amazon\_Web\_Services* (AWS) and *Microsoft\_Azure*. A *Default* profile is also included. Although the profile names include *Amazon* and *Microsoft*, you can use these profiles for any services, including free services.

You can select one of these IPsec profiles when you add a site-to-site VPN connection (see [Add a site-to-site IPsec VPN connection](#) on page 227).

The following table lists the predefined settings for IPsec profiles for use with a site-to-site VPN connection. For detailed descriptions of these settings, see [Add a custom IPsec VPN profile](#) on page 221.

Table 4. Predefined IPSec VPN profiles for site-to-site connections

Settings	Amazon Web Services	Microsoft Azure	Default
IKE Version	IKE1	IKE1	IKE2
Protocol Selection	ESP	ESP	ESP
<b>Phase I Options</b>			
Encryption	AES-128	AES-256	AES-128
Authentication	SHA-1	SHA-1	SHA-1
DH Group	Group2 - 1024bits	Group2 - 1024bits	Group5 - 1536bits
SA lifetime	28800	28800	28800
<b>Phase II Options</b>			
Encryption	AES-128	AES-256	AES-128
Authentication	SHA-1	SHA-1	SHA-1
DH Group	Group2 - 1024bits	Group2 - 1024bits	Group5 - 1536bits
SA lifetime	3600	3600	3600

## Predefined IPSec VPN profiles for client-to-site VPN connections

The router includes predefined VPN IPSec profiles that you can use for client-to-site VPN services. These profiles include *Default\_Client\_to\_Site\_IKE1* and *Default\_Client\_to\_Site\_IKE2*.

You can select one of these IPSec profiles when you add a client -to-site VPN connection (see [Add a site-to-site IPSec VPN connection](#) on page 227).

The following table lists the predefined settings for IPSec profiles for use with a client-to-site VPN connection. For detailed descriptions of these settings, see [Add a custom IPSec VPN profile](#) on page 221.

Table 5. Predefined IPSec VPN profiles for client-to-site connections

Settings	Default_Client_to_Site_IKE1	Default_Client_to_Site_IKE2
IKE Version	IKE1	IKE2
Protocol Selection	ESP	ESP
<b>Phase I Options</b>		

Table 5. Predefined IPSec VPN profiles for client-to-site connections (Continued)

Settings	Default_Client_to_Site_IKE1	Default_Client_to_Site_IKE2
Encryption	AES-256	Proposal 1: AES-256 Proposal 2: AES-128
Authentication	SHA2-256	Proposal 1: SHA2-256 Proposal 2: SHA-1
DH Group	Group14 - 2048bits	Proposal 1: Group14 - 2048bits Proposal 2: Group14 - 1024bits
SA lifetime	28800	28800
<b>Phase II Options</b>		
Encryption	AES-256	Proposal 1: AES-256 Proposal 2: AES-128 Proposal 3: AES-256 Proposal 4: AES-128
Authentication	SHA2-256	Proposal 1: SHA2-256 Proposal 2: SHA-1 Proposal 3: SHA2-256 Proposal 4: SHA-1
DH Group	Off	Proposal 1: Group14 - 2048bits Proposal 2: Group14 - 1024bits Proposal 3: Off Proposal 4: Off
SA lifetime	3600	3600

## Add a custom 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 227) or between a client and a VPN router (see [Add a client-to-site IPSec VPN connection](#) on page 240), you must define the IPSec profile that secures the VPN tunnel between the sites or the client and the site.

Internet Key Exchange (IKE) is the protocol that is used to set up security associations (SAs) between VPN routers or a client and a VPN router to ensure the following:

- The VPN tunnel is established between the correct partners.
- 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:



### To add a custom 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

**! NOTE:** The only selection from the **Protocol Selection** menu is ESP (Encapsulating Security Payload, which authenticates, encrypts, and guards against data changes during transmission. This is the fixed setting.

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
Encryption	<p>Select one of the following encryption algorithms, each of which, in ascending order, provides more security:</p> <ul style="list-style-type: none"> <li>• <b>3DES:</b> Triple Data Encryption Standard (3DES).</li> <li>• <b>AES-128:</b> Advanced Encryption Standard (AES) with a 128-bit key size. (The default setting.)</li> <li>• <b>AES-192:</b> AES with a 192-bit key size.</li> <li>• <b>AES-256:</b> AES with a 256-bit key size.</li> <li>• <b>AES128-CGM-16:</b> AES with a 128-bit key size and Galois/Counter Mode (CGM) with an Integrity Check Value (ICV) of 16 bytes. For Phase I, this algorithm is available only if you select IKE2.</li> <li>• <b>AES256-CGM-16:</b> AES with a 256-bit key size and CGM with an ICV of 16 bytes. For Phase I, this algorithm is available only if you select IKE2.</li> </ul>
Authentication	<p>Select one of the following authentication algorithms, each of which, in ascending order, provides more security:</p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> Hash algorithm that produces a 128-bit digest.</li> <li>• <b>SHA1:</b> Hash algorithm that produces a 160-bit digest. (The default setting.)</li> <li>• <b>SHA2-256:</b> Hash algorithm that produces a 256-bit digest.</li> </ul>
DH Group	<p>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.</p> <p>The default setting is Group5 - 1536 bits, which provides an algorithm with 1536 bits.</p>

9. To add another algorithm for the same Phase 1, click the **Add Algorithm** button, and repeat the previous step.

Adding more algorithms improves the chances of devices being able to find a match, because not all devices might support the same types of algorithms.

10. In the **SA Lifetime** field for the Phase I, type the period in seconds during which the IKE security association (SA) is valid.

If the period times out, the next rekeying occurs. The default is 28800 seconds (8 hours). The period can be between 3600 and 86400 seconds.

11. 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
Encryption	<p>Select one of the following encryption algorithms, each of which, in ascending order, provides more security:</p> <ul style="list-style-type: none"> <li>• <b>3DES</b>: Triple Data Encryption Standard (3DES).</li> <li>• <b>AES-128</b>: Advanced Encryption Standard (AES) with a 128-bit key size. (The default setting.)</li> <li>• <b>AES-192</b>: AES with a 192-bit key size.</li> <li>• <b>AES-256</b>: AES with a 256-bit key size.</li> <li>• <b>AES128-CGM-16</b>: AES with a 128-bit key size and Galois/Counter Mode (CGM) with an Integrity Check Value (ICV) of 16 bytes.</li> <li>• <b>AES256-CGM-16</b>: AES with a 256-bit key size and CGM with an ICV of 16 bytes.</li> </ul>
Authentication	<p>Select one of the following authentication algorithms, each of which, in ascending order, provides more security:</p> <ul style="list-style-type: none"> <li>• <b>MD5</b>: Hash algorithm that produces a 128-bit digest.</li> <li>• <b>SHA1</b>: Hash algorithm that produces a 160-bit digest. (The default setting.)</li> <li>• <b>SHA2-256</b>: Hash algorithm that produces a 256-bit digest.</li> </ul>
DH Group	<p>The Diffie-Hellman (DH) group sets the strength of the algorithm in bits. From the menu, select one of the DH groups, each of which, in ascending order, provides more security but might require more computing power and slow down the Phase II traffic.</p> <p>The default setting is Group5 - 1536 bits, which provides an algorithm with 1536 bits.</p>

12. To add another algorithm for the same Phase II, click the **Add Algorithm** button, and repeat the previous step.

Adding more algorithms improves the chances of devices being able to find a match, because not all devices might support the same types of algorithms.

13. In the **SA Lifetime** field for the Phase II, type the period in seconds during which the IKE security association (SA) is valid.

If the period times out, the next rekeying occurs. The default is 3600 seconds (1 hour). The period can be between 3600 and 28800 seconds.

14. 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.

You also cannot change an IPSec VPN profile that is in use for an IPSec VPN connection.

**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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 a custom IPSec VPN profile](#) on page 221.

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 that you added, you can remove it. You cannot remove a predefined IPSec VPN profile.

You also cannot remove an IPSec VPN profile that is in use for an IPSec VPN connection.

The device UI uses the following icons:



### 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

Your 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 determine 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 IPSec VPN profiles for site-to-site VPN connections](#) on page 219) or that you already set up ([Add a custom IPSec VPN profile](#) on page 221).

When you add a site-to-site IPSec VPN connection, in addition to selecting an IPSec profile, 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.

## 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 IPSec VPN profiles for site-to-site VPN connections](#) on page 219) or that you already set up ([Add a custom IPSec VPN profile](#) on page 221).
- 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:



### **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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Site-to-Site**.

The Site-to-Site page displays.

5. Click the **Add** icon.

The Add/Edit a 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 IPSec VPN profiles for site-to-site VPN connections](#) on page 219 or [Add a custom IPSec VPN profile](#) on page 221.

9. In the **Remote Endpoint** field, type either the WAN IP address or the domain name of the remote VPN router.

10. 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.

To display the password on the page, click the **eye** icon.

11. In the **Local Networks** section, click the **Add** icon to create a local network.

The Add/Edit Local Network page displays.

- a. In the **Add/Edit Local Network** page, from the menu, select a VLAN or **Custom**.
- b. In the **IP Address** field, type an IP address.
- c. In the **Subnet Mask** field, type a subnet mask.
- d. Click the **Add** button.

Your settings are saved and the local network is created.

To change the local network, click the **Edit** icon and change the IP address or subnet mask.

To delete the local network, select the associated check box, and click the **Delete** icon.

12. In the **Remote Networks** section, click the **Add** icon to create a remote network.

The Add/Edit Remote Network page displays.

- a. In the **Add/Edit Remote Network** page, in the **IP Address** field, type an IP address.
- b. In the **Subnet Mask** field, type a subnet mask.
- c. Click the **Add** button.

Your settings are saved and the remote network is created.

To change the remote network, click the **Edit** icon and change the IP address or subnet mask.

To delete the remote network, select the associated check box, and click the **Delete** icon.

13. In the **Local Identifier** section, specify one of the following settings:


- **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.

These settings specify the LAN IP addresses that the VPN tunnel can access on the router.

14. In the Remote Identifier section, specify one of the following settings:

- **Remote WAN IP:** The WAN IP address of the remote VPN router.
- **Remote FQDN:** The domain name for the remote VPN router.

These settings 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.

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 234).

# Configure remote device management and DPD options for a site-to-site IPSec VPN connection

You can set up the following optional features that apply to the site-to-site VPN connection:

- **Remote Device Management:** You can either allow or disallow remote device management the router. By default, remote device management is disallowed.
- **Dead Peer Detection:** Dead Peer Detection (DPD) is a mechanism that can prevent a VPN tunnel from being disconnected when traffic is idle. In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use DPD to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason. For DPD to function, the peer VPN device on the other end of the tunnel also needs to support DPD.

The device UI uses the following icons:

 Add  Add from existing VLAN  Edit  Delete

## To configure remote device management and DPD options for 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 client-to-site IPSec VPN connection, and click the **Edit** icon.

The Add/Edit a New Connection window displays and shows the basic settings.

6. Select the **Advanced Settings** tab.

The Add/Edit a New Tunnel window adjusts and shows the advanced settings.

7. Click the **Allow Remote Device Management** toggle to allow or disallow remote management of the router:

- **Allow Remote Device Management:** Click the **Allow Remote Device Management** toggle so that it is blue and positioned to the right.
- **Disallow Remote Device Management:** Click the **Allow Remote Device Management** toggle so that it is gray and positioned to the left (the default setting).

8. To configure DPD, in the DPD Options section, do the following:

- a. Make sure that the DPD options are enabled:

By default, the **Enable DPD Option** toggle is blue and positioned to the right, which means that dead peer detection (DPD) is enabled. If the DPD is disabled, the **Enable DPD Option** toggle is gray and positioned to the left.

- b. Set the DPD delay period:

In the **DPD Delay** field, type the period in seconds between consecutive DPD messages. The default is 10 seconds. The period can be between 10 and 300 seconds.

- c. Set the DPD detection time:

In the **Detection Time** field, type the period in seconds during which the client must receive a DPD response from the remote VPN router. If this period is exceeded, the VPN tunnel is torn down and the client attempts to reestablish it.

The default is 30 seconds. The period can be between 30 and 1800 seconds.

- d. Select the action that must occur if no timely DPD response is received from the remote VPN router:

- **None:** No action.
- **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.

If the router detects a connection failure with the remote VPN router, it tears down the VPN tunnel and attempts to reestablish it.

9. Click the **Apply** button.

Your settings are saved.

## 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 the site-to-site VPN configurations 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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:

- **Enabled:** Displays if the VPN configuration is enabled (the check box is selected) or disabled (the check box is cleared).
- **Connection Name:** The name for the site-to-site configuration.
- **Remote Endpoint:** The WAN IP address of the remote endpoint.
- **IPSec Profile:** The IPSec profile that you selected for the site-to-site configuration.
- **Local Networks:** The LAN IP address or group on the router.
- **Remote Networks:** 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.

- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.

- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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/Edit a New Connection page 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 227.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

Your settings are saved. The connection is removed from the table.

## Example of a site-to-site VPN tunnel

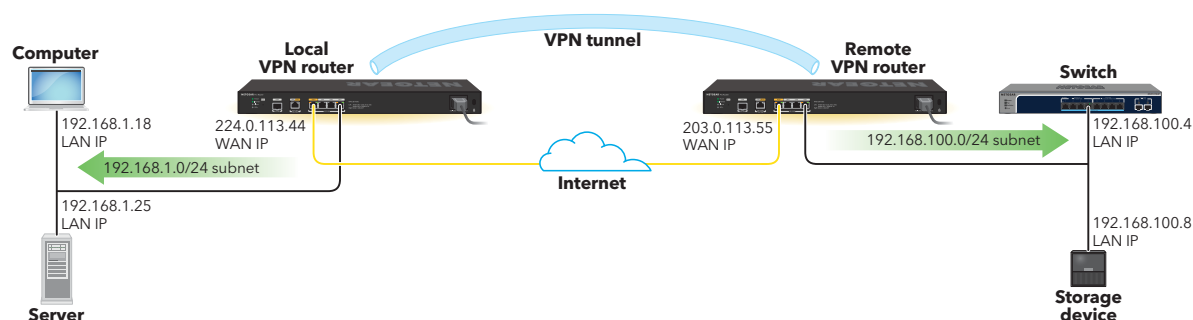


Figure 3. Site-to-site VPN tunnel

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 224.0.113.44, which is the local identifier in the site-to-site IPSec VPN connection settings.
- The local group LAN subnet is 192.168.1.0/24.
- A computer that is connected to the local router receives a DHCP-assigned IP address of 192.168.1.18, and a server receives a DHCP-assigned IP address of 192.168.1.25
- **Remote VPN router (the remote endpoint):**
  - An ISP assigns the remote router a public WAN IP address of 203.0.113.55, which is the remote endpoint IP address in the site-to-site IPSec VPN connection settings.
  - The remote group LAN subnet is 192.168.100.0/24.
  - The remote router is connected to an existing office network that includes a switch that receives a DHCP-assigned IP address of 192.168.100.4, and storage device that receives a DHCP-assigned IP address of 192.168.100.8.

In this VPN configuration, after the VPN tunnel is up, the following applies to the computer with IP address 192.168.1.18 on the local network, depending on any additional security settings for individual devices:

- The computer with LAN IP address 192.168.1.18 can ping the remote endpoint at LAN IP address 192.168.100.1 and the local router at LAN IP address 192.168.1.1 because the computer and both routers function in the same VPN network.
- The computer can access devices in the LAN subnet 192.168.100.0/24 at the office network of the remote endpoint. For example, the computer can access devices behind the switch at IP address 192.168.100.4 and a share on the storage device at IP address 192.168.100.8.
- The computer can access devices in the LAN subnet 192.168.1.0/24 at the site of the local router. For example, the computer can access the server at LAN IP address 192.168.1.25.

In general, devices (clients) at each site can access devices at both sites, at an IP address in the LAN subnet of each router.

## Client-to-site IPSec VPN settings

To set up a client-to-site IPSec VPN tunnel, you do not need to install any special software (such as OpenVPN) on the VPN clients. The client-to-site VPN settings determine the WAN and LAN IP addresses at which the VPN client can reach the router.

When you define the settings for a client-to-site VPN tunnel, you must select an IPSec profile that is either predefined (see [Predefined IPSec VPN profiles for client-to-site VPN](#))

[connections](#) on page 220) or that you already set up ([Add a custom IPSec VPN profile](#) on page 221).

When you add a client-to-site IPSec VPN connection, in addition to selecting an IPSec profile, you must define the following VPN settings:

- **Authentication method:** The authentication method that lets the VPN client and the router identify and authenticate each other before the VPN tunnel is established:
  - **PSK:** The pre-shared key (PSK) is a password that must be present on both the VPN client and the router.
  - **EAP-MSCHAPv2:** Protected Extensible Authentication Protocol (AEP) Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2) is an authentication method that requires the same authentication certificate on both the VPN client and the router.

If you use an authentication certificate, you must first either create one or import one (see [Certificates](#) on page 271) on the router and then export the certificate to the VPN clients so that they can use it when establishing a VPN tunnel to the router.
- **Local identifier:** The local IP address settings of the router, which can be either the router's IP address or the router's local WAN IP address or local FQDN (for this purpose, you can use any name to identify the router).
- **Remote identifier:** The WAN IP address or FQDN of the VPN client. You can also specify ANY, which means that any identifier or even no identifier is accepted by router.
- **IP address range for the client LAN IP addresses:** The LAN IP address pool from which the router assigns the VPN client an IP address after initial connection, and which cannot not overlap with any WAN, VLAN, or other VPN IP subnets that are in use on the router.
- **DNS servers:** The DNS servers that the router assigns to the VPN client after initial connection.

**! NOTE:** The settings that are defined on the VPN client and the router must match:

- On the VPN client, the local settings are for the VPN client and the remote settings are for the router.
- On the router, the local settings are for the router and the remote settings are for the VPN client.
- On both the VPN client and the router, the IP addressing scheme must be coordinated and both the IPSec phase I options and IPSec phase II options must be identical on the VPN client and the router.

# Operating systems, tunneling protocol, and authentication supported for VPN clients

The following table shows the tunnel protocol and authentication that are supported by operating systems on clients establishing a VPN connection to the router.

Table 6. Operating systems, tunneling protocol, and authentication supported for VPN clients

Tunneling Protocol and Authentication	Windows 10, 11	iOS/iPad OS 12, 15, 16, 17	Mac OS 12, 13, 14	Android 12, 13, 14
IKEv1 PSK + XAUTH (PSK, user name, password)	---	<b>Yes</b>	<b>Yes</b>	---
IKEv2 (PSK)	---	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
IKEv2 EAP - MSCHAPv2 (CA certificate, server certificate, user name, password)	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>

## Add a client-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 IPSec VPN profiles for client-to-site VPN connections](#) on page 220) or that you already set up ([Add a custom IPSec VPN profile](#) on page 221).
- Set the authentication method for authentication between the VPN client and the router and, depending on the method, select a server certificate or pre-shared key.

**NOTE:** If you plan on using the EAP-MSCHAPv2 authentication method, you must have imported or created a certificate (see [Certificates](#) on page 271) on the router so that you can select the certificate.

- Set the local identifier (a local IP address, WAN IP address, or FQDN) that is used for the VPN tunnel on the router.

When you configure the settings on the router, the local identifier refers to the settings for the router.

- Set the remote identifier (the remote WAN IP address, FQDN, or any) that is used for the VPN tunnel on the VPN client.

When you configure the settings on the router, the remote identifier refers to the settings for the VPN client.

- Set the pool of LAN IP addresses on the router from which the router assigns an IP address to the VPN client.
- Set the DNS servers that the VPN client must use.

**ⓘ NOTE:** You can add a single client-to-site IPSec VPN connection only. However, you can use this connection configuration for multiple VPN clients. After you add a client-to-site IPSec VPN connection, the Add button no longer displays in the device UI.

The device UI uses the following icons:



### To add a client-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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Client-to-Site**.

The Client-to-Site page displays.

5. Click the **Add** button.

The Add/Edit a New Tunnel pop-up window displays and shows the basic settings.

6. To enable the VPN connection after you click the Apply button, keep the **Enable Connection** toggle blue and positioned to the right (the default setting).  
If you do not want the VPN connection to be enabled, click the **Enable Connection** toggle so that it is gray and positioned to the left. However, if disabled, the VPN client cannot initiate a VPN tunnel.
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 IPSec VPN profiles for client-to-site VPN connections](#) on page 220 or [Add a custom IPSec VPN profile](#) on page 221.
9. From the **Authentication Method** menu, select the **EAP-MSCHAPv2** or **PSK** method and the associated server certificate or pre-shared key:
  - **EAP-MSCHAPv2**: From the **Server Certificate** menu, select a certificate. If you did not yet add a certificate, see [Certificates](#) on page 271.
  - **PSK**: In the **Pre-Shared Key** field, type an authentication key that a user must type on the VPN client during the authentication process.
10. From the **Local Identifier** menu, select **IP Address**, **Local WAN IP**, or **Local FQDN**, and type either the IP address or domain name of the router:
  - **IP Address**: Type the router's IP address.
  - **Local WAN IP**: The local WAN IP address is detected by the router.
  - **Local FQDN**: Type any unique name, numbers, or a combination of both. This can be the FQDN for the WAN IP address that the router is using, but does not need to be the FQDN.
11. From the **Remote Identifier** menu, select **Remote WAN IP**, **Remote FQDN**, or **ANY**, and type either the IP address or domain name of the VPN client:
  - **Remote WAN IP**: Type the remote VPN client's WAN IP address.
  - **Remote FQDN**: Type any unique name, numbers, or a combination of both. This can be the FQDN for the WAN IP address that the VPN client is using, but does not need to be the FQDN.
  - **ANY**: The VPN client's WAN IP address or FQDN is used or the remote identifier is ignored. That is, if the VPN client does not have a remote identifier, that is also accepted.
12. In the IP Address Range for VPN Clients section, in the **Start IP Address** field and **End IP Address** field, type the IP addresses that make up the LAN IP address range on the router from which VPN clients are assigned an IP address for the VPN tunnel.

❗ **NOTE:** Be sure that the range of IP addresses for the pool does not overlap with any WAN, VLAN, or other VPN IP address subnets that are already in use in the network.

13. In the DNS Servers section, select a radio button to set the DNS servers that the VPN client must use:

- **Auto:** The primary DNS server is automatically detected. Type the IP address for the secondary DNS server in the **Secondary DNS Server** field.
- **Custom:** In the **Primary DNS Server** field and **Secondary DNS Server** field, type the IP addresses for the primary and secondary DNS servers.

14. Click the **Apply** button.

Your settings are saved. The VPN connection is added to the table on the Client-to-Site page.

## Configure client isolation, a split tunnel, and DPD options for a client-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.

You can set up the following optional features that apply to the client-to-site VPN connection:

- **Client isolation:** You can either allow or disallow communication between VPN clients that are connected to the router. By default, communication is disallowed.
- **Split tunnel:** A split tunnel lets sensitive data be transferred over the VPN tunnel but other data over a second Internet connection. Compared to a regular VPN tunnel, a split tunnel can offer a faster speed, but it can also be less secure. A split VPN tunnel allows you to manage bandwidth by reserving the full VPN tunnel for specific IP addresses only:
  - **Full VPN tunnel:** Sends all of the client's traffic across the VPN tunnel. This is the default setting.

For example, if you work from home and log in over a VPN connection to your company, all traffic goes over the company intranet. For example, if you access

social media or streaming media, your company might disallow such traffic, depending on their network policy.

- **Split VPN tunnel:** Sends only traffic for specific IP addresses (for example, for a specific server or service) over the VPN tunnel. You define the IP addresses as described in the following procedure. All other traffic is sent over the Internet.

For example, if you work from home and log in over a VPN connection to your company, only select traffic goes over the company intranet. Social media or streaming media traffic does not go over the company intranet and is not subject to the network policy of your company.

- **Dead Peer Detection:** Dead Peer Detection (DPD) is a mechanism that can prevent a VPN tunnel from being disconnected when traffic is idle. In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use DPD to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason. For DPD to function, the peer VPN device on the other end of the tunnel also needs to support DPD.

The device UI uses the following icons:

 Add  Add from existing VLAN  Edit  Delete

### To set up a split tunnel, split DNS, and DPD options for a client-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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Client-to-Site**.

The Client-to-Site page displays.

5. In the table, select the check box for the client-to-site IPSec VPN connection, and click the **Edit** button.

The Add/Edit a New Tunnel pop-up window displays and shows the basic settings.

6. Select the **Advanced Settings** tab.

Add/Edit a New Tunnel pop-up window adjusts and shows the advanced settings.

7. Click the **Client Isolation** toggle to allow or disallow communication between VPN clients that are connected to the router:

- **Allow Client Isolation:** Click the **Client Isolation** toggle so that it is gray and positioned to the left.
- **Disallow Client Isolation:** Click the **Client Isolation** toggle so that it is blue and positioned to the right (the default setting).

8. To configure a split tunnel, in the Split Tunnel section, do the following:

- a. Enable the split tunnel:

By default, the **Split Tunnel** toggle is gray and positioned to the left, which means that the split tunnel option is disabled. To enable the split tunnel option and configure the split tunnel settings, click the **Split Tunnel** toggle so that the toggle is blue and positioned to the right.

- b. Set an IP address and netmask (for example, for a server or service) for a split tunnel:

You can either manually enter the IP address and subnet mask that must be sent over the split tunnel or import the IP address and subnet mask from an existing VLAN that is already defined (see [Add a VLAN profile](#) on page 89):

- **Manually enter the IP address and netmask:** Click the **Add** button, and type the IP address and subnet mask in the **IP Address** and **Netmask** fields.
  - **Add the IP address and netmask form the VLAN:** Click the **Add from existing VLAN** button, select the check box for the VLAN, and click the **Apply** button.
- c. Optionally, add another IP address and subnet mask for traffic that must also be sent over the split tunnel.

Traffic to each IP address and subnet mask that you define is sent over the split tunnel. Other traffic is not.

9. To configure DPD, in the DPD Options section, do the following:

- a. Make sure that the DPD options are enabled:

By default, the **Enable DPD Option** toggle is blue and positioned to the right, which means that dead peer detection (DPD) is enabled. If the DPD is disabled, the **Enable DPD Option** toggle is gray and positioned to the left.

- b. Set the DPD delay period:

In the **DPD Delay** field, type the period in seconds between consecutive DPD messages. The default is 10 seconds. The period can be between 10 and 300 seconds.

- c. Set the DPD detection time:

In the **Detection Time** field, type the period in seconds during which the client must receive a DPD response from the remote VPN router. If this period is exceeded, the VPN tunnel is torn down and the client attempts to reestablish it.

The default is 30 seconds. The period can be between 30 and 1800 seconds.

If the router detects a connection failure with the remote VPN router, it tears down the VPN tunnel and attempts to reestablish it.

10. Click the **Apply** button.

Your settings are saved.

## Display the client-to-site VPN configurations

You can display the client-to-site VPN configurations.

### To display the client-to-site VPN configurations:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Client-to-Site**.

The Client-to-Site page displays.

The table displays the following information for each site-to-site VPN configuration:

- **Tunnel Name:** The name for the client-to-site configuration.
- **Authentication Method:** The authentication method for the connection between the client and the remote VPN router.
- **Local Identifier:** The LAN IP address or domain name of the client.
- **Remote Identifier:** The LAN IP address or domain name of the remote VPN router.
- **Client IP Range:** The IP address range from which the remote VPN router assigns a tunnel IP address to the client.
- **DNS Servers:** The IP addresses of the DNS servers that the client uses for the tunnel traffic.
- **Enabled:** Displays if the client-to-site configured is enabled or disabled. For more information, see [Enable or disable a client-to-site IPSec VPN connection](#) on page 247.

## Enable or disable a client-to-site IPSec VPN connection

You can enable or disable a client-to-site IPSec VPN connection. If disabled, the client cannot initiate a VPN tunnel.

### To enable or disable 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 32.
3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Client-to-Site**.

The Client-to-Site page displays.

5. In the table, select the check box for the client-to-site IPSec VPN connection.
6. Click the **Edit** button.

The Add/Edit a New Tunnel page displays.

7. Click the **Enable Connection** toggle to enable or disable the VPN connection:
  - **Enable the VPN connection:** Click the **Enable Connection** toggle so that it is blue and positioned to the right.
  - **Disable the VPN connection:** Click the **Enable Connection** toggle so that it is gray and positioned to the left.
8. Click the **Apply** button.

Your settings are saved.

## Change a client-to-site VPN connection

You can change a client-to-site VPN connection.

**ⓘ NOTE:** If you change a client-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 client-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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Client-to-Site**.

The Client-to-Site page displays.

5. In the table, select the check box for the client-to-site IPSec VPN connection, and click the **Edit** button.

The Add/Edit a New Tunnel pop-up window displays and shows the basic settings.

6. Change the settings for the connection.

For more information about the settings, see [Add a client-to-site IPSec VPN connection](#) on page 240.

7. Click the **Apply** button.

Your settings are saved. The modified connection displays in the table.

## Remove a client-to-site VPN connection

If you no longer need a client-to-site VPN connection, you can remove it.

The device UI uses the following icons:

 Add  Edit  Delete

### To remove a client-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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Client-to-Site**.

The Client-to-Site page displays.

5. In the table, select the check box for the client-to-site IPSec VPN connection.

6. Click the **Delete** icon.

A pop-up window displays.

7. Click the **OK** button.

Your settings are saved. The connection is removed from the table.

## Client-to-site VPN tunnel examples

The following sections provides examples of client-to-site VPN tunnels.

## Client-to-site VPN tunnel with the router directly connected to the Internet through a modem

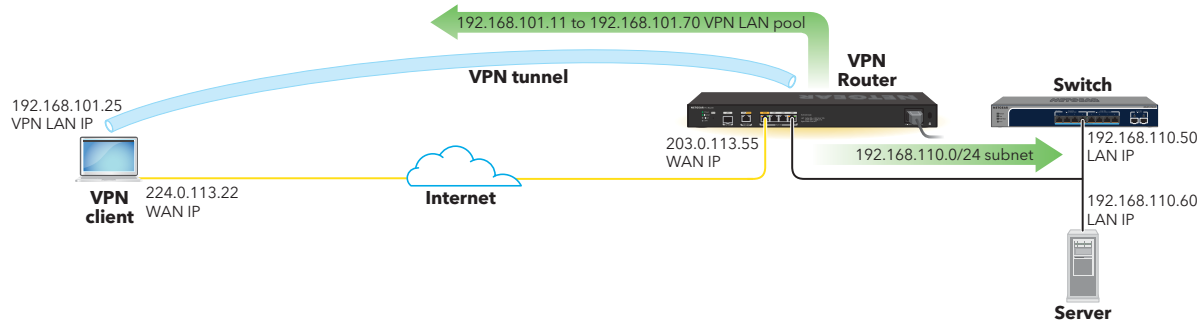


Figure 4. Client-to-site VPN tunnel with the router directly connected to the Internet through a modem

Consider the following client-to-site VPN scenario in which the router (the VPN router in the description below) is directly connected to the Internet through a modem:

- **VPN client (the local computer, tablet, or smartphone):**

- For authentication with the VPN router, the VPN client uses either the certificate authority (CA) that is associated with the server certificate on the VPN router or a pre-shared key that is identical to the one on the VPN router.
- After initial authentication with the VPN router, the VPN client identifies itself through the user name and password that is configured on the VPN router.
- As the local identifier, the VPN client uses WAN IP address 224.0.113.22.

- **Remote VPN router to which the VPN client connects:**

- As a remote identifier, the VPN router has WAN IP address 203.0.113.55.

**NOTE:** You can use the public IP address 203.0.113.55 in a server certificate as both the common name (CN) and the Subject Alternative Name (SAN).

- The VPN router issues IP addresses in the 192.168.110.0/24 subnet to devices that are located behind it, such as the switch at LAN IP address 192.168.110.50 and the server at LAN IP address 192.168.110.60.
- Depending on the configured authentication method, for authentication with the VPN client, the VPN router uses either a server certificate that is based on the same certificate authority that is installed on the VPN client or a pre-shared key that is identical to the one on the VPN client.
- As the pool range for the VPN client LAN, the VPN router assigns VPN clients a VPN LAN IP address in the range from 192.168.101.11 to 192.168.101.70. This pool range is a unique VPN pool range in a different subnet than the 192.168.110.0/24 subnet of the LAN.

**Results:**

In this VPN configuration, after the VPN tunnel is up, the following applies to the VPN client, depending on any additional security settings for individual devices and VLANs:

- The VPN client is connected to the VPN router at WAN IP address 203.0.113.55.
- The VPN client receives VPN LAN IP address 192.168.101.25 from the VPN router, which is in the VPN LAN IP address range of 192.168.101.11 to 192.168.101.70.
- Depending on your security settings, the VPN client can access devices in the LAN with subnet 192.168.110.0/24 behind the VPN router, including the switch at IP address 192.168.110.50 (and including any devices behind the switch) and the server at IP address 192.168.110.60.

## Client-to-site VPN tunnel with the router behind another router

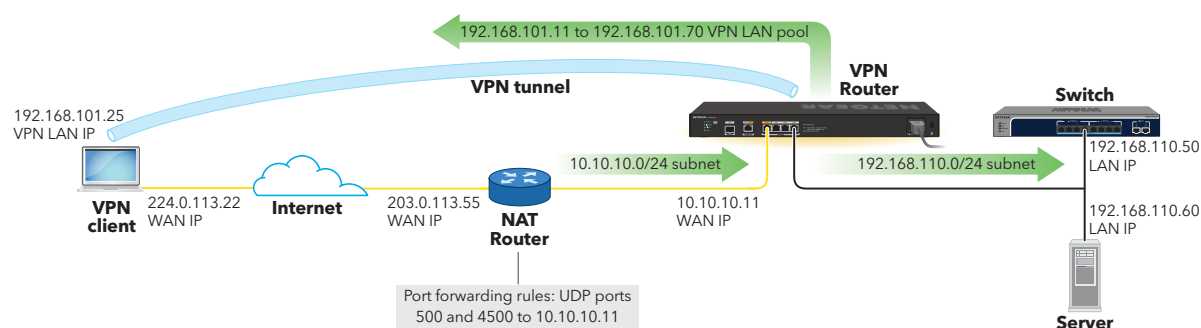


Figure 5. Client-to-site VPN tunnel with the router behind another router

Consider the following common client-to-site VPN scenario in which the router (the VPN router in the description below) is located behind another router that performs network address translation (NAT) :

- **VPN client (the local computer, tablet, or smartphone):**
  - For authentication with the VPN router, the VPN client uses either the certificate authority (CA) that is associated with the server certificate on the VPN router or a pre-shared key that is identical to the one on the VPN router.
  - After initial authentication with the VPN router, the VPN client identifies itself through the user name and password that is configured on the VPN router.
  - As the local identifier, the VPN client uses WAN IP address 224.0.113.22.
- **Remote NAT router to which the VPN client connects:**
  - As a remote identifier for the VPN configuration, the remote NAT router has WAN IP address 203.0.113.55.

**ⓘ NOTE:** You can use the public IP address 203.0.113.55 in a server certificate as both the common name (CN) and the Subject Alternative Name (SAN).

- The NAT router issues IP addresses in the 10.10.10.0/24 subnet to devices that are located in the LAN behind it.
- The NAT router includes a port forwarding rule that uses protocol UDP and port 500 to forward IKE service traffic to the VPN router with IP address 10.10.10.11.
- The NAT router includes another port forwarding rule that uses protocol UDP and port 4500 to forward NAT-Traversal (NAT-T) service traffic to the VPN router with IP address 10.10.10.11.
- **VPN router behind the NAT router:**
  - The IP address of the VPN router is 10.10.10.11, which is in the subnet that the NAT router has reserved for devices that are located behind it.
  - The VPN router, in turn, issues IP addresses in the 192.168.110.0/24 subnet to devices that are located in the LAN behind it, such as the switch at LAN IP address 192.168.110.50 and the server at LAN IP address 192.168.110.60.
  - Depending on the configured authentication method, for authentication with the VPN client, the VPN router uses either a server certificate that is based on the same certificate authority that is installed on the VPN client or a pre-shared key that is identical to the one on the VPN client.
  - As the pool range for the VPN client LAN, the VPN router assigns VPN clients a VPN LAN IP address in the range from 192.168.101.11 to 192.168.101.70. This pool range is a unique VPN pool range in a different subnet than the 192.168.110.0/24 subnet of the LAN.

### Results:

In this VPN configuration, after the VPN tunnel is up, the following applies to the VPN client, depending on any additional security settings for individual devices and VLANs:

- The VPN client is connected to the NAT router at WAN IP address 203.0.113.55.
- The NAT router forwards VPN traffic to the VPN router at WAN IP address 10.10.10.11.
- The VPN client receives VPN LAN IP address 192.168.101.25 from the VPN router, which is in the VPN LAN IP address range of 192.168.101.11 to 192.168.101.70.
- Depending on your security settings, the VPN client can access devices in the LAN with subnet 192.168.110.0/24 behind the VPN router, including the switch at IP address 192.168.110.50 (and including any devices behind the switch) and the server at IP address 192.168.110.60.

# Client-to-site OpenVPN settings

The router supports OpenVPN software, which uses the Secure Socket Layer (SSL) encryption protocol and is available free of charge to users who want to install the software on their VPN clients.

To set up a client-to-site OpenVPN tunnel, remote users must install the OpenVPN utility on their computer or OpenVPN Connect app on their mobile device.

The client-to-site OpenVPN settings on the router determine the WAN IP address at which the VPN client can reach the router and other settings for the OpenVPN connection.

OpenVPN requires a static IP address or DDNS service on the router (see [Dynamic DNS](#) on page 61) to enable a remote client such as a computer or mobile device to connect with the router.

If the router uses a static WAN IP address that never changes, OpenVPN can use that IP address to connect to the network over a VPN connection.

If the router does not use a static WAN IP address, you can use a DDNS service for the router and register for an account with a host name (also referred to as a domain name). A remote client such as a computer or mobile device can use that host name to connect with the router and access the network over a VPN connection. For more information, see [Dynamic DNS](#) on page 61.

## Enable and configure OpenVPN on the router

**❗ NOTE:** Some knowledge of OpenVPN tunnels can make it easier for you to set up a functioning OpenVPN connection.

When you add an OpenVPN tunnel connection, you must do the following, as described in the procedure that follows this list:

- Set the VPN server address, which is the WAN IP address or FQDN at which an OpenVPN client can reach the router.
- Set the protocol (UDP or TCP), port number, and service mode (TUN or TAP) for the OpenVPN connection.
- Select a server certificate, which you must have imported or created (see [Certificates](#) on page 271).

- Set the pool of LAN IP addresses on the router from which the router assigns an IP address to the OpenVPN client.
- Set the DNS servers that the OpenVPN client must use.

**❗ NOTE:** You can add a single client-to-site OpenVPN connection only. However, you can use this connection configuration for multiple OpenVPN clients.

You must enable OpenVPN and configure the OpenVPN service settings on the router before any VPN client can make an OpenVPN connection to the router.

**❗ NOTE:** Make sure that remote clients install their VPN client configuration file (also referred to as a profile) after you configure OpenVPN on the router. If you make changes to the OpenVPN configuration on the router, the VPN client configuration file that the remote clients use might change, requiring the remote clients to download and install the new VPN client configuration file.

## Enable and configure OpenVPN with TUN mode on the router

TUN mode is based on a layer 3 IP tunnel (TUN), carries IP packets through an OpenVPN tunnel, and is the default service mode for OpenVPN connections. The IP address range that you assign to VPN clients cannot overlap with any WAN, VLAN, or other IP address subnets that are already in use in the network.

### To enable and configure OpenVPN with TUN mode on 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > OpenVPN**.

The OpenVPN page displays. By default, the Basic Settings tab is selected.

5. Click the **Enable Connection** toggle to enable OpenVPN so that it is blue and positioned to the right.

You must enable OpenVPN so that you can configure the settings. By default, OpenVPN is disabled and the toggle is gray and positioned to the left.

6. In the **Connection Name** field, type a name.

The name is for identification purposes.

7. In the **Server Address** field, type the IP address or hostname to which the VPN client must connect.

8. From the **Protocol** menu, select the protocol that the VPN connection must use:

- **UDP**: This is the default protocol for OpenVPN connections.
- **TCP**: Select this protocol if clients experience difficulties with traffic over UDP. Some types of traffic might require TCP.

9. In the **Port** field, type the port number.

The OpenVPN default port number for UDP or TCP is 1194. The port number can be in the range from 1024 to 65535.

10. From the **Server Certificate** menu, select a server certificate.

If you did not yet create or import a server certificate for use with the OpenVPN connection, see [Certificates](#) on page 271. To create a server certificate, you first must create or import a certificate authority (CA) on which you can base the server certificate.

11. From the **Service Mode Type** menu, select **TUN** as the service mode for OpenVPN.

12. In the IP Address Range for VPN Clients section, in the **IP Address** field and **Netmask** field, specify the IP subnet on the router from which VPN clients are assigned an IP address for the VPN tunnel.

**ⓘ NOTE:** Be sure that the range of IP address range does not overlap with any WAN, VLAN, or other VPN IP address subnets that are already in use in the network.

13. In the DNS Servers section, select a radio button to set the DNS servers that the VPN client must use:

- **Auto:** The primary and secondary DNS servers are automatically detected.
- **Custom:** In the **DNS 1** field and **DNS 2** field, type the IP addresses for the primary and secondary DNS servers.

14. Click the **Apply** button.

Your settings are saved. OpenVPN service is enabled on the router.

Users must install and set up OpenVPN software and the router client configuration file on their computer or mobile device before they can establish a VPN connection to the router.

## Enable and configure OpenVPN with TAP mode on the router

TAP mode is based on a layer 2 Ethernet TAP, carries Ethernet frames through an OpenVPN tunnel, and allows you to place the OpenVPN traffic in a specific VLAN. The IP address range that you assign to VPN clients must be in the same network as the selected VLAN and cannot overlap with the DHCP IP address pool for that VLAN.

**ⓘ NOTE:** iOS and Android devices do not support OpenVPN connections with the TAP mode. For these devices, use TUN mode (see [Enable and configure OpenVPN with TUN mode on the router](#) on page 255).

### To enable and configure OpenVPN with TAP mode on 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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > OpenVPN**.

The OpenVPN page displays. By default, the Basic Settings tab is selected.

5. Click the **Enable Connection** toggle to enable OpenVPN so that it is blue and positioned to the right.

You must enable OpenVPN so that you can configure the settings. By default, OpenVPN is disabled and the toggle is gray and positioned to the left.

6. In the **Connection Name** field, type a name.

The name is for identification purposes.

7. In the **Server Address** field, type the IP address or hostname to which the VPN client must connect.

8. From the **Protocol** menu, select the protocol that the VPN connection must use:

- **UDP**: This is the default protocol for OpenVPN connections.
- **TCP**: Select this protocol if clients experience difficulties with traffic over UDP. Some types of traffic might require TCP.

9. In the **Port** field, type the port number.

The OpenVPN default port number for UDP or TCP is 1194. The port number can be in the range from 1024 to 65535.

10. From the **Server Certificate** menu, select a server certificate.

If you did not yet create or import a server certificate for use with the OpenVPN connection, see [Certificates](#) on page 271. To create a server certificate, you first must create or import a certificate authority (CA) on which you can base the server certificate.

11. From the **Service Mode Type** menu, select **TAP** as the service mode for OpenVPN.

12. From the **VLAN** menu, select the VLAN in which the OpenVPN traffic must be placed.

13. In the IP Address Range for VPN Clients section, in the **Start IP Address** field and **End IP Address** field, type the IP addresses that make up the LAN IP address range on the router from which VPN clients are assigned an IP address for the VPN tunnel.

**! NOTE:** The IP address range that you assign to the VPN clients must be in the same network as the selected VLAN and cannot overlap with the DHCP IP address pool for that VLAN.

14. Click the **Apply** button.

Your settings are saved. OpenVPN service is enabled on the router.

Users must install and set up OpenVPN software and the router client configuration file on their computer or mobile device before they can establish a VPN connection to the router.

## Configure duplicate connections, client isolation, a domain name, and a split tunnel for a client-to-site OpenVPN connection

**! NOTE:** Some knowledge of OpenVPN tunnels can make it easier for you to set up a functioning OpenVPN connection.

You can set up the following optional features that apply to the OpenVPN connection:



- **Duplicate Connection:** You can let a single OpenVPN user establish more than one VPN tunnel. If you enable this feature, a single VPN user can establish up to three VPN tunnels, depending on the connection limit that you set.
- **Client isolation:** You can either allow or disallow communication between VPN clients that are connected to the router. By default, communication is disallowed.
- **Domain Name:** The fully qualified domain name (FQDN) for the domain that the VPN clients join after establishing the VPN tunnel.

**! NOTE:** A domain name is an option for the TUN service mode only.

- **Split tunnel:** A split tunnel lets sensitive data be transferred over the VPN tunnel but other data over a second Internet connection. Compared to a regular VPN tunnel, a split tunnel can offer a faster speed, but it can also be less secure. A split VPN tunnel allows you to manage bandwidth by reserving the full VPN tunnel for specific IP addresses only:
  - **Full VPN tunnel:** Sends all of the client's traffic across the VPN tunnel. This is the default setting.  
For example, if you work from home and log in over a VPN connection to your company, all traffic goes over the company intranet. For example, if you access social media or streaming media, your company might disallow such traffic, depending on their network policy.
  - **Split VPN tunnel:** Sends only traffic for specific IP addresses (for example, for a specific server or service) over the VPN tunnel. You define the IP addresses as described in the following procedure. All other traffic is sent over the Internet.  
For example, if you work from home and log in over a VPN connection to your company, only select traffic goes over the company intranet. Social media or

streaming media traffic does not go over the over the company intranet and is not subject to the network policy of your company.

The device UI uses the following icons:

 Add  Add from existing VLAN  Edit  Delete

**To set up duplicate connections, client isolation, a domain name, and split tunnel options for an OpenVPN 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > OpenVPN**.

The OpenVPN page displays. By default, the Basic Settings tab is selected.

5. Select the **Advanced Settings** tab.

The page adjusts and shows the advanced settings.

6. To enable more than one VPN tunnel from a single VPN user, do the following:

- a. Click the **Duplicate connection** toggle so that it is blue and positioned to the right.

By default, this feature is disabled and the **Duplicate connection** toggle is gray and positioned to the left.

- b. In the **Duplicate Connection Limit** field, type the number of simultaneous VPN tunnels that are allowed from the same VPN user.

By default, three simultaneous VPN tunnels are allowed, but you can also allow only one or two.

7. Click the **Client Isolation** toggle to allow or disallow communication between VPN clients that are connected to the router:
  - **Allow Client Isolation:** Click the **Client Isolation** toggle so that it is gray and positioned to the left.
  - **Disallow Client Isolation:** Click the **Client Isolation** toggle so that it is blue and positioned to the right (the default setting).
8. As an option for the TUN service mode only, in the **Domain Name** field, type the fully qualified domain name (FQDN) for the domain that the VPN clients join after establishing the VPN tunnel.
9. To configure a split tunnel, in the Split Tunnel section, do the following:
  - a. Enable the split tunnel:
 

By default, the **Split Tunnel** toggle is gray and positioned to the left, which means that the split tunnel option is disabled. To enable the split tunnel option and configure the split tunnel settings, click the **Split Tunnel** toggle so that the toggle is blue and positioned to the right.
  - b. Set an IP address and subnet mask (for example, for a server or service) for a split tunnel:
 

You can either manually enter the IP address and subnet mask that must be sent over the split tunnel or import the IP address and subnet mask from an existing VLAN that is already defined (see [Add a VLAN profile](#) on page 89):

    - **Manually enter the IP address and netmask:** Click the **Add** icon, and type the IP address and subnet mask in the **IP Address** and **Netmask** fields.
    - **Add the IP address and netmask from the VLAN:** Click the **Add from existing VLAN** icon, select the check box for the VLAN, and click the **Apply** button.
  - c. Optionally, add another IP address and subnet mask for traffic that must also be sent over the split tunnel.
  - d. To make a change to an existing split tunnel configuration, select the associated check box, and click the **Edit** icon.
  - e. To remove an existing split tunnel configuration, select the associated check box, and click the **Delete** icon.

Traffic to each IP address and netmask that you define is sent over the split tunnel. Other traffic is not.
10. Click the **Apply** button.
 

Your settings are saved.

# Export the router's OpenVPN client configuration file

You can export the router's OpenVPN client configuration file (also referred to as a profile) to a computer or storage device that is connected to the router, and then forward the client configuration file to a VPN client that you want to allow to set up OpenVPN connectivity to the router.

## To export the router's OpenVPN client configuration file:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > OpenVPN**.

The OpenVPN page displays. By default, the Basic Settings tab is selected.

5. Next to Export Client Configuration, click the **Download** link.

Depending on the browser that you are using, a pop-up window might display.

6. Navigate to a location on the connected computer or storage device, and save the client configuration file.
7. Send the client configuration file (or make it available through a URL) to each user that must be able to use an OpenVPN connection to connect to the router.

# Install OpenVPN client software and the VPN router client configuration file on a remote client

To establish a VPN connection to the router using OpenVPN software, a remote user must install OpenVPN client software on their Windows-based or Mac computer or the OpenVPN Connect app on their Android or iOS mobile device.

For a Windows-based computer and a Mac computer, either download the client for TUN mode or TAP mode, depending on the mode that is configured on the router. This information is typically provided by an administrator. An Android or iOS device supports TUN mode only.

In addition, a remote user must install the client configuration file that is generated on the router to which the OpenVPN client must connect. (This file is also referred to as the client connection profile.) Typically, this file is provided by an administrator or is available from a URL on a company website.

A remote must also get their user name and password for the OpenVPN connection from a network administrator.

## Install the OpenVPN client utility and configuration file for TUN mode on a Windows-based computer

### **To download and install the OpenVPN client utility and VPN router's client configuration file for TUN mode on a Windows-based computer:**

1. Visit [openvpn.net/client/](https://openvpn.net/client/), download the OpenVPN client utility for a Windows-based computer, and install it on the Windows-based computer.

You might need administrative privileges to install the OpenVPN client utility.

2. Get the VPN router's client configuration file (also referred to as a profile).

The client configuration file is an `.ovpn` file that is generated on the router to which the OpenVPN client must connect. Typically, this `.ovpn` file is provided by an administrator or is available from a URL on a company website.

3. On the Windows-based computer, start the OpenVPN client utility, and search for and import the `.ovpn` file.
4. Get your user name and password for the OpenVPN connection.

Typically, this information is provided by a network administrator.

The computer is now ready to for you to set up a VPN connection to the router.

For more information about using OpenVPN on a Windows-based computer, visit [openvpn.net/client/client-connect-vpn-for-windows](https://openvpn.net/client/client-connect-vpn-for-windows).

## Install the OpenVPN client utility and configuration file for TAP mode on a Windows-based computer

### **To download and install the OpenVPN client utility and VPN router's client configuration file for TAP mode on a Windows-based computer:**

1. Visit [community.openvpn.net/openvpn/wiki/Downloads](https://community.openvpn.net/openvpn/wiki/Downloads), download the OpenVPN client utility for TAP mode for a Windows-based computer, and install it on the Windows-based computer.

You might need administrative privileges to install the OpenVPN client utility.

2. Get the VPN router's client configuration file (also referred to as a profile).

The client configuration file is an `.ovpn` file that is generated on the router to which the OpenVPN client must connect. Typically, this `.ovpn` file is provided by an administrator or is available from a URL on a company website.

3. On the Windows-based computer, start the OpenVPN client utility, and search for and import the `.ovpn` file.

4. Get your user name and password for the OpenVPN connection.

Typically, this information is provided by a network administrator.

The computer is now ready to for you to set up a VPN connection to the router.

## Install the OpenVPN client utility and configuration file for TUN mode on a Mac

### **To download and install the OpenVPN client utility and VPN router's client configuration file for TUN mode on a Mac:**

1. Visit [openvpn.net/client/](https://openvpn.net/client/), download the OpenVPN client utility for a Mac, and install it on the Mac.

You might need administrative privileges to install the OpenVPN client utility.

2. Get the VPN router's client configuration file (also referred to as a profile).

The client configuration file is an `.ovpn` file that is generated on the router to which the OpenVPN client must connect. Typically, this `.ovpn` file is provided by an administrator or is available from a URL on a company website.

3. On the Mac, start the OpenVPN client utility, and search for and import the `.ovpn` file.

4. Get your user name and password for the OpenVPN connection.

Typically, this information is provided by a network administrator.

The Mac is now ready to for you to set up a VPN connection to the router.

For more information about using OpenVPN on a Mac computer, visit [openvpn.net/client-connect-vpn-for-mac-os](https://openvpn.net/client-connect-vpn-for-mac-os).

## Install the OpenVPN client utility and configuration file for TAP mode on a Mac

### **To download and install the OpenVPN client utility and VPN router's client configuration file for TAP mode on a Mac:**

1. Visit [tunnelblick.net/downloads.html](https://tunnelblick.net/downloads.html), download the OpenVPN client utility for a Mac, and install it on the Mac.

You might need administrative privileges to install the OpenVPN client utility.

2. Get the VPN router's client configuration file (also referred to as a profile).

The client configuration file is an `.ovpn` file that is generated on the router to which the OpenVPN client must connect. Typically, this `.ovpn` file is provided by an administrator or is available from a URL on a company website.

3. On the Mac, start the OpenVPN client utility, and search for and import the `.ovpn` file.

4. Get your user name and password for the OpenVPN connection.

Typically, this information is provided by a network administrator.

The Mac is now ready to for you to set up a VPN connection to the router.

For more information about using OpenVPN on a Mac computer, visit [tunnelblick.net/index.htm](https://tunnelblick.net/index.htm).

## Install the OpenVPN Connect app and client configuration file for TUN mode on an Android device

An Android device can support TUN mode only.

### **To download and install the OpenVPN Connect app and VPN router's client configuration file for TUN mode on an Android device:**

1. On your Android device, visit the Google Play Store and download and install the OpenVPN Connect app.
2. Get the VPN router's client configuration file (also referred to as a profile).

The client configuration file is an `.ovpn` file that is generated on the router to which the OpenVPN client must connect. Typically, this `.ovpn` file is provided by an administrator or is available from a URL on a company website.

3. On your Android device, start the OpenVPN Connect app, and search for and import the `.ovpn` file.

4. Get your user name and password for the OpenVPN connection.

Typically, this information is provided by a network administrator.

The Android device is now ready to for you to set up a VPN connection to the router.

For more information about using OpenVPN on an Android device, visit [openvpn.net/client/](https://openvpn.net/client/).

## Install the OpenVPN Connect app and client configuration file for TUN mode on an iOS device

An iOS device can support TUN mode only.

### **To download and install the OpenVPN Connect app and VPN router's client configuration file for TUN mode on an iOS device:**

1. On your iOS device, visit the Apple app store and download and install the OpenVPN Connect app.

2. Get the VPN router's client configuration file (also referred to as a profile).

The client configuration file is an `.ovpn` file that is generated on the router to which the OpenVPN client must connect. Typically, this `.ovpn` file is provided by an administrator or is available from a URL on a company website.

3. On your iOS device, open the `.ovpn` file, select the OpenVPN Connect app, and import the `.ovpn` file.

4. Get your user name and password for the OpenVPN connection.

Typically, this information is provided by a network administrator.

The iOS device is now ready to for you to set up a VPN connection to the router.

For more information about using OpenVPN on an iOS device, visit [openvpn.net/client/](https://openvpn.net/client/).

## VPN user accounts

For each user who must be able to connect over a VPN tunnel to the router, whether over IPSec VPN or OpenVPN, you must set up user a VPN user account and communicate the associated user name and password to the user.

A user account can be used only on one client device at any time. If you use the same user account on a second device at the same time, the first device is disconnected.

# Add a VPN user account

Adding a VPN user account consists of adding a user name and password that a user must enter when they want to establish a VPN tunnel. For added security, you can set user access control, which limits the user account to one or more VLAN interfaces, one or more custom IP addresses and subnet masks, or a combination of these.

The device UI uses the following icons:



## To add a VPN user account:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > VPN Users**.

The VPN Users page displays.

5. Click the **Add** icon.

The Add/Edit VPN User pop-up window displays.

6. In the **User Name** field, type a name.

The name is for identification purposes.

7. In the **Password** field, type a password.

The password must be between 8 and 64 characters and cannot contain spaces.

8. To enable the VPN user account after you click the Add button, keep the **Enable** toggle blue and positioned to the right (the default setting).

If you want the VPN user account to be disabled, click the **Enable** toggle so that it is gray and positioned to the left.

9. To set access control, which lets you limit the user account to one or more VLAN interfaces, one or more custom IP addresses and subnet masks, or a combination of these, click the **Enable Access Control** toggle so that it is blue and positioned to the right.

By default, access control is disabled for the user account, and the toggle is gray and positioned to the left.

Do the following:

- a. Add a VLAN interface or custom IP address and subnet mask:
  - **Limit access to a VLAN interface:** From the **Interface name** menu, select a VLAN interface. The IP address and subnet mask are automatically entered.
  - **Limit access to a custom IP address and mask:** From the **Interface name** menu, select **Custom**, and then enter an IP address in the **IP Address** field and a subnet mask in the **Subnet Mask** field.
- b. To add another VLAN interface or custom IP address and subnet mask, click the **Add** icon and repeat the previous substep.

10. Click the **Add** button.

Your settings are saved. The VPN user account is added to the VPN Users table.

## Change a VPN user account

You can change the user name, password, and access control for a VPN user account, and you can enable or disable a VPN user account.

The device UI uses the following icons:

 Add  Edit  Delete

### To change a VPN user account:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > VPN Users**.

The VPN Users page displays..

5. Select the check box for the user account.

6. Click the **Edit** icon.

The Add/Edit VPN User pop-up window displays.

7. To change the user name, in the **User Name** field, type a name.

The name is for identification purposes.

8. To change the password, in the **Password** field, type a password.

The password must be between 8 and 64 characters and cannot contain spaces.

9. To enable or disable the VPN user account, click the **Enable** toggle:

- **The toggle is blue and positioned to the right:** The VPN user account is enabled.
- **The toggle is gray and positioned to the left:** The VPN user account is disabled.

10. To enable or disable access control, click the **Enable Access Control** toggle:

- **The toggle is blue and positioned to the right:** Access control is enabled.
- **The toggle is gray and positioned to the left:** Access control is disabled.

11. If access control is enabled, do the following to make changes to the access control list:

- To change an access control entry, select the associated check box, and then click the **Edit** icon:
  - **Limit access to a VLAN interface:** From the **Interface name** menu, select a VLAN interface. The IP address and subnet mask are automatically entered.

- **Limit access to a custom IP address and mask:** From the **Interface name** menu, select **Custom**, and then enter an IP address in the **IP Address** field and a subnet mask in the **Subnet Mask** field.
- To delete an access control entry, select the associated check box, and then click the **Delete** icon

12. Click the **Add** button.

Your settings are saved. The modified settings are displayed in the VPN Users table.

## Remove a VPN user account

You can remove a VPN user account that you no longer need.

The device UI uses the following icons:



### To remove a VPN user account:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > VPN Users**.

The VPN Users page displays..

5. Select the check box for the user account.

6. Click the **Delete** icon.

A confirmation pop-up window displays.

7. Click the **Proceed** button

Your settings are saved. The user account is removed from the VPN Users table.

## Certificates

A digital server certificate, in short, a certificate, is a means of authenticating a device. A certificate is required on both the router and the VPN client if you select to use EAP-MSCHAPv2 authentication for a client-to-site IPsec VPN configuration (see [Add a client-to-site IPsec VPN connection](#) on page 240).

A certificate authority and certificate function together:

- **Certificate Authority:** A certificate authority (CA), is an organization or company that validates the identity of the person or company, or the associated website or email address, that uses the certificate.

You can also let the router create a CA, which then can be used for a self-signed server certificate that you can install on the router. Typically, you forward the CA on which the server certificate is based to the VPN client that must be able to initiate a VPN tunnel to the router.

**! NOTE:** Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed certificate might trigger a warning from most browsers because it provides no protection against identity theft of the server.

- **Server Certificate:** The router uses digital certificates to authenticate connecting VPN clients. A digital certificate that authenticates a client is a file that contains the following elements:
  - A public encryption key to be used by clients for encrypting messages to the router.
  - Information identifying the operator of the router.
  - A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

A certificate can also be self-signed, in which case its certificate authority was created by the router. A self-signed certificate can be useful in a test situation or for internal VPN traffic in a secure environment, but generally not for a production environment.

The following table illustrates the function of a certificate authority and server certificate by comparing them to the authentication that occurs when you visit a bank to withdraw money from an account.

Bank Withdrawal Authentication	VPN Tunnel Authentication
Bank (financial institution)	Certificate authority
Bank teller badge: <ul style="list-style-type: none"> <li>Employee name</li> <li>Employee ID</li> </ul>	Server certificate: <ul style="list-style-type: none"> <li>common name (CN)</li> <li>Subjective Alternative Name (SAN)</li> </ul>
Bank account	VPN user name
Bank account PIN or an identification that you provide (for example, a driver's license)	VPN user password

The router lets you do the following:

- Import a certificate (see [Import an existing server certificate](#) on page 284)
- Create a certificate based on an imported or self-generated certificate authority (see [Create a server certificate](#) on page 281)
- Import a certificate authority (see [Import an existing certificate authority](#) on page 275)
- Create a certificate authority (see [Create a certificate authority](#) on page 272)

After you have imported or created a certificate authority on the router, you must export the certificate authority (see [Export a certificate authority or private key](#) on page 277) so that you can provide them to each VPN client that intends to use EAP-MSCHAPv2 authentication to establish a VPN connection to the router. Each such VPN client must import the certificate authority. During the VPN authentication process, the certificate authority can then be checked against the associated server certificate on the router.

## Create a certificate authority

You can create a self-signed certificate authority (CA) that you then can use the add certificates, and in turn, to set up a client-to-site VPN configuration.

**ⓘ NOTE:** After you have saved the certificate authority, you cannot change it. However, you can delete it and create a new certificate authority.

The device UI uses the following icons:

 Add  Import

**To create a certificate authority:**

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. Click the **Add** icon.

The Create Certificate Authority pop-window displays.

6. In the **Descriptive Name** field, type a name.

The name is for identification purposes.

7. From the **Type** menu, select the type of self-signed CA:

- **Root CA Certificate:** A custom root certificate authority that is issued by the router and that can form the basis of an intermediate certificate authority or a server certificate.

**NOTE:** Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed certificate might trigger a warning from most browsers because it provides no protection against identity theft of the server.

- **Intermediate Certificate Authority:** An intermediate certificate authority (CA) must be based on a root CA certificate (either one that you imported or one that you created). An intermediate CA provides an additional level of security for the root CA itself because you do not need to build server certificates off the root CA but can use an intermediate CA instead.

8. In the Internal Certificate Authority section, specify the settings as described in the following table.

Name	Setting
Certificate Authority	<p>This menu display only if you select <b>Intermediate Certificate Authority</b> from the <b>Type</b> menu in the previous step.</p> <p>From the <b>Certificate Authority</b> menu, select a certificate authority that you imported or an internal root certificate authority that you created.</p>
Key Length (bits)	<p>Select one of the following key lengths in bits, each of which, in ascending order, provides more security but slower performance:</p> <ul style="list-style-type: none"> <li>• <b>1024</b></li> <li>• <b>2048</b> (The default setting.)</li> <li>• <b>4096</b></li> </ul>
Key Type	The only option is RSA (Rivest-Shamir-Adleman).
Digest Algorithm	<p>Select one of the following digest algorithms, each of which, in ascending order, provides more security but slower performance:</p> <ul style="list-style-type: none"> <li>• <b>SHA1:</b> Hash algorithm that produces a 160-bit digest. (We recommend that you use a stronger hash algorithm.)</li> <li>• <b>SHA256:</b> Hash algorithm that produces a 256-bit digest. (The default setting.)</li> <li>• <b>SHA384:</b> Hash algorithm that produces a 384-bit digest.</li> <li>• <b>SHA512:</b> Hash algorithm that produces a 512-bit digest.</li> </ul>
Lifetime (Days)	The period that the CA is active. By default, the period is 3650 days (10 years). The range is from 1 day to 3650 days.

(Continued)

Name	Setting
Common Name	The common name (CN) is the domain name that you are securing, for example, YourCompany.com. The default name is internal-ca.
Country Code	These are self-explanatory optional fields.
State or Province	
City	
Organization	
Organizational Unit	

- Click the **Apply** button.

Your settings are saved. The CA is added to the Authorities table.

For information about managing CAs, see [Manage imported and created certificate authorities](#) on page 277.

## Import an existing certificate authority

You can import an existing certificate authority (CA) that you then can use to create certificates, and in turn, to set up a client-to-site VPN configuration.

Typically, you import an existing certificate authority file and associated private key file from a computer or a storage device that is connected to your computer or directly to the router.

The device UI uses the following icons:

 Add  Import

### To import an existing certificate authority:

- Launch a web browser from a computer or mobile device that is connected to the router network.
- 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 32.

- Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities table is selected.

5. Click the **Import** icon.

The Import Certificate Authority pop-window displays.

6. In the **Certificate Name** field, type a name.

**!** **NOTE:** The only encoding option is PEM, which is the file format for Privacy Enhanced Mail.

7. Next to the **Select Certificate** menu, click the **Browse** button, and navigate to and select the CA file.
8. Next to the **Select Private Key** menu, click the **Browse** button, and navigate to and select the private key file.
9. To require a password to later export the private key file, type a password in the **Password** field.

Be sure to store the password for later use.

10. Click the **Import** button.

Your settings are saved. The CA is added to the Authorities table.

For information about managing CAs, see [Manage imported and created certificate authorities](#) on page 277.

# Manage imported and created certificate authorities

After you have imported or created one or more certificate authorities (CAs, see [Import an existing certificate authority](#) on page 275 or [Create a certificate authority](#) on page 272), you can manage these CAs by exporting them or their private keys, renewing them, or removing them.

## Export a certificate authority or private key

You can export a certificate authority (CA) file or private key file from the router to a computer or storage device that is connected to the router, and then forward the CA file or associated private key file to a VPN client that you want to allow to set up VPN connectivity to the router.

The device UI uses the following icons:

 Export
  Export Private Key
  Renew Certificate
  Delete Certificate

### To export a certificate authority or associated private key:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. To export a certificate authority file, do the following:

- a. In the Authorities table, in the Action column for the certificate authority, click the **Export** icon.

Depending on the browser that you are using, a pop-up window might display.

- b. Navigate to a location on the connected computer or storage device, and save the file.

6. To export a private key file, do the following:

- a. In the Authorities table, in the Action column for the certificate authority, click the **Export Private Key** icon.

If you set up a password when you imported the private key file (see [Import an existing certificate authority](#) on page 275), the Export Private Key pop-up window displays.

- b. If the Export Private Key pop-up window displays, type and confirm the password.

Depending on the browser that you are using, a pop-up window might display.

- c. Navigate to a location on the connected computer or storage device, and save the file.

## Display details about a certificate authority

You can display detailed information about a certificate authority (CA).

### To display detailed information about a certificate authority:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

The Authorities table displays the following information:

- **Name:** The name of the certificate authority file
- **Internal:** Whether the certificate authority is internally generated on the router.
- **Issuer:** The issuing organization, or self-signed
- **Certificates:** The number server certificates that use this certificate authority
- **Distinguished Name:** The type of certificate authority and the period that the certificate authority is valid.
- **Details:** See the following step.
- **In Use:** Whether the certificate authority is in use for an IPSec tunnel


5. To display detailed information, click the icon in the Details columns for the certificate authority.

The Certificate Detail pop-up window displays.

6. To close the pop-up window, click the **Close** button.

## Renew a certificate authority

By default, a certificate authority (CA) file is valid for about 10 years. You can renew a certificate authority so that a new period of about 10 years starts.

 **CAUTION:** If you renew a CA file, you must export the CA file (see [Export a certificate authority or private key](#) on page 277), and then make the new CA file available to all VPN users so that they can install the new CA file on their VPN client devices.

The device UI uses the following icons:



Export



Export Private Key



Renew Certificate



Delete Certificate

### To renew a certificate authority:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

The Distinguished Name column shows the dates and times from which and until which the certificate authority is valid.

5. In the Authorities table, in the Action column for the certificate authority, click the **Renew Certificate** button.

The Renew CA Certificate pop-up window displays.

6. Click the **Renew** button.

The Distinguished Name column shows the updated dates and times for the validity of the certificate authority.

## Remove a certificate authority

You can remove a certificate authority (CA) file that you no longer need. You cannot remove a certificate authority that is being used in a server certificate.

The device UI uses the following icons:

 Export
  Export Private Key
  Renew Certificate
  Delete Certificate

**To remove a certificate authority:**

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 32.
3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.  
The Certificate page displays. By default, the Authorities table is selected.
5. In the Authorities table, in the Action column for the certificate authority, click the **Delete Certificate** button.  
A confirmation pop-up window displays.
6. Click the **OK** button.  
Your settings are saved. The certificate authority is removed.

## Create a server certificate

You can create a server certificate (in short, a certificate) that is based on a certificate authority (CA) that you imported (see [Import an existing certificate authority](#) on page 275) or a CA that you created (see [Create a certificate authority](#) on page 272). You can use a certificate to set up a client-to-site VPN configuration.

**! NOTE:** After you have saved the certificate, you cannot change it. However, you can delete it and create a new certificate.

The device UI uses the following icons:



### To create a certificate:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. Select the **Certificates** tab.

The page adjusts.

6. Click the **Add** icon.

The Add/Sign a New Certificate pop-window displays.

7. In the **Descriptive Name** field, type a name.

The name is for identification purposes.

8. In the Internal Certificate section, specify the settings as described in the following table.

Name	Setting
Certificate Authority	From the <b>Certificate Authority</b> menu, select a certificate authority that you imported or added.
Key Length (bits)	<p>Select one of the following key lengths in bits, each of which, in ascending order, provides more security but slower performance:</p> <ul style="list-style-type: none"> <li>• <b>1024</b></li> <li>• <b>2048</b> (The default setting.)</li> <li>• <b>4096</b></li> </ul>
Key Type	The only option is RSA (Rivest-Shamir-Adleman).
Digest Algorithm	<p>Select one of the following digest algorithms, each of which, in ascending order, provides more security but slower performance:</p> <ul style="list-style-type: none"> <li>• <b>SHA1</b>: Hash algorithm that produces a 160-bit digest. (We recommend that you use a stronger hash algorithm.)</li> <li>• <b>SHA256</b>: Hash algorithm that produces a 256-bit digest. (The default setting.)</li> <li>• <b>SHA384</b>: Hash algorithm that produces a 384-bit digest</li> <li>• <b>SHA512</b>: Hash algorithm that produces a 512-bit digest</li> </ul>
Lifetime (Days)	<p>The period that the CA is active. By default, the period is 365 days (1 year).</p> <p>Do not set this field to more than 398 days to prevent the certificate from being considered invalid by some platforms.</p>
Common Name	The fully qualified domain name (FQDN) of the router. If the router has a static WAN IP address, you can enter the IP address.

9. In the Certificate Attributes section, specify the settings as described in the following table.

Name	Setting
Subjective Alternative Type and Subjective Alternative Name	<p>To ensure secure VPN connectivity, you must also set a Subject Alternative Name (SAN), which can be a FQDN, the static WAN IP address of the router, or the external public IP address.</p> <p>From the <b>Subjective Alternative Type</b> menu, select the type of SAN (<b>FQDN</b> or <b>IP Address</b>), and in the <b>Subjective Alternative Name</b> field, enter the name or IP address.</p> <p>You can enter multiple SANs. To manage the SANs, do the following:</p> <ul style="list-style-type: none"> <li>• To add an additional SAN, click the <b>Add</b> button, from the <b>Subjective Alternative Type</b> menu, select the type of SAN (<b>FQDN</b> or <b>IP Address</b>), and in the <b>Subjective Alternative Name</b> field, enter the name or IP address.</li> <li>• To remove a SAN, select the check box for the SAN, and click the <b>Delete</b> button.</li> </ul>
Country Code	These are self-explanatory optional fields.
State or Province	
City	
Organization	
Organizational Unit	

10. Click the **Apply** button.

Your settings are saved. The CA is added to the Authorities table.

For information about managing CAs, see [Manage imported and created certificate authorities](#) on page 277.

## Import an existing server certificate

You can import an existing server certificate (in short, a certificate) that you then can use to set up a client-to-site VPN configuration.

Typically, you import an existing certificate file and associated private key file from a computer or a storage device that is connected to your computer or directly to the router.

The device UI uses the following icons:



### To import an existing certificate:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. Select the **Certificates** tab.

The page adjusts.

6. Click the **Import** icon.

The Import Certificate pop-window displays.

7. In the **Certificate Name** field, type a name.

The name is for identification purposes.

8. Select the radio button for the type of encoding that the certificate uses and import the file or files:

- **PKCS#12**: This type of encoding includes both a certificate and a private key in a single file. Next to the **Select PKCS#12 (P12) File** menu, click the **Browse** button, and navigate to and select the P12 file.
- **PEM**: Privacy Enhanced Mail (PEM) encoding requires both a certificate file and a private key file. Do the following:
  - a. Next to the **Select Certificate** menu, click the **Browse** button, and navigate to and select the certificate file.
  - b. Next to the **Select Private Key** menu, click the **Browse** button, and navigate to and select the private key file.

9. To require a password to later export the P12 file or private key file, type a password in the **Password** field.

Be sure to store the password for later use.

10. Click the **Import** button.

Your settings are saved. The certificates is added to the Server Certificates table.

For information about managing certificates, see [Manage imported and created server certificates](#) on page 285.

## Manage imported and created server certificates

After you have imported or created one or more server certificates (see [Import an existing server certificate](#) on page 284 or [Create a server certificate](#) on page 281), you can manage these server certificates by exporting them or their private keys, renewing them, or removing them.

### Export a server certificate or private key

You can export a server certificate, in short a certificate, from the router to a computer or storage device that is connected to the router, and then forward the certificate or

associated private key file to a VPN router that you want to allow to accept VPN connections from a VPN client.

The device UI uses the following icons:

 Export  Export Private Key  Renew Certificate  Delete Certificate

### To export a certificate or associated private key:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities table is selected.

5. Select the **Certificates** tab.

The page adjusts.

6. To export a certificate file, do the following:

- a. In the Server Certificates table, in the Action column for the certificate authority, click the **Export Certificate** button.

The Export Certificate pop-up window displays.

- b. Select one of the following radio buttons:

- **PEM:** Only the certificate file is exported. A password does not apply.
- **PKCS#12:** Both the certificate and private key files are exported. If you imported the certificate file (see [Import an existing server certificate](#) on page 284), type and confirm the password.

Depending on the browser that you are using, a pop-up window might display.

- Navigate to a location on the connected computer or storage device, and save the file.
- To export a private key file, do the following:
    - In the Authorities table, in the Action column for the certificate authority, click the **Export Private Key** button.  
If you set up a password when you imported the P12 or private key file (see [Import an existing server certificate](#) on page 284), the Export Private Key pop-up window displays.
    - If the Export Private Key pop-up window displays, type and confirm the password.  
Depending on the browser that you are using, a pop-up window might display.
    - Navigate to a location on the connected computer or storage device, and save the file.

## Display details about a server certificate

You can display detailed information about a server certificate, in short, a certificate.

### To display detailed information about a certificate:

- Launch a web browser from a computer or mobile device that is connected to the router network.
- 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 32.
- Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the

router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. Select the **Certificates** tab.

The page adjusts.

The Server Certificate table displays the following information:

- **Certificate:** The name of the certificate file
- **Type:** The type of certificate is always server.
- **Issuer:** The certificate authority that is used for the certificate
- **Distinguished Name:** The Common Name (CN) name of the certificate (or the IP address that is associated with the certificate) and the period that the certificate is valid.
- **Details:** See the following step.
- **In Use:** Whether the certificate is in use for an IPSec tunnel

6. To display detailed information, click the icon in the Details columns for the certificate.

The Certificate Detail pop-up window displays.

7. To close the pop-up window, click the **Close** button.

## Renew a server certificate

By default, a server certificate, in short, a certificate, file is valid for about one year. You can renew a certificate authority so that a new period of about one year starts.

The device UI uses the following icons:

 Export  Export Private Key  Renew Certificate  Delete Certificate

### To renew a certificate:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. Select the **Certificates** tab.

The page adjusts.

The Distinguished Name column shows the dates and times from which and until which the certificate is valid.

6. In the Server Certificates table, in the Action column for the certificate, click the **Renew Certificate** button.

The Renew Server Certificate pop-up window displays.

7. Click the **Renew** button.

The Distinguished Name column shows the updated dates and times for the validity of the certificate.

## Remove a server certificate

You can remove a server certificate, in short, a certificate, that you no longer need. You cannot remove a certificate that is being used in a client-to-site VPN connection.

The device UI uses the following icons:



Export



Export Private Key



Renew Certificate



Delete Certificate

### To remove a certificate:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > Certificate**.

The Certificate page displays. By default, the Authorities tab is selected.

5. Select the **Certificates** tab.

The page adjusts.

6. In the Certificate table, in the Action column for the certificate authority, click the **Delete Certificate** button.

A confirmation pop-up window displays.

7. Click the **OK** button.

Your settings are saved. The certificate is removed.

# 10

## Manage WireGuard VPN Tunnels

---

The router supports manually configured profiles for client-to-site WireGuard VPN tunnels.

This chapter describes how to set up WireGuard VPN profiles on the router using the device UI.

The chapter includes the following sections:

- [About WireGuard VPN](#)
- [About configuring WireGuard on the router](#)
- [WireGuard VPN client accounts](#)
- [Install the WireGuard utility or app and configuration file on a WireGuard client](#)

**!** **NOTE:** If you are using the Insight Cloud Portal or Insight app to set up WireGuard VPN tunnels on the router, visit [kb.netgear.com/000065774](https://kb.netgear.com/000065774) for knowledge base articles about NETGEAR Insight.

# About WireGuard VPN

The router supports WireGuard VPN software, which generally relies on public-key cryptography with the use of private keys and associated public keys for encryption and authentication between a VPN client and the VPN server. WireGuard VPN software is available free of charge to users who want to install the software on their VPN clients.

A main advantage of WireGuard VPN is that it is very fast and supports roaming of VPN clients without losing VPN connectivity. A disadvantage can be that WireGuard VPN does not assign a dynamic IP address to a VPN client: An assigned IP address is a static IP address.

To set up a client-to-site WireGuard tunnel, remote users must install the WireGuard utility on their computer or WireGuard app on their mobile device, and import the WireGuard VPN client configuration, which is usually provided by a network or system administrator.

The client-to-site WireGuard settings on the router determine the WAN IP address at which the VPN client can reach the router and other settings for the WireGuard connection.

WireGuard requires a static IP address or DDNS service on the router (see [Dynamic DNS](#) on page 61) to enable a remote client such as a computer or mobile device to connect with the router.

If the router uses a static WAN IP address that never changes, WireGuard can use that IP address to connect to the network over a VPN connection.

If the router does not use a static WAN IP address, you can use a DDNS service for the router and register for an account with a host name (also referred to as a domain name). A remote client such as a computer or mobile device can use that host name to connect with the router and access the network over a VPN connection. For more information, see [Dynamic DNS](#) on page 61.

## About configuring WireGuard on the router

**❗ NOTE:** Some knowledge of WireGuard VPN tunnels can make it easier for you to set up a functioning WireGuard VPN connection. For information about WireGuard, visit [wireguard.com](https://wireguard.com).

When you add a WireGuard VPN tunnel connection, you must do the following, as described in the procedure that follows this list:

- Set the VPN server address, which is the WAN IP address or FQDN at which a WireGuard VPN client can reach the router.
- Set the UDP port number for the WireGuard VPN connection.
- Generate a private key and an associated public key for traffic encryption and authentication.
- Set the pool of LAN IP addresses on the router from which the router assigns an IP address to the WireGuard VPN client.
- Set the DNS servers that the WireGuard VPN client must use.

**! NOTE:** You can add a single client-to-site WireGuard VPN connection only. However, you can use this connection configuration for up to 30 WireGuard VPN clients.

You must enable WireGuard VPN and configure the WireGuard VPN service settings on the router before any VPN client can make a WireGuard VPN connection to the router.

**! NOTE:** Make sure that remote clients install their VPN client configuration file (also referred to as a profile) after you configure WireGuard VPN on the router. If you make changes to the WireGuard VPN configuration on the router, the VPN client configuration file that the remote clients use might change, requiring the remote clients to download and install the new VPN client configuration file.

## Enable and configure WireGuard VPN on the router

The IP address range that you assign to WireGuard VPN clients in the following procedure cannot overlap with any WAN or VLAN IP address subnets that are already in use in the network.

### To enable and configure WireGuard VPN on 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > WireGuard**.

The WireGuard page displays. By default, the Basic Settings tab is selected.

5. Click the **Enable Connection** toggle to enable WireGuard VPN so that it is blue and positioned to the right.

You must enable WireGuard VPN so that you can configure the settings. By default, WireGuard VPN is disabled and the toggle is gray and positioned to the left.

6. To specify the router's WireGuard VPN server IP address, do one of the following:

- **Select a detected IP address:** Click in the **Server Address** field, and from the pop-up menu that displays, select the IP address of the WAN interface or the external public IP address, depending on the options that display.
- **Type an IP address or FQDN:** In the **Server Address** field, type an IP address or fully qualified domain name (FQDN or hostname).

The WireGuard client must connect to the specified IP address or FQDN.

7. In the **Port** field, type the UDP port number.

The WireGuard VPN default UDP port number is 51820. The port number can be in the range from 1024 to 65535.

8. Click the **Generate Public and Private Keys** button.

The generated keys display in the Private Key and Public Key fields. The public key is the key that the router uses to authenticate the traffic to and from the client.

9. In the IP Address Range for VPN Clients section, in the **IP Address** field and **Netmask** field, specify the IP subnet on the router from which VPN clients are assigned an IP address for the VPN tunnel.

**ⓘ NOTE:** Be sure that the range of IP address range does not overlap with any WAN, VLAN, or other VPN IP address subnets that are already in use in the network.

10. In the DNS Servers section, select a radio button to set the DNS servers that the VPN client must use:

- **Auto:** The primary and secondary DNS servers are automatically detected.
- **Custom:** In the **DNS 1** field and **DNS 2** field, type the IP addresses for the primary and secondary DNS servers.

11. Click the **Apply** button.

Your settings are saved. WireGuard VPN service is enabled on the router.

For information about setting up WireGuard client accounts, see [WireGuard VPN client accounts](#) on page 296.

Clients must install and set up WireGuard VPN software and the router client configuration file on their computer or mobile device before they can establish a VPN connection to the router.

## Configure client isolation and the MTU for a client-to-site WireGuard VPN connection

You can set up the following optional features that apply to the WireGuard VPN connection:

- **Client isolation:** You can either allow or disallow communication between VPN clients that are connected to the router. By default, communication is disallowed.
- **MTU:** You can set maximum size of the MTU that is applied to the VPN connection after it is established.

### To set up client isolation and the MTU for a WireGuard 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.

- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > WireGuard**.

The WireGuard page displays. By default, the Basic Settings tab is selected.

5. Select the **Advanced Settings** tab.

The page adjusts and shows the advanced settings.

6. Click the **Client Isolation** toggle to allow or disallow communication between VPN clients that are connected to the router:

- **Allow client isolation:** Click the **Client Isolation** toggle so that it is gray and positioned to the left.
- **Disallow client isolation:** Click the **Client Isolation** toggle so that it is blue and positioned to the right (the default setting).

7. In the **MTU** field, enter the maximum size of the MTU for the VPN connection.

The range from 576 to 1440 bytes. The default MTU is 1420 bytes.

8. Click the **Apply** button.

Your settings are saved.

## WireGuard VPN client accounts

For each client who must be able to connect over a WireGuard VPN tunnel to the router, you must set up a client account and communicate the associated user name and password to the client.

A client account can be used only on one client device at any time. If you use the same client account on a second device at the same time, both connections might be negatively affected and unpredictable behavior might occur.

For each client account individually, you can set up a split tunnel, which lets sensitive data be transferred over the VPN tunnel but other data over a second Internet connection. Compared to a regular VPN tunnel, a split tunnel can offer a faster speed, but it can also be less secure. A split VPN tunnel allows you to manage bandwidth by reserving the full VPN tunnel for specific IP addresses only:

- **Full VPN tunnel:** Sends all of the client's traffic across the VPN tunnel. This is the default setting.

For example, if you work from home and log in over a VPN connection to your company, all traffic goes over the company intranet. For example, if you access social media or streaming media, your company might disallow such traffic, depending on their network policy.

- **Split VPN tunnel:** Sends only traffic for specific IP addresses (for example, for a specific server or service) over the VPN tunnel. You define the IP addresses. All other traffic is sent over the Internet.

For example, if you work from home and log in over a VPN connection to your company, only select traffic goes over the company intranet. Social media or streaming media traffic does not go over the over the company intranet and is not subject to the network policy of your company.

## Add a WireGuard VPN client account

Adding a WireGuard VPN client account consists of adding a client name, a public key, and a pre-shared key that a user must import on their client device when they want to establish a WireGuard VPN tunnel. (In many situations, this information is imported by scanning a QR code.) For added convenience and faster speed, you can set up a split tunnel that applies only to the individual client account.

The device UI uses the following icons:



### To add a WireGuard VPN client account:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.

- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > WireGuard**.

The WireGuard page displays. By default, the Basic Settings tab is selected.

5. Select the **WireGuard Clients** tab.

The page adjusts and shows the clients settings.

6. Click the **Add** icon.

The Add/Edit WireGuard Client pop-up window displays.

7. To enable the client account after you click the Apply button, keep the **Enable** toggle blue and positioned to the right (the default setting).

If you want the client account to be disabled after you click the Apply button, click the **Enable** toggle so that it is gray and positioned to the left.

8. In the **Name** field, type a name for the client.

The name is for identification purposes.

9. As an option, in the **IP Address** field, change the IP address.

The IP address must be in the subnet from which WireGuard VPN clients are assigned an IP address for the VPN tunnel (see [About configuring WireGuard on the router](#) on page 292).

By default, an IP address from the defined subnet is automatically entered in the field.

10. As an option, in the **Keepalive** field, change the keep-alive time.

When there is no traffic activity and the keep-alive time expires, the VPN connection is automatically terminated.

The range from 0 to 600 seconds. The default time is 25 seconds. If you set the time to 0 seconds, the keep-alive timer is disabled and the connection is not terminated.

11. To generate a new public key, click the **Generate** button next to the Public Key field.

The client must use the public key to encrypt, decrypt, and authenticate the traffic to and from the router.

12. To generate a new pre-shared key, click the **Generate** button next to the Pre-Shared Key field.

The client must use the pre-shared key as an additional security measure to encrypt and decrypt the traffic to and from the router.

13. To configure a split tunnel, in the Split Tunnel section, do the following:

a. Enable the split tunnel:

By default, the **Split Tunnel** toggle is gray and positioned to the left, which means that the split tunnel option is disabled. To enable the split tunnel option and configure the split tunnel settings, click the **Split Tunnel** toggle so that the toggle is blue and positioned to the right.

b. Set an IP address and netmask (for example, for a server or service) for a split tunnel:

You can either manually enter the IP address and subnet mask that must be sent over the split tunnel or import the IP address and netmask from an existing VLAN that is already defined (see [Add a VLAN profile](#) on page 89):

- **Manually enter the IP address and netmask:** From the menu in the Interface Name column, select **Custom** (the default setting), and type the IP address and subnet mask in the **IP Address** and **Subnet Mask** fields.
- **Add the IP address and netmask from the VLAN:** From the menu in the Interface Name column, select a VLAN, and click the **Apply** button.

c. Optionally, click the **Add** icon, and add another IP address and subnet mask for traffic that must also be sent over the split tunnel.

d. To make a change to an existing split tunnel configuration, select the associated check box, and click the **Edit** icon.

e. To remove an existing split tunnel configuration, select the associated check box, and click the **Delete** icon.

Traffic to each IP address and netmask that you define is sent over the split tunnel. Other traffic is not.

14. Click the **Apply** button.

Your settings are saved. The WireGuard VPN client account is added to the clients table.

## Change a WireGuard VPN client account

You can change the settings for a WireGuard VPN client account, and you can enable or disable a WireGuard VPN client account.

The device UI uses the following icons:

 Add  Edit  Delete

**To change a WireGuard VPN client account:**

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > WireGuard**.

The WireGuard page displays. By default, the Basic Settings tab is selected.

5. Select the **WireGuard Clients** tab.

The page adjusts and shows the clients settings.

6. Select the check box for the client account.
7. Click the **Edit** icon.

The Add/Edit WireGuard Client pop-up window displays.

For more information about changing the settings, see [Add a WireGuard VPN client account](#) on page 297. You cannot change the client name.

8. Click the **Apply** button.

Your settings are saved. The modified settings are displayed in the clients table.

## Remove a WireGuard VPN client account

You can remove a WireGuard VPN client account that you no longer need.

The device UI uses the following icons:

 Add  Edit  Delete

**To remove a WireGuard VPN client account:**

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > WireGuard**.

The WireGuard page displays. By default, the Basic Settings tab is selected.

5. Select the **WireGuard Clients** tab.

The page adjusts and shows the clients settings.

6. Select the check box for the client account.
7. Click the **Delete** icon.

A confirmation pop-up window displays.

8. Click the **Proceed** button

Your settings are saved. The client account is removed from the clients table.

# Export the router's WireGuard VPN client configuration file or QR code

You can export the router's WireGuard VPN client configuration file to a computer or storage device that is connected to the router, and then forward the client configuration file to a WireGuard VPN client that you want to allow to set up WireGuard VPN connectivity to the router. You can also display the WireGuard QR code and make a screenshot of it so that you can forward it to a WireGuard VPN client.

## To export the router's WireGuard VPN client configuration file or WireGuard QR code:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **VPN > WireGuard**.

The WireGuard page displays. By default, the Basic Settings tab is selected.

5. Select the **WireGuard Clients** tab.

The page adjusts and shows the clients settings.

6. For an individual client account, in the Action column, click the **Export** link.

The Export WireGuard Client Config pop-up window displays. By default, the Export tab is selected.

7. Do one of the following:
  - **Export the WireGuard configuration file:** Do the following:
    - a. Keep the Export tab selected, and click the **Export** button.
    - b. Navigate to a location on the connected computer or storage device, and save the client configuration file.
  - **Display and make a screenshot of the WireGuard QR code:** Do the following:
    - a. Click the **QR Code** tab.  
The QR code displays.
    - b. Make a screenshot of the QR code.
8. Send the client configuration file, QR code, or both (or make them available through a URL) to each user that must be able to use a WireGuard VPN connection to connect to the router.

## Install the WireGuard utility or app and configuration file on a WireGuard client

To establish a WireGuard VPN connection to the router using WireGuard software, a remote client must install WireGuard client software utility on their Windows-based or Mac computer or the WireGuard app on their Android or iOS mobile device.

In addition, a remote client must install the client configuration file that is generated on the router to which the WireGuard client must connect, or use the WireGuard QR code that is generated on the router. Typically, this file or QR code is provided by an administrator or is available from a URL on a company website.

For more information about WireGuard, visit [wireguard.com](https://wireguard.com).

### **To download and install the WireGuard utility or app and the router's client configuration file on a Windows-based computer, Mac, iOS device, or Android device:**

1. Download the WireGuard utility or WireGuard app:
  - **Windows-based computer:** Visit [wireguard.com/install/](https://wireguard.com/install/), download the WireGuard utility for a Windows-based computer, and install it on the computer.  
You might need administrative privileges to install the WireGuard client utility.
  - **Mac:** Visit [wireguard.com/install/](https://wireguard.com/install/), download the WireGuard utility for a Mac, and install it on the Mac.

- **Android device:** On your Android device, visit the Google Play Store and download and install the WireGuard app.
- **iOS device:** On your iOS device, visit the Apple app store and download and install the WireGuard app.

2. Get the WireGuard VPN router's client configuration file or QR code.

The client configuration file is a `.conf` file that is generated on the router to which the WireGuard VPN client must connect. The QR code contains the same information as the client configuration file.

Typically, the `.conf` file or QR code is provided by an administrator or is available from a URL on a company website.

3. Do one of the following:

- Start the WireGuard VPN utility, search for and import the `.conf` file, and follow the prompts in the utility to complete the setup.
- Open the WireGuard app, scan the QR code, import the client configuration file, and follow the prompts in the app to complete the setup.

The client device is now ready for setting up a WireGuard VPN connection to the router.

# 11

## Manage the QoS Settings

---

This chapter describes how you can manage the quality of service (QoS) settings in the form of Smart Queue Management (SQM) for WAN interfaces.

SQM keeps latency as low as possible on all types of traffic. You can enable and configure SQM for each WAN interface.

The chapter includes the following sections:

- [Use a speed test to automatically configure SQM for a WAN port](#)
- [Manually configure SQM for a WAN port](#)

**!** **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/000065774](http://kb.netgear.com/000065774) for knowledge base articles about NETGEAR Insight.

# Use a speed test to automatically configure SQM for a WAN port

## To use a speed test automatically configure Smart Queue Management (SQM) for a WAN 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **QoS > SQM**.

The Smart Queue Management page displays. By default the WAN1 tab is selected.

5. To configure the WAN2 port instead of the WAN1 port, click the **WAN2** tab.

6. Enable SQM by clicking the **Enable** toggle so that so the toggle is blue and positioned to the right.

By default, SQM is disabled and the **Enable** toggle is gray and positioned to the left.

The Internet Bandwidth section displays.

7. Click the **Take a Speed Test** button.

A pop-up window displays.

8. Click the **Test Speed** button.

The Privacy Policy pop-up window displays.

9. 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.

10. (Optional) To stop the speed test, click the **Stop Test** 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 Done.

11. Click the **Done** button.

The detected speeds are automatically entered in the **Download** and **Upload** fields.

12. To change the speeds in the fields, manually overwrite them.

13. Click the **Apply** button.

Your settings are saved.

## Manually configure SQM for a WAN port

### To manually configure Smart Queue Management (SQM) for a WAN 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **QoS > SQM**.

The Smart Queue Management page displays. By default the WAN1 tab is selected.

5. To configure the WAN2 port instead of the WAN1 port, click the **WAN2** tab.
6. Enable SQM by clicking the **Enable** toggle so that so the toggle is blue and positioned to the right.

By default, SQM is disabled and the **Enable** toggle is gray and positioned to the left.

The Internet Bandwidth section displays.

7. In the **Download** field, type the maximum download bandwidth that must be applied to the WAN port, and set the unit as **Kbps**, **Mbps**, or **Gbps**.

The range is from 300 Kbps to 5 Gbps.

8. In the **Upload** field, type the maximum upload bandwidth that must be applied to the WAN port, and set the unit as **Kbps**, **Mbps**, or **Gbps**.

The range is from 300 Kbps to 5 Gbps.

9. Click the **Apply** button.

Your settings are saved.

# 12

## Install and Launch Third-Party Applications

---

This chapter describes how you can install and launch third-party applications on the router.

The chapter includes the following sections:

- [Overview of supported applications](#)
- [Install and launch an application](#)
- [Disable or enable an application](#)
- [Uninstall an application](#)

**!** **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/000065774](http://kb.netgear.com/000065774) for knowledge base articles about NETGEAR Insight.

# Overview of supported applications

The router supports the following third-party applications:

- **Domotz:** Domotz is a network monitoring and remote management tool designed to simplify and enhance the management of IT networks and connected devices. It provides real-time monitoring, device discovery, scripting & automations, and remote access capabilities allowing users to troubleshoot issues, perform remote maintenance, and ensure optimal performance of their networks.

For more information, see <https://www.domotz.com/features.php> and <https://help.domotz.com/>.

## Install and launch an application

After installation and launch of an application, you need account credentials to log in to the application. You can set up an account by visiting the third-party vendor who developed the application.

### To install and launch an application:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Applications**.

The Applications page displays.

5. For the application that you want to install, click the **Install** button.

A confirmation pop-up window displays.

6. Click the **Continue** button.

The application is installed on the router.

7. Click the **Launch** button.

The login page displays.

## Disable or enable an application

After installation, an application is automatically enabled. You can disable the application or reenable it.

### To disable or enable an application:

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Applications**.

The Applications page displays.

5. For the application that you want to disable or reenable, click the toggle:
  - **The toggle is blue and positioned to the right:** The Insight mode is enabled. This is the default setting after installing the application.
  - **The toggle is gray and positioned to the left:** The Insight mode is disabled.

A confirmation pop-up window displays.

## Uninstall an application

You can uninstall an application that you no longer need.

### To uninstall an application:

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

The Dashboard displays.

4. Select **Applications**.  
The Applications page displays.
5. For the application that you want to uninstall, click the **Uninstall** button.  
A confirmation pop-up window displays.
6. Click the **OK** button.

The application is uninstalled from the router and confirmation pop-up window displays.

# 13

## 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:

- [Check the Internet speed](#)
- [Ping the IP address or domain name of a device or network location](#)
- [Look up a DNS domain name or IP address](#)
- [Trace a route](#)
- [Capture Ethernet packets](#)
- [Sequence to restart the router network](#)
- [Troubleshoot with the LEDs](#)
- [You cannot log in to the device UI of the router](#)
- [Troubleshoot Internet browsing](#)
- [Changes are not saved](#)
- [Check the WAN port IP address](#)
- [You enter the wrong password and can no longer log in to the router](#)
- [Troubleshoot the network using your computer's ping utility](#)

**!** **NOTE:** If you are using the Insight Cloud Portal or Insight app to perform diagnostics and troubleshoot the router, visit [kb.netgear.com/000065774](http://kb.netgear.com/000065774) 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:
  - Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
  - If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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.

(Continued)

Setting	Description
Ping Interval	The interval between pings. The range is from 1 to 10. The default interval is 1 second.
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	<p>From the <b>Ping Interface</b> menu, select a specific interface or VLAN from which to send the ping, or select <b>Any</b> to send the ping from any interface or VLAN:</p> <ul style="list-style-type: none"> <li>• WAN interfaces are for the physical WAN ports</li> <li>• LAN interfaces are for the physical LAN ports</li> <li>• br-lan, or if you set up a VLAN2 and VLAN3, br-vlan2 and br-vlan3 are the Linux bridge interfaces</li> <li>• VLAN interfaces are the virtual interfaces that are created on top of the physical LAN port</li> </ul> <p>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.</p>

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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	<p>From the <b>Capture Interface</b> menu, select a specific interface or VLAN on which packets must be captured, or select <b>Any</b> to capture packets on any interface and VLAN:</p> <ul style="list-style-type: none"> <li>• WAN interfaces are for the physical WAN ports</li> <li>• LAN interfaces are for the physical LAN ports</li> <li>• br-lan, or if you set up a VLAN2 and VLAN3, br-vlan2 and br-vlan3 are the Linux bridge interfaces</li> <li>• VLAN interfaces are the virtual interfaces that are created on top of the physical LAN port</li> </ul> <p>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.</p>
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	<p>To capture packets for a specific client only, click the <b>Client Filter</b> toggle so that it is blue and positioned to the right and type the client's MAC address in the <b>Client Filter</b> field.</p> <p>The MAC address must be in hexadecimal format with each octet separated by a hyphen, for example 00-11-22-33-44-55.</p> <p>By default, the Client Filter toggle is gray and positioned the left, indicating that client filtering is disabled and packets for <i>all</i> clients are captured.</p>
Capture Duration	<p>Type the maximum duration of the capture process (that is, if you do not click the <b>Stop</b> button).</p> <p>The range is from 10 to 3600 seconds. By default, the maximum duration is 300 seconds.</p>

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 211), 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 216. 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/](https://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 21). You can also manually set up your Internet connection (see [Manage the Internet Settings for the WAN1 port](#) on page 45).
- 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 51 or [Manually configure a static Internet connection for the WAN1 port](#) on page 48.

## 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 41.

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 183.

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 321.

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 216.

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](https://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 211).

## 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/](https://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 89 or [Change a VLAN profile](#) on page 94), 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 or 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 329.

## 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 32.

3. Type one of the following passwords:

- Type 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 managing the router through the Engage Controller, type the site password for the Engage site to which the router is onboarded.
- If you are managing the router through the Insight Cloud Portal or Insight app, type the Insight network password for the Insight network location to which the router is added. (The Engage Controller and NETGEAR Insight are mutually exclusive management methods.)

For more information about the credentials, see [Credentials for the device UI](#) on page 42.

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 321.

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 45 and [Set Up and Configure a Dual WAN Connection](#) on page 66.

## 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 191), you must reset the router to factory default settings (see [Use the Reset button to reset the router](#) on page 216) 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 329 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

## Configure IPSec VPN Client Settings

---

This appendix includes information about how you can configure IPSec VPN settings on an IPSec VPN client device.

The appendix covers the following topics:

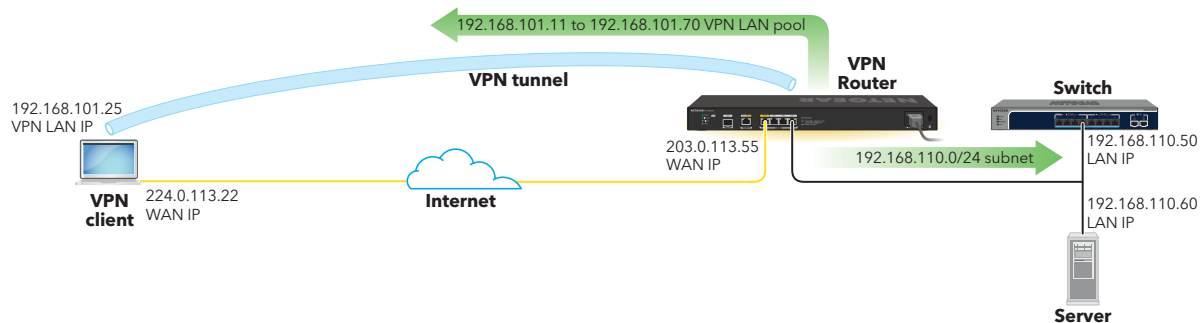
- [Windows-based computers](#)
- [Mac computers](#)
- [iOS/iPad devices](#)
- [Android devices](#)

# Windows-based computers

Follow these steps to set up a secure client-to-site VPN connection on your Windows-based computer. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

## IKEv2 EAP - MSCHAPv2 VPN setup on a Windows-based computer

For this authentication with the VPN router, the VPN client uses a Certificate Authority (CA) associated with the server certificate on the VPN router. In this example, the VPN client uses the WAN IP address 224.0.113.22 as the local identifier, and the WAN IP address of the VPN router is 203.0.113.55.



## Transfer the CA certificate to a Windows-based computer for IKEv2 EAP - MSCHAPv2 VPN setup

Transfer the necessary Certificate Authority (CA) certificate and configure the VPN settings to securely access your organization's network from anywhere with an internet connection.

### To transfer the CA certificate to a Windows-based computer for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Transfer the CA certificate to the client device using a method like email, USB drive, or cloud storage.
2. Locate the CA certificate file, double-click it, and click **Open**.
3. In the Certificate Information window, click **Install Certificate**.

The Certificate Import Wizard displays.

4. When prompted to select the Store Location, select **Local Machine**, and click **Next**.
5. For Certificate Store, select **Place all certificates in the following store** and click **Browse**.
6. Select **Trusted Root Certification Authorities** and click **Next**.
7. Verify the specified settings by selecting **Certificate Store Selected by User** and click **Finish**.

## Configure VPN settings on a Windows-based computer for IKEv2 EAP - MSCHAPv2 VPN setup

Configure a Windows-based computer to establish a secure VPN connection to your organization's network using IKEv2 EAP - MSCHAPv2.

### To configure VPN settings on a Windows-based computer for IKEv2 EAP - MSCHAPv2:

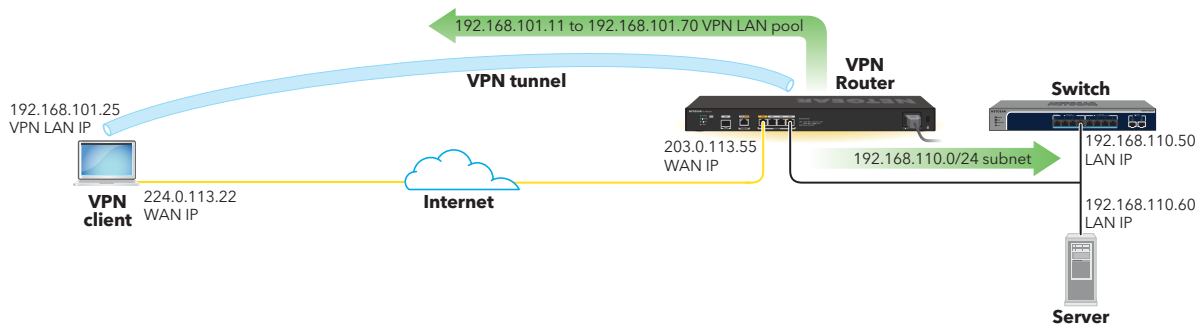
1. Click the **Start menu** and click **Settings** (the gear icon).
2. Click **Network & Internet**, and then click **VPN**.
3. Under VPN connections, click **Add VPN**.
4. Configure the VPN connection:
  - **Connection name**: Enter a connection name, for example: OfficeVPN.
  - **Server name or address**: Enter the server IP address or server name, for example: 203.0.113.55.
  - **VPN type**: Select **IKEv2**.
  - **Type of sign-in info**: Select **Username and password**.
  - **Username**: Enter the VPN username, for example: Netgear.
  - **Password**: Enter the VPN password, for example: OfficePassword.
5. Click **Save**.  
The VPN connection you created appears under the list of available VPN connections.
6. Click **Connect** to initiate the VPN connection. You can also verify your connection by checking the network icon in the system tray.

## Mac computers

Follow these steps to set up a secure client-to-site VPN connection on your Mac computer. Ensure that you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

# IKEv2 EAP - MSCHAPv2 VPN setup on a Mac computer

For this authentication with the VPN router, the VPN client uses a Certificate Authority (CA) associated with the server certificate on the VPN router. In this example, the VPN client uses the WAN IP address 224.0.113.22 as the local identifier, and the WAN IP address of the VPN router is 203.0.113.55.



## Transfer the CA certificate to a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup

Transfer the necessary Certificate Authority (CA) certificate and configure the VPN settings to securely access your organization's network from anywhere with an internet connection.

### To transfer the CA certificate to a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Transfer the CA certificate to the client device using a method such as email, AirDrop, USB drive, or cloud storage.
2. Locate the CA certificate file, double-click it, and open it with Keychain Access.
3. Keychain access prompts you to add the certificate. Click **Add**.  
By default, the certificate is added to the login keychain.
4. (Optional) For broader use, move the certificate to the system keychain.

## Configure VPN settings on a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup

Configure a Mac computer to establish a secure VPN connection to your organization's network using IKEv2 EAP - MSCHAPv2.

### To configure VPN settings on a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Click the **Apple** logo and select **System Settings**.
2. Click **Network**.
3. Click the **+** button and select **Add VPN Connection > IKEv2**.
4. Configure the VPN connection by entering the following details:
  - **Interface:** VPN
  - **VPN Type:** IKEv2
  - **Service Name:** Enter a service name, for example: OfficeVPN.
5. Click **Create**.
6. Enter the following VPN information:
  - **Server Address:** Enter the service IP address, for example: 203.0.113.55.
  - **Remote ID:** Enter the remote ID, for example: 203.0.113.55
  - **Local ID:** Optional entry; fill as required.

### Set PSK on a MAC computer for IKEv2 EAP - MSCHAPv2 VPN setup

IKEv2 EAP-MSCHAPv2 is a method for establishing a secure VPN connection using the second version of the Internet Key Exchange (IKEv2) protocol. It uses the Extensible Authentication Protocol (EAP) combined with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2) for robust user authentication.

### To set the PSK on a Mac computer for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Click **Authentication Settings**.
2. Select **None** in **Authentication Setup**.
3. Select **Shared Secret** and enter the pre-shared key.
4. Click **OK** to close the Authentication Settings window.
5. Click **Apply** to save the VPN configuration.
6. Click **Connect** next to the VPN connection you just created.
7. If prompted, enter any additional authentication credentials (such as username and password).

The VPN Status changes to Connected and a VPN icon displays in the menu bar at the top of your screen. Click the VPN icon to view connection details and status.

# IKEv2 PSK VPN setup on a Mac computer

Configure your Mac computer as a VPN client using the IKEv2 PSK authentication for secure access to your organization's network resources.

## Configure VPN settings on a Mac computer for IKEv2 PSK VPN setup

Configure a Mac computer to establish a secure VPN connection to your organization's network using IKEv2 PSK.

### To configure VPN settings on a Mac computer for IKEv2 PSK VPN setup:

1. Click the **Apple** logo and select **System Preferences**.
2. Click on **Network**.
3. Click the **+** button and select **Add VPN Connection > IKEv2**.
4. Configure the VPN connection by entering the following information:
  - **Interface:** VPN
  - **VPN Type:** IKEv2
  - **Service Name:** Enter a service name.
  - **Server Address:** Enter the IP address or domain name of the VPN server provided by your administrator.

## Set PSK on a Mac computer for IKEv2 PSK VPN setup

IKEv2 PSK is a method for establishing a secure VPN connection using the second version of the Internet Key Exchange (IKEv2) protocol. It utilizes a pre-shared key (PSK) for authentication, ensuring a secure connection between the VPN client and server.

### To set the PSK on a Mac computer for IKEv2 PSK VPN setup:

1. Click on **Authentication Settings**.
2. Select **Machine Authentication** and for **Shared Secret**, enter the pre-shared key (PSK) provided by your administrator.
3. Click **OK** to close the Authentication Settings window.
4. Click **Create** to save the VPN configuration.
5. Click **Connect** next to the VPN connection you just created.
6. If prompted, enter any additional authentication credentials (such as username and password).

The VPN Status changes to Connected and a VPN icon displays in the menu bar at the top of your screen. Click the VPN icon to view connection details and status.

## IKEv1 PSK + XAuth VPN setup on a Mac computer

Follow these steps to set up a secure client-to-site VPN connection on your Mac computer. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

### Configure VPN settings on a Mac computer for IKEv1 PSK + XAUTH VPN setup

Configure a Mac computer to establish a secure VPN connection to your organization's network using IKEv1 PSK + XAUTH.

#### To configure VPN settings on a Mac computer for h IKEv1 PSK + XAUTH VPN setup:

1. Click the **Apple** logo and select **System Settings**.
2. Click **Network**.
3. Click the **+** button to add a new network connection.
4. Configure the VPN connection by entering the following information:
  - **Interface:** VPN
  - **VPN Type:** L2TP over IPSec
  - **Service Name:** Enter a service name.
  - **Servicer Address:** Enter the IP address or domain name of the VPN server provided by your administrator, for example: 203.0.113.55.

### Set PSK on a Mac computer for IKEv1 PSK + XAUTH VPN setup

IKEv1 PSK is a method for establishing a secure VPN connection using the first version of the Internet Key Exchange (IKEv1) protocol. It uses a pre-shared key (PSK) to create a secure connection. Optionally, additional extended authentication (XAUTH) can be used to verify the user's identity.

#### To set PSK on a Mac computer for IKEv1 PSK + XAUTH VPN setup:

1. Click **Authentication Settings**.
2. Select **Shared Secret**, enter the pre-shared key provided by your administrator.

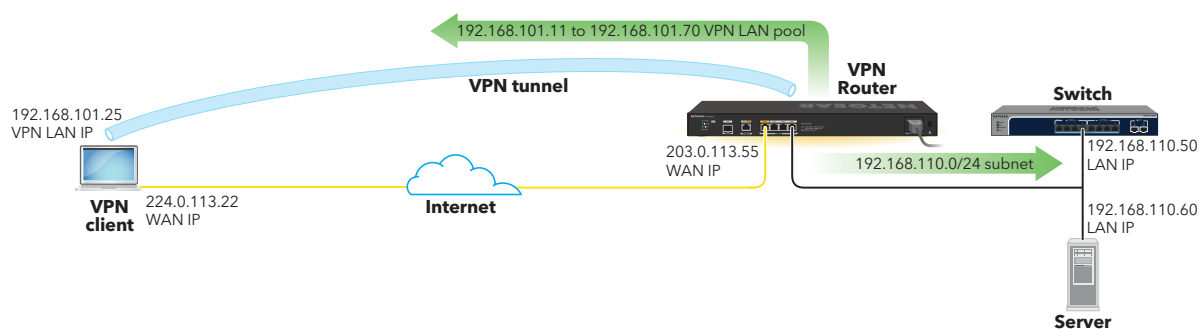
3. Click **Options** and select the **User Authentication** checkbox.
4. Enter your VPN account username and password provided by your administrator.
5. Click **OK** to close the Authentication Settings window.
6. Click **Create** to save the VPN configuration.
7. Click **Connect** next to the VPN connection you just created.
8. If prompted, enter any additional authentication credentials (such as username and password).

## iOS/iPad devices

Follow these steps to set up a secure client-to-site VPN connection on your iOS/iPad devices. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

## IKEv2 EAP - MSCHAPv2 VPN setup on an iOS/iPad device

For this authentication with the VPN router, the VPN client uses a Certificate Authority (CA) associated with the server certificate on the VPN router. In this example, the VPN client uses the WAN IP address 224.0.113.22 as the local identifier, and the WAN IP address of the VPN router is 203.0.113.55.



## Transfer the CA certificate to an iOS/iPad device for IKEv2 EAP - MSCHAPv2 VPN setup

Transfer the necessary Certificate Authority (CA) certificate and configure the VPN settings to securely access your organization's network from anywhere with an internet connection.

### To transfer the CA certificate to an iOS/iPad device for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Transfer the CA certificate to the client device using a method such as email, AirDrop, or cloud storage.
2. On the iOS device, open the email or cloud storage app where you transferred the CA certificate file.
3. Tap on the CA certificate file to open it. iOS will prompt you to install the certificate.
4. Tap **Install** and follow the prompts to complete the installation.
5. If prompted to review the profile in the Settings app for installation, tap Settings and tap **Profile Downloaded**, and follow the prompts to complete the installation.

## Configure VPN settings on an iOS/iPad device for IKEv2 EAP - MSCHAPv2 VPN setup

Configure an iOS/iPad device to establish a secure VPN connection to your organization's network using IKEv2 EAP - MSCHAPv2.

### To configure VPN settings on an iOS/iPad device for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Open the Settings app on your iOS device.
2. Tap **General**, then scroll down and tap **VPN & Device Management** to access VPN settings.
3. Tap **VPN** and then **Add VPN Configuration**.
4. Enter the following VPN information:
  - **Type:** IKEv2
  - **Description:** Enter a name for this VPN connection, for example: OfficeVPN.
  - **Server:** Enter the server IP address, for example: 203.0.113.55
  - **Remote ID:** Enter the Remote ID, for example: 203.0.113.55
  - **Local ID:** Optional entry; specify as required.
  - **User Authentication:** Select **Username**.

- **Username:** Enter the VPN username, for example: Netgear.
  - **Password:** Enter VPN user password, for example: OfficePassword.
5. Tap **Done** to save the VPN configuration.
  6. To connect to the VPN, toggle the VPN switch to the **On** position in the VPN settings.  
Once connected, a VPN icon displays in the status bar of your iOS device's screen. You can also check the VPN status in the Settings app, tap **VPN**, and look for the status indicator which will show Connected or Not Connected.

## IKEv2 PSK VPN setup on an iOS/iPad device

Follow these steps to set up a secure client-to-site VPN connection on your iOS/iPad device. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

### Configure VPN settings on an iOS/iPad device for IKEv2 PSK VPN setup

Configure an iOS/iPad device to establish a secure VPN connection to your organization's network using IKEv2 PSK.

#### To configure VPN settings on an iOS/iPad device for IKEv2 PSK VPN setup:

1. Open the Settings app on your iOS device.
2. Tap **General**, then scroll down and tap **VPN & Device Management** to access VPN settings.
3. Tap **VPN** and then **Add VPN Configuration**.
4. Enter the following VPN information:
  - **Type:** IKEv2
  - **Description:** Enter a name for this VPN connection, for example: OfficeVPN.
  - **Server:** Enter the server IP address or domain name of the VPN server provided by your administrator, for example: 203.0.113.55
  - **Remote ID:** Enter the Remote ID configured from Client-to-Site, for example: 203.0.113.55
  - **Local ID:** Optional entry; specify as required.
5. Tap **Done** to save the VPN configuration.
6. To connect to the VPN, toggle the VPN switch to the **On** position in the VPN settings.

Once connected, a VPN icon displays in the status bar of your iOS device's screen. You can also check the VPN status in the Settings app, tap **VPN**, and look for the status indicator which will show Connected or Not Connected.

## Set PSK on an iOS/iPad device for IKEv2 PSK setup

IKEv2 PSK is a method for establishing a secure VPN connection using the second version of the Internet Key Exchange (IKEv2) protocol. It utilizes a pre-shared key (PSK) for authentication, ensuring a secure connection between the VPN client and server.

### **To set the PSK on an iOS/iPad device for IKEv2 PSK VPN setup:**

1. Scroll down to the Authentication section.
  2. Set User Authentication to **Username**.
  3. Enter the username and password for the VPN user credentials provided by your administrator.
  4. Tap **Done** to save the VPN configuration.
  5. To connect to the VPN, toggle the **VPN** switch to the **On** position in the VPN settings.
- Once connected, a VPN icon displays in the status bar of your iOS device's screen. You can also check the VPN status in the Settings app under VPN.

## IKEv1 PSK + XAUTH VPN setup on an iOS/iPad device

Follow these steps to set up a secure client-to-site VPN connection on your iOS/iPad device. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

## Configure VPN settings on an iOS/iPad device for IKEv1 PSK + XAUTH VPN setup

Configure an iOS/iPad device to establish a secure VPN connection to your organization's network using IKEv1 PSK + XAUTH.

### **To configure VPN settings on an iOS/iPad device for IKEv1 PSK + XAUTH VPN setup:**

1. Open the Settings app on your iOS device.
2. Tap **General**, then scroll down and tap **VPN & Device Management** to access VPN settings.
3. Tap **VPN** and then **Add VPN Configuration**.

4. Enter the following VPN information:
  - **Type:** IPSec
  - **Description:** Enter a name for this VPN connection, for example: OfficeVPN.
  - **Server:** Enter the server IP address or domain name of the VPN server provided by your administrator, for example: 203.0.113.55
  - **Account:** Enter the VPN username, for example: Netgear.
  - **Password:** Enter the VPN password, for example: OfficePassword.
5. Tap **Done** to save the VPN configuration.
6. To connect to the VPN, toggle the VPN switch to the **On** position in the VPN settings.  
Once connected, a VPN icon displays in the status bar of your iOS device's screen. You can also check the VPN status in the Settings app, tap **VPN**, and look for the status indicator which will show Connected or Not Connected.

## Set PSK and enable XAUTH on an iOS/iPad device for IKEv1 PSK + XAUTH VPN setup

A PSK + XAUTH VPN setup uses a pre-shared key (PSK) to create a secure connection, then asks for additional extended authentication (XAUTH) to verify the user's identity. This two-step process enhances security by ensuring both the device and the user are authenticated.

### To set the PSK and enable XAUTH on an iOS/iPad device for IKEv1 PSK + XAUTH VPN setup:

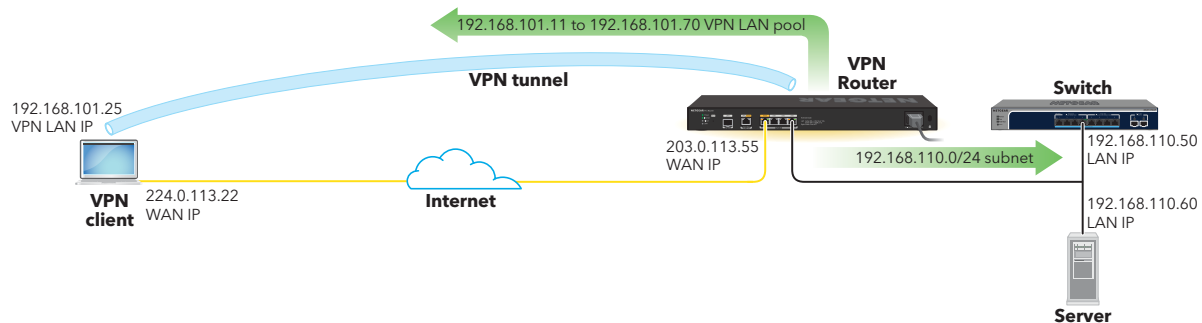
1. Toggle the **Use Certificate** option to the **off** position.
2. For Shared Secret and Machine Authentication, enter the pre-shared key (PSK) provided by your administrator.
3. Scroll down and tap **Extended Authentication (XAUTH)**.
4. Toggle the **XAUTH** option to the **On** position.
5. Enter your VPN account username and password provided by your administrator.
6. Tap **Done** to save the VPN configuration.
7. To connect to the VPN, toggle the **VPN** switch to the **On** position in the VPN settings.  
Once connected, a VPN icon displays in the status bar of your iOS device's screen. You can also check the VPN status in the Settings app under VPN.

# Android devices

Follow these steps to set up a secure client-to-site VPN connection on your Android devices. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

## IKEv2 EAP - MSCHAPv2 VPN setup on an Android device

For this authentication with the VPN router, the VPN client uses a Certificate Authority (CA) associated with the server certificate on the VPN router. In this example, the VPN client uses the WAN IP address 224.0.113.22 as the local identifier, and the WAN IP address of the VPN router is 203.0.113.55.



## Transfer the CA Certificate to an Android device for IKEv2 EAP - MSCHAPv2 VPN setup

Transfer the necessary Certificate Authority (CA) certificate and configure the VPN settings to securely access your organization's network from anywhere with an internet connection.

### To transfer the CA certificate to an Android device for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Transfer the CA certificate to the client device using a method such as email, file transfer, or cloud storage.
2. On the Android device, open the email or file manager app where you transferred the CA certificate file.

3. Tap on the CA certificate file to open it. Android will prompt you to install the certificate.
4. Tap **Install** and follow the prompts to complete the installation.

Alternatively, you can manually install the CA certificate by going to **Settings > Security and privacy > More / Other security settings > Install from device storage > CA certificate**.

## Configure VPN settings on an Android device for IKEv2 EAP - MSCHAPv2 VPN setup

Configure an Android device to establish a secure VPN connection to your organization's network using IKEv2 EAP - MSCHAPv2.

### To configure VPN settings on an Android device for IKEv2 EAP - MSCHAPv2 VPN setup:

1. Open the Settings app on your Android device.
2. Tap **Connections** and then **VPN**.  
Depending on the version of Android, tap **More connection settings** to find the VPN option.
3. Tap the **+** icon or select the more options menu (three dots) and select **Add VPN** to add a new VPN configuration.
4. Enter the following VPN information:
  - **Name:** Enter a connection a name, for example: OfficeVPN.
  - **Type:** Select **IKEv2/IPSEC MSCHAPv2**.
  - **Server address:** Enter server IP address or domain name of the VPN server provided by your administrator, for example: 203.0.113.55.
  - **IPSec CA certificate:** Select **Don't verify server**.
  - **IPSec server certificate:** Select **Received from server**.
  - **Username:** Enter your VPN username, for example: Netgear.
  - **Password:** Enter VPN your password, for example: OfficePassword.
5. Tap **Save** or **Done** to save the VPN configuration.
6. To connect to the VPN, go back to the VPN settings screen and tap on the VPN configuration you just created, and tap **Connect**.

Once connected, you'll see a VPN icon in the status bar at the top of your Android device's screen. You can also check the VPN status in the Settings app under VPN.

# IKEv2 PSK VPN setup on an Android device

Follow these steps to set up a secure client-to-site VPN connection on your Android device. Ensure you have all the necessary VPN security settings and follow any recommendations provided by your company's network administrator.

## Configure VPN settings on an Android device for IKEv2 PSK setup

Configure an Android device to establish a secure VPN connection to your organization's network using IKEv2 PSK.

### To configure VPN settings on an Android device for IKEv2 PSK setup:

1. Open the Settings app on your Android device.
2. Tap **Connections** and then **VPN**.  
Depending on the version of Android, you may need to tap **More connection settings** to find the VPN option.
3. Tap the **+** icon or select the more options menu (three dots) and select **Add VPN** to add a new VPN configuration.
4. Enter the following VPN details:
  - **Name:** Enter a name for the VPN connection, for example: OfficeVPN.
  - **Type:** Select **IKEv2/IPSec PSK**.
  - **Server address:** Enter the server IP address or domain name of the VPN server provided by your administrator, for example: 203.0.113.55.
  - **IPsec pre-shared key:** Enter the pre-shared key (PSK) provided by your administrator.
5. Tap **Save** or **Done** to save the VPN configuration.
6. To connect to the VPN, go back to the VPN settings screen, tap on the VPN configuration you just created, and tap **Connect**.

Once connected, a VPN icon displays in the status bar at the top of your Android device's screen. You can also check the VPN status in the Settings app under VPN.

# B

## 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 214.

Table 7. Factory default settings


Feature	Default Setting
<b>Management and login settings</b>	
Management mode	<p>Standalone</p> <p>or</p> <p>Standalone <i>and</i> NETGEAR Engage Controller management (both modes can be supported simultaneously)</p> <p>or</p> <p>Standalone <i>and</i> NETGEAR Insight remote management (both modes can be supported simultaneously)</p> <p> <b>NOTE:</b> The Engage Controller and Insight are mutually exclusive management methods.</p>
User login URL	www.routerlogin.net (or www.routerlogin.com or 192.168.1.1)
User name	<b>admin</b> , nonconfigurable
Router login password	<p>The first time that you log in to the device UI, you must define the router login password.</p> <p>If you let the NETGEAR Engage Controller onboard the router, type the Engage site password. For more information, see <a href="#">Credentials for the device UI</a> on page 42.</p> <p>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, type the Insight network password for the Insight network location. For more information, see <a href="#">Credentials for the device UI</a> on page 42.</p>
Idle session time-out	45 minutes
Password recovery	Disabled
<b>Internet connection</b>	
WAN MAC address	Use default hardware address
WAN MTU size	Determined by the protocol that is used for the Internet connection
Dynamic DNS	Not set up
Port speed	AutoSensing

Table 7. Factory default settings (Continued)

Feature	Default Setting
<b>Default VLAN and LAN</b>	
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
Sequential IP address	Disabled
VLANs	VLAN 1 with all LAN ports as untagged members
mDNS Gateway	Disabled
<b>General system settings</b>	
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
LLDP	Enabled, except for the WAN1 port
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
Third-party applications	None installed
<b>WAN security and Firewall</b>	
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)

Table 7. Factory default settings (Continued)

Feature	Default Setting
Port scan and DoS protection	Enabled
DMZ server	None
Respond to ping on Internet port	Disabled
SIP ALG	Enabled
Simple Network Management Protocol (SNMP)	Not set up
TCP session time-out	1800 seconds
ICMP session time-out	30 seconds
Maximum concurrent connections	250,000
IPSec pass-through	Enabled
PPTP pass-through	Enabled
L2TP pass-through	Enabled
Traffic rules	None set up
Dual WAN traffic rules	None set up
Outbound NAT rules	None set up
Port forwarding rules	None set up
Port triggering rules	None set up
<b>VPN</b>	
IPSec profiles	Amazon Web Services Microsoft Azure Default Default Client to Site IKEv1 Default Client to Site IKEv2
Site-to-site	None set up
Client-to-site	None set up
VPN users	None set up
Certificates	None set up
OpenVPN	Disabled

Table 7. Factory default settings (Continued)

Feature	Default Setting
WireGuard VPN	Disabled
<b>QoS</b>	
SQM	Disabled

## 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/](https://netgear.com/support/download/).

Table 8. 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)
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